ICT TECHNICAL HANDBOOK

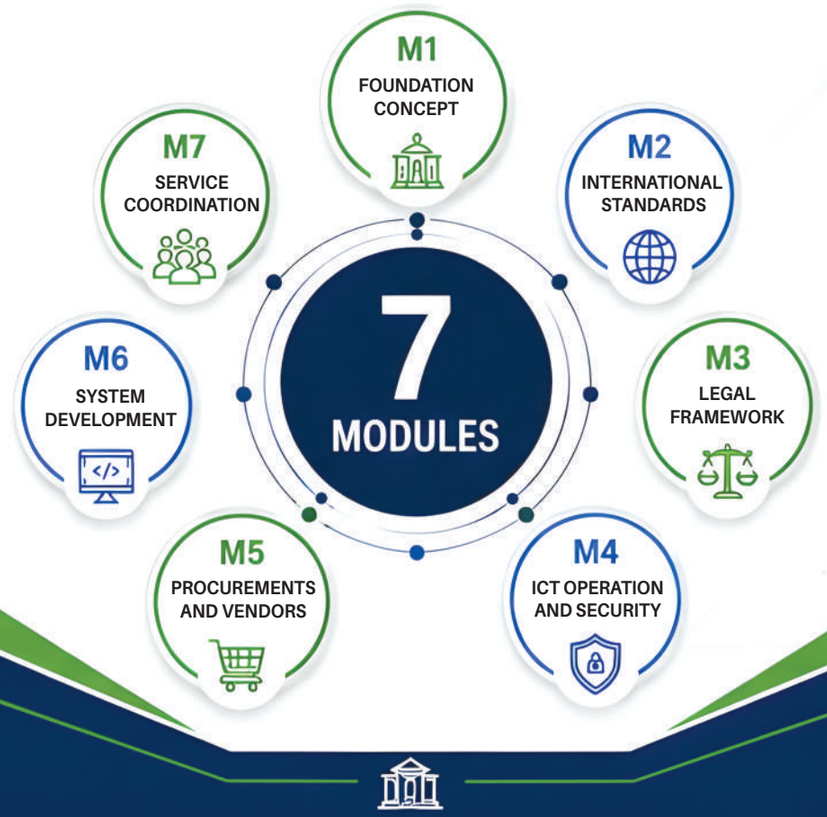
for Province and Local Government

ICT TECHNICAL HANDBOOK

STANDARDIZED

ICT TECHNICAL HANDBOOK

for Province and Local Government



Gandaki Province Government
Office of the Chief Minister and Council of Ministers (OCMCM)
Provincial and Local Governance Strengthening Programme (PLGSP)

© Gandaki Province Government,
Office of the Chief Minister and Council of Ministers,
Provincial and Local Governance Strengthening Programme (PLGSP)

Pokhara, Nepal
+977-061-457648, 457851
ocmcm@gandaki.gov.np
www.ocmcm.gandaki.gov.npp

This handbook was produced for ICT officials of Gandaki Province Government offices and Local Governments by OCMCM, PLGSP, Gandaki Province.

Rights and Permissions

The material in this work is subject to copyright. However, as the PLGSP encourages the dissemination of knowledge for public administration excellence, the contents of this handbook may be copied, adapted, and modified for contextual use in official ICT operations.

Reproduction for non-commercial purposes is fully permitted, provided that full attribution is given. Any utilization beyond non-commercial adaptation—including commercial use, resale, or commercial redistribution—requires prior written permission from OCMCM, PLGSP. Permitted adaptations must not digitally alter the content in a manner that distorts its original meaning or context.

Attribution:

Please cite this work as follows:

"OCMCM, PLGSP, Gandaki Province. 2026. Standardized ICT Technical Handbook for Provincial and Local Government Offices, Gandaki Province."

Preface / प्रस्तावना

शुभकामना

नेपालको संविधानले निर्दिष्ट गरेको प्रदेशको एकल तथा साझा अधिकार क्षेत्रको कार्यान्यन मार्फत लोकतान्त्रिक मूल्य-मान्यता र नागरिक अधिकारलाई संस्थागत गर्दै सुशासनको प्रत्याभूति गराउन गण्डकी प्रदेश सरकार पूर्ण रूपमा प्रतिबद्ध छ। वर्तमान सूचना, सञ्चार र प्रविधिको युगमा परम्परागत प्रशासनिक कार्यशैलीलाई रूपान्तरण गर्दै सार्वजनिक सेवालाई चुस्त, दुरुस्त, पारदर्शी र जवाफदेही बनाउन डिजिटल शासन प्रणाली अपरिहार्य भइसकेको छ। यस सन्दर्भमा, गण्डकी प्रदेश सरकार नागरिक-केन्द्रित डिजिटल सुशासन स्थापना गर्न कटिबद्ध रहेको प्रतिबद्धता समेत व्यक्त गर्दछु। सो सन्दर्भमा गण्डकी प्रदेश सरकार, मुख्यमन्त्री तथा मन्त्रिपरिषद्को कार्यालयद्वारा प्रदेश र स्थानीय तहका सरकारी कार्यालयहरूका लागि "सूचना प्रविधि गतिविधी सञ्चालनको प्राविधिक हातेपुस्तिका" प्रकाशन गरी कार्यान्वयनमा ल्याउन पाउँदा मलाई अत्यन्त खुसी लागेको छ। प्रदेशको प्रशासनिक इतिहासमा विशिष्टीकृत प्राविधिक मार्गदर्शन र मापदण्ड समेटिएको यस प्रकृतिको हातेपुस्तिका पहिलो पटक प्रकाशन हुनु आफैंमा एक उपलब्धि हो।

यस हातेपुस्तिकाले प्रदेश र स्थानीय सरकारको सञ्चालन प्रणालीमा बहुआयामिक योगदान पुर्‍याउने अपेक्षा गरिएको छ। यसले प्रदेश तथा स्थानीय तहका सम्पूर्ण सरकारी कार्यालयहरूमा प्रयोग हुने सूचना प्रविधिका नवीन अवधारणाहरू, अन्तर्राष्ट्रिय मानकहरू र खरिद प्रक्रियाहरूलाई व्यवस्थित र प्रणालीकरण गर्न मार्गनिर्देश गर्नेछ। हातेपुस्तिकामा समावेश गरिएका दैनिक, साप्ताहिक एवं मासिक चेकलिस्ट र प्राविधिक मार्गदर्शनहरूले यसअघि सूचना प्रविधि प्रणालीको विकास, सञ्चालन, साइबर सुरक्षा र खरिदका क्षेत्रमा रहँदै आएका प्राविधिक अन्योल र असंगतिहरूलाई अन्त्य गरी कार्यप्रक्रियामा एकरूपता ल्याउने विश्वास गरेको छु। गण्डकी प्रदेश सरकारको सुशासनप्रतिको प्रतिबद्धतालाई व्यवहारमा उतार्न यो हातेपुस्तिका एक बलियो प्राविधिक खम्बा साबित हुनेछ।

हाम्रो लक्ष्य प्रविधिमैत्री, जनउत्तरदायी, सक्षम र सुशासित स्थानीय तथा प्रदेश सरकार निर्माण गर्नु हो। यस पुस्तकमा समाविष्ट डिजिटल सेवा प्रवाह, डाटा सुरक्षाका सिद्धान्त र डिजिटल सार्वजनिक पूर्वाधारसँगको एकीकरण सम्बन्धी मार्गदर्शनले जनताको घरदैलोमा छिटो, छरितो र सुरक्षित प्रविधिमा आधारित सेवा पुर्‍याउन महत्वपूर्ण भूमिका खेल्नेछ। अन्त्यमा, यस हातेपुस्तिका तयार गर्न मुख्यमन्त्री तथा मन्त्रिपरिषद्को कार्यालय अन्तर्गत संचालित प्रदेश तथा स्थानीय शासन सवलीकरण कार्यक्रम, परामर्शदाताका विज्ञ समूह तथा यस कार्यमा प्रत्यक्ष एवं परोक्ष रूपमा योगदान दिनु हुने सम्पूर्ण राष्ट्रसेवक कर्मचारी एवं सरोकारवालाहरूलाई हार्दिक धन्यवाद ज्ञापन गर्दछु। यस हातेपुस्तिकाको पूर्ण कार्यान्वयनले गण्डकी प्रदेशलाई 'डिजिटल सुशासन' को मार्गमा अग्रणी बनाउने विश्वासका साथ सफलताको शुभकामना व्यक्त गर्दछु।

(सुरेन्द्रराज पाण्डे)
मुख्यमन्त्री

शुभकामना

विश्वमा पछिल्लो शासकीय प्रवन्ध र सुशासन अन्तरगत विद्युतीय सुशासन (Digital Governance) लाई प्रमुख विशेषताको रुपमा लिईन्छ। नेपाल सरकार तथा प्रदेश सरकारले समेत आम नागरिकको हितका लागि 'डिजिटल सुशासन' को दूरगामी दृष्टिकोण अघि सारेका छन्। सोहि सन्दर्भमा प्रदेश तथा स्थानीय तहको शासन प्रणाली र क्षमता सुदृढ गर्दै नागरिकलाई सङ्घीयताको लाभ, प्रभावकारी सेवा र विकासको प्रतिफल सुनिश्चित गर्न गण्डकी **प्रदेशमा प्रदेश तथा स्थानीय शासन सवलीकरण कार्यक्र**म (PLGSP) कार्यान्यनमा रहेको छ। यस कार्यक्रमको प्रतिफल ४ ले राष्ट्रसेवक कर्मचारीहरु सुशासन प्रत्याभूति गर्न र समावेशी सेवा प्रवाह प्रवाह गर्न सक्षम हुनेछन बह्न्ने ध्येय बमोजिम प्राविधिक जनशक्तिको क्षमता विकासका लागि प्राविधिक हातेपुस्तिकाको प्रकाशन गरिएको छ। सूचना प्रविधि कार्य सञ्चालनको क्षमता, पारदर्शीता र समग्र डिजिटल सेवा वितरणको गुणस्तरमा रूपान्तरण ल्याउन यो हातेपुस्तिका एक कोसेढुङ्गा साबित हुनेछ।

नेपालकै प्रशासनिक इतिहासमा प्रदेश सरकारको तर्फबाट स्थानीय र प्रादेशिक तहका सूचना प्रविधि क्षेत्रलाई व्यवस्थित गर्न तयार पारिएको सम्भवत यो पहिलो 'paradigm shift' हो। सूचना प्रविधि क्षेत्र अझै पनि नेपालमा विकासोन्मुख चरणमै रहेको र सबै आवश्यक नियामक तथा मानक ढाँचाहरू पूर्ण रूपमा परिपक्व भइनसकेको पृष्ठभुमि/यथार्थलाई आत्मसात् गर्दै यो हातेपुस्तिका तयार गरिएको छ। यस पुस्तिका लाई उच्च-स्तरीय अवधारणा र अन्तर्राष्ट्रिय उत्तम अभ्यासहरूदेखि नेपालको राष्ट्रिय कानुनी ढाँचा र दैनिक कार्य सञ्चालन, खरिद, एवं प्रणाली विकाससम्मका व्यावहारिक मोडलहरू समेटेर सातवटा परिपूरक मोड्युलहरूमा विभाजन गरिएको छ। सूचना प्रविधिको क्षेत्रमा आउने तीव्र उतारचढाव, परिवर्तन व्यवस्थापन र बदलिँदो प्राविधिक परिवेश तथा हाल सम्मको अनुभवको आधारमा समयसापेक्ष रूपमा निरन्तर परिमार्जन र अद्यावधिक गर्दै हातेपुस्तिकालाई जीवन्त दस्तावेजको रुपमा विकास गरिएको छ ।

यस हातेपुस्तिकाको तत्कालीन प्रतिफलका रूपमा प्रदेश र स्थानीय तहमा कार्यरत सूचना प्रविधि जनशक्तिको क्षमता सुदृढ भई दैनिक कार्य सञ्चालन तथा सेवा प्रवाह, खरिद प्रक्रिया र प्रणाली विकासमा सहजता एवं कार्यदक्षता हासिल हुनेछ। यसले प्राविधिकहरूले भोग्दै आएका सीमित विशेषज्ञता र फराकिलो कार्यबोझका चुनौतीहरूलाई सम्बोधन गर्दै तदर्थ निर्णय लिने परिपाटी र खरिदका अनियमितता जोखिमहरूलाई अन्त्य गर्नेछ। अन्ततः, यस प्रयासको अन्तिम प्रतिफलका रूपमा आम नागरिकले आधुनिक, भरपर्दो, छिटो, छरितो र झन्झटरहित नागरिक-केन्द्रित डिजिटल सेवा प्राप्त गर्नेछन्।

यस प्रकाशनका लागि महत्वपूर्ण शुभकामना मन्तव्य तथा नियमित मार्गनिर्देशनका लागि माननीय मुख्यमन्त्री एवं प्रादेशिक निर्देशक समितिको अधक्ष्य **सुरेन्द्रराज पाण्डे**ज्यू प्रति विशेष धन्यवाद र आभार प्रकट गर्दछु र प्रशासनिक नेतृत्वको भूमिकामा रहेर यस कार्य लाई सफल बनाउन निरन्तर घचघच्याइरहने श्रीमान प्रमुख सचिव श्री भूपाल बरालज्यू र व्यवस्थापकीय समन्वय गर्नुहुने सचिव श्री ऋषिराज आचार्यज्यू प्रति आभार प्रकट गर्दछु। साथै, यस पुस्तकको तयारी प्रक्रियामा निरन्तर प्राविधिक दिशानिर्देशन प्रदान गर्ने प्रादेशिक निर्देशन समिति तथा निरन्तर खटेर कार्य गर्ने मुख्यमन्त्री तथा मन्त्रिपरिषद्को कार्यालय एवं प्रदेश तथा स्थानीय शासन सवलीकरण कार्यक्रमको प्रदेश कार्यक्रम व्यवस्थापक श्री पार्वती लामिछाने र सम्पूर्ण टोलीलाई विशेष धन्यवाद दिन चाहन्छु । अन्तमा: गण्डकी प्रदेश र अन्तरगतका सम्पूर्ण स्थानीय तहका प्राविधिक कर्मचारीहरुले यस हातेपुस्तिकालाई आफ्नो दैनिक कार्यको श्रोत पुस्तिकाको रुपमा पूर्ण रुपमा उपयोग गरि प्रदेशको डिजिटल रुपान्तरण अभियानलाई सफल बनाउनुहुनेछ भन्नेमा पूर्ण विश्वस्त छु।

(कृष्णप्रसाद लम्साल)
सचिव

How to Use This Handbook
यो हातेपुस्तिका कसरी प्रयोग गर्ने

If you are...	Start here	Most useful modules
A newly appointed IT Official	Module 1 (Foundational Concepts) → Module 8 Annex 8.2 (QRC-1 and QRC-2)	Modules 1, 2, 4, 8
An IT Official managing daily operations	Module 4, Section 4.4 (F 4.9 Combined Operations Checklist) and Section 4.2 (F 4.3 Incident Log)	Modules 4, 8
An IT Official initiating any procurement	Module 5, Section 5.2 (Thresholds) → Section 5.3 (TCN) → Section 5.5 (Procurement Process SOP)	Modules 3, 5, 8
An IT Official overseeing a software project	Module 6, Section 6.1 (Sign-Off Gates) → Section 6.2 (GEA 2.0 Artifacts)	Modules 3, 5, 6, 7
An IT Official requesting a government ICT service	Module 7 — find the organization, then the service in the summary table, then how to submit	Module 7
An IT Official or designated authority preparing for audit	Module 8, Annex 8.1 (Master Tools Cross-Reference) → verify all relevant tools are complete	Module 8, then referenced modules
A designated authority approving ICT decisions	Module 2 (Standards overview), Module 3 (Legal obligations), Module 4 Section 4.1 (IT Governance)	Modules 2, 3, 4
A Procurement Officer preparing bids	Module 5 (all sections) → Module 3 Sections 3.3.5 (GEA 2.0) and 3.3.6 (IT Norms 2082)	Modules 3, 5

Quick reference cards (QRC-1 to QRC-6): Print the six laminated cards from Module 8 Annex 8.2 on A5 cardstock. Post QRC-1 and QRC-2 at the IT Official workstation. Post QRC-6 (Emergency Contacts) in the server room and with the designated authority. The cards cover: Server Room Daily Checklist · Incident Triage · Procurement Quick Reference · Password and 2FA Policy · Backup and DR · Emergency Contacts.

Callout box colours

Box	Meaning (same colour in every module)
IMPORTANT (⚠️)	Mandatory action or a common CIAA/OAG audit finding — do not skip
Note / See Also (📌)	Helpful context, or a pointer to related detail elsewhere in the handbook
Cross-Reference (🔗)	A related tool, form, or section located in another module
Legal Basis (⚖️)	The specific Act, Regulation, or Directive that requires this step

Table of Contents

MODULE 1 FOUNDATIONAL CONCEPTS

Service Delivery	Digital Governance	Inclusive Design	AI in Government

Module 1 establishes the foundational conceptual framework for all subsequent modules of this handbook. Before implementing security controls, managing procurements, or developing software systems, every ICT official must understand why ICT service delivery matters in Nepal's federal context, what principles should guide it, how it must be inclusive of all citizens, and how technologies can and should be deployed responsibly. This module provides foundation.

Three Layers of Digital Government

1. Governance and Standards
2. Secure Digital Systems
3. Citizen Services

1.1 ICT Service Delivery / ICT सेवा प्रवाह

ICT Service Delivery encompasses the complete lifecycle of aligning, designing, building, delivering, and continuously improving technology solutions to co-create value for citizens and government staff. It is not merely about deploying technology — it is about ensuring that technology investments translate into measurable improvements in the quality, accessibility, and efficiency of public services.

A core principle of Nepal's digital governance strategy — expressed in GEA 2.0 and the Digital Nepal Framework 2.0 — is the vision of a 'connected government': a digital ecosystem in which federal, provincial, and local government systems share data seamlessly, avoid duplication, and collectively deliver better services to citizens.

In Nepal's federal structure, provincial and local governments have constitutional responsibility to deliver services under Schedules 8 and 9 of the Constitution of Nepal 2015. ICT is the primary enabler for meeting these obligations at scale, with speed, and with transparency.

ICT Service Delivery — 7 Key Stages / ICT सेवा प्रवाहका ७ मुख्य चरणहरू

Stage / चरण	What Government Does / सरकारले के गर्छ	Module Reference
1. Identify Need आवश्यकता पहिचान	Identify citizen service gap or operational inefficiency. Align with Annual Work Plan. Document need in Annual ICT Procurement Plan (M5-T01).	Module 5
2. Plan and Align योजना र संरेखण	Prepare Technical Concept Note (TCN). Align with GEA 2.0, DNF 2.0, IT Norms 2082. Obtain designated authority approval before any procurement.	Module 5
3. Design डिजाइन	Design system: GEA 2.0 REST/JSON APIs, GIDC hosting, NID integration, WCAG accessibility, Privacy-by-Design from the start.	Module 6
4. Procure / Build खरिद / निर्माण	PPA-compliant procurement with anti-corruption templates, IT Norms cost estimation, and brand-neutral specifications.	Module 5
5. Test and Accept परीक्षण र स्वीकृति	Government-conducted UAT with actual users (not developer only). NCSC VAPT security clearance. designated authority go-live authorization.	Module 6
6. Operate and Support सञ्चालन र समर्थन	Service Desk: incident management, monthly SLA monitoring, regular security patches, and backup verification.	Module 4
7. Improve सुधार	Measure citizen outcomes and KPIs. Collect user feedback. Report to IT Steering Committee. Plan next improvement cycle.	Modules 4, 5

See Also (📌):

Detailed operational procedures for each stage: Module 4 (Operations), Module 5 (Procurement), Module 6 (System Development). Legal framework: Module 3.

1.2 Key Conceptual Distinctions / मुख्य अवधारणागत भिन्नताहरू

To prevent systemic misconceptions that result in deficient technical architectures and misaligned strategic objectives, it is imperative that ICT officials thoroughly comprehend three foundational conceptual distinctions. Ensuring absolute clarity on these core principles is essential for the seamless design, robust deployment, and strategic alignment of all public sector information systems.

1.2.1 Digitization vs. Digitalization vs. Digital Transformation डिजिटाइजेसन, डिजिटलाइजेसन र डिजिटल रूपान्तरण

Concept	नेपाली	Definition / परिभाषा	Example in Gandaki Province LG
Digitization (Narrowest)	डिजिटाइजेसन	Converting analog/paper-based records into digital format. The CONTENT changes from paper to digital, but the PROCESS stays the same.	Scanning paper birth certificates into PDF files. The citizen still visits the counter; the record is now digital.

Concept	नेपाली	Definition / परिभाषा	Example in Gandaki Province LG
Digitalization	डिजिटलाइजेसन	Using digital technology to CHANGE HOW a process works. The process itself is redesigned to use digital tools — making it faster, more efficient, or more accessible.	Online birth certificate application: citizens submit the form digitally, staff process it in a digital workflow. The process is now digital, not just the record.
Digital Transformation (Broadest)	डिजिटल रूपान्तरण	Comprehensive rethinking of HOW government delivers value using digital technology. Redesigns entire service ecosystems around citizen needs — proactive, integrated, and data-driven.	Nagarik App : citizen completes all life-event services (birth, marriage, property, tax) through one integrated platform. Government proactively notifies citizens; data flows between agencies without manual transfer.

Note (📌):

Where are the Province LGs now?

Most are at the Digitization stage (scanning documents) or beginning Digitalization (some online forms). The target under Digital Nepal Framework 2.0 is Digital Transformation — where citizens experience seamless, proactive, integrated public services. Each module in this handbook helps LGs progress along this continuum.

1.2.2 IMS vs MIS / IMS र MIS बीचको भिन्नता

In public sector administration, a frequent source of technical over-expenditure and operational failure is the mischaracterization of an Information Management System (IMS) as a Management Information System (MIS), or vice versa. To establish robust government systems, ICT officials must carefully differentiate these two architectures based on their objective, analytical depth, and ultimate purpose.

IMS सूचना व्यवस्थापन प्रणाली	MIS व्यवस्थापन सूचना प्रणाली
Information Management System — a broad term for any system that captures, stores, manages, and retrieves information within an organization. IMS is the general category that includes all government databases, document management systems, civil registration systems, etc.	Management Information System — a specific type of IMS designed to generate structured reports and dashboards for management decision-making. MIS converts raw operational data into summarized information (budget reports, service statistics, staff performance) for decision makers and senior officials.
Key distinction: IMS is the container of data; MIS is what extracts intelligence from that data for management decisions. GIOMS is an IMS; the municipal budget dashboard is part of a MIS.	
Directive for ICT Officials: Prior to the ratification of any System Requirements Specification (SRS), procuring entities must explicitly audit whether the business requirement dictates a digital archive (IMS) or a decision-support platform (MIS). Systems must be procured based on this analytical baseline to avoid the "illusion of progress" where paper forms are merely transcribed into static computer records without altering administrative outcomes.	

1.2.3 e-Governance vs Digital Governance / ई-गभर्नेन्स र डिजिटल गभर्नेन्स

e-Governance ई-गभर्नेन्स	Digital Governance डिजिटल गभर्नेन्स
Electronic delivery of existing government services using ICT. The PRIMARY goal is EFFICIENCY — doing the same things faster and cheaper. The fundamental structure of government and service delivery remains unchanged. e-Governance automates what exists. Example: Online tax payment form that replaces a paper form at the counter.	Comprehensive transformation of how the government WORKS using digital technology. The PRIMARY goal is CITIZEN VALUE — redesigning services and government itself around citizen needs. Breaks down silos. Makes government data-driven, proactive, and participatory. Digital Governance reimagines what the government does. Example: Proactive tax system that automatically calculates citizen tax, sends reminders, accepts payment from multiple channels, and issues receipts — without citizens visiting any office.
Key distinction: e-Governance is a stepping stone To Digital Governance. Nepal's Digital Nepal Framework 2.0 sets Digital Governance as the destination.	

1.3 Inclusive and Citizen-Centred Service Design / समावेशी र नागरिक-केन्द्रित सेवा डिजाइन

In alignment with the constitutional guarantees of the state, public sector technical frameworks must undergo a strategic shift from administrative convenience to citizen-centric architectures. The Article 18 of Constitution of Nepal guarantees equal access to state services for all citizens. In the digital governance domain, inclusive, barrier-free design is not merely a technical preference; it is the primary mechanism through which Information and Communication Technology (ICT) fulfills this constitutional obligation.

To operationalize this mandate, government information systems must be engineered around the explicit needs of the end-user rather than the structural conveniences of the implementing agency.

Design Principle / डिजाइन सिद्धान्त	What it means for LG IT Officials	Standard
Citizen-Centred नागरिक-केन्द्रित	Design around citizen needs, not internal processes. Before procurement, consult the citizens the service will serve. Measure success by citizen satisfaction, not system uptime alone.	Good Governance Act 2064
Accessible to All सबैका लागि सुलभ	All web portals: WCAG 2.1 Level AA minimum. Mobile-first design for smartphone users. Nepali as primary language. Audio/visual guidance for low-literacy users. Ward-level assisted access for those who cannot self-serve digitally.	WCAG 2.1; DNF 2.0
Inclusive by Default पूर्वनिर्धारित समावेशिता	Test with persons with disabilities, elderly and remote ward citizens before go-live — not only with office staff. Services must reach ALL citizens, not just the digitally connected.	Constitution 2015, Article 18
Multi-Channel Delivery बहु-माध्यम सेवा प्रवाह	Maintain physical service channels alongside digital. Citizens who cannot access digital services must still receive them at the counter. Digital should add options, not reduce access.	IT Policy 2015

Design Principle / डिजाइन सिद्धान्त	What it means for LG IT Officials	Standard
Simple Language सरल भाषा	All citizen-facing content in clear, plain Nepali. No bureaucratic jargon. Icons and images to supplement text for low-literacy users.	Good Governance Act 2064

Complete before publishing any citizen-facing digital service.

F 1.1 | Inclusive ICT Service Delivery Assessment Checklist — complete before any new digital service is procured or deployed	
Check	Status
Multiple access channels offered (not smartphone/internet-only) — counter, IVR/SMS, or agent-assisted option retained	[ ] Yes [ ] No
Interface defaults to Nepali with plain-language labels and instructions	[ ] Yes [ ] No
WCAG 2.1 Level AA accessibility verified (screen-reader compatible, no colour-only cues, keyboard navigable)	[ ] Yes [ ] No
Tested with users of varying digital literacy, gender, and disability status before go-live	[ ] Yes [ ] No
Low-bandwidth fallback available (usable on 2G/3G, lightweight pages)	[ ] Yes [ ] No
Only the minimum personal data needed for the service is collected (data minimization)	[ ] Yes [ ] No

See Also (📌):
Inclusive ICT Service Delivery Assessment Checklist (F 1.1): use before any new digital service procurement to verify all five principles are addressed. Full checklist provided above.

1.4 Digital One-Stop Service Delivery / एकद्वार सेवा प्रवाह

Digital One-Stop Service Delivery is shifting the focus from government convenience to the end-user's needs. A citizen can access multiple government services from a single platform without needing to know which office or department handles each service. The goal is 'No Wrong Door' — however a citizen enters, they reach the right service. One-Stop Service Delivery (OSSD) framework replaces manual "file shifting" with standardized, automated workflows. This citizen-centric approach radically simplifies processes, ensures universal accessibility for vulnerable demographics, and optimizes transaction velocity—reducing citizen wait time

Dimension	Traditional Governance / Status Quo	Citizen-Centric Design / OSSD Framework
Service Architecture	**Government-Centric Convenience:** Fragmented "multi-desk" workflows requiring citizens to physically visit multiple administrative rooms and offices.	**Citizen-Centric Accessibility:** Integrated One-Stop Service Delivery (OSSD) hubs where all administrative transactions occur at a single physical desk or unified digital platform.
System Flow & Design	**"File Shifting" Culture:** Rigid, manual, and paper-based tracking that maximizes wait times and limits procedural transparency.	**Algorithmic Simplification:** Standardized Operating Procedures (SOPs) and digital tracking engines that accelerate transactional velocity.

Inclusivity & UX	Barrier-heavy interfaces that neglect vulnerable demographics like senior citizens, women, and individuals with disabilities.	**Inclusive Design:** Proactive integration of universal accessibility tools, digital feedback walls, and dedicated assistance mechanisms.

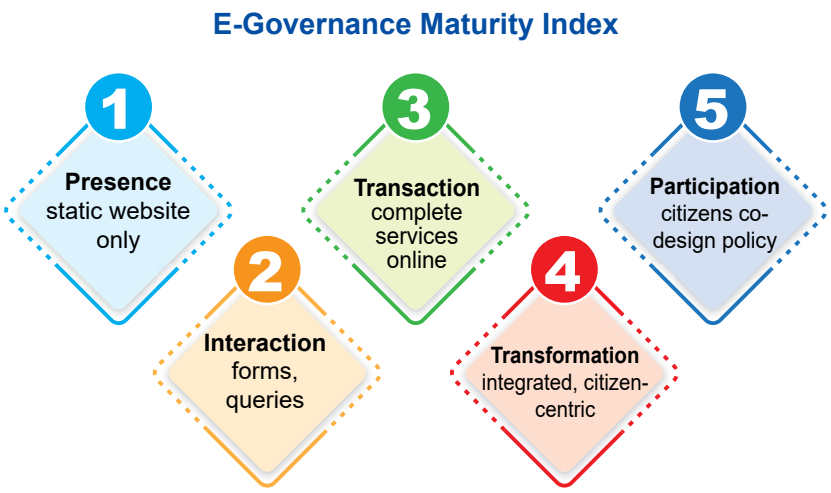
The Digital Nepal Framework 2.0 sets the national target: every citizen should be able to access all government services digitally by 2085 BS, using a single National ID (NID) for authentication across all services. Government Offices are expected to integrate their services with NID and Nagarik App as a primary action under DNF 2.0.

Complete monthly, and before granting any vendor access to citizen data.

F 1.2 | Data Protection Quick Reference Card — monthly review; also complete at every vendor onboarding	
Check	Status
Lawful, documented purpose exists for every category of personal data collected	[ ] Yes [ ] No
Data minimization applied — no fields collected beyond what the service needs	[ ] Yes [ ] No
Citizens given notice (in Nepali, plain language) of what is collected and why	[ ] Yes [ ] No
Personal data encrypted at rest and in transit	[ ] Yes [ ] No
Data retention period defined and enforced; data purged after expiry	[ ] Yes [ ] No
Any vendor/processor with data access has signed an NDA (M5-T16) and data-protection clause	[ ] Yes [ ] No

1.5 E-Governance Maturity Index / ई-गभर्नेन्स परिपक्वता सूचकांक

The E-Governance Maturity Index is a framework for assessing how advanced a government's use of ICT is for service delivery. It describes a progression from basic information presence to full digital transformation. Understanding where Province and LGs currently stand — and where the national and provincial targets require them to go — is essential for planning ICT investments.



Stage / चरण	Name, Description, and Gandaki Province LG Application
1	**Presence / उपस्थिति** / The government has a website with static information — office hours, contact details, downloadable forms. No online transaction capability.
2	**Interaction / अन्तरक्रिया** / **◄ Gandaki LGs now** Citizens can submit queries by email or online form. The government responds. Downloadable forms available. Basic two-way communication but no complete online transactions.
3	**Transaction / कारोबार** / Citizens can complete entire service transactions online — apply, pay, receive certificate — without visiting the office. All citizen-facing services available digitally end-to-end.
4	**Transformation / रूपान्तरण** / **► Target 2085 BS** All government services are integrated across agencies. Single-window (Nagarik App / portal) access. Citizens use **Digital Public Infrastructure (DPI)** like NID for authentication and ConnectIPS for payments. Data flows automatically between agencies via secure data exchange platforms
5	**Participation / सहभागिता** / Citizens actively co-design policies and services. Open government data. Participatory budgeting. Real-time feedback loops between government and citizens.

Note (📌):

Current status of Provincial and Local government Offices: Most LGs are at Stage 2 — basic websites (.gov.np via GIWMS) and limited online forms. A few leading municipalities are beginning Stage 3 with online tax payment and permit applications. The target under Digital Nepal Framework 2.0 is Stage 4 by 2085 BS — integrated services via Nagarik App with NID authentication. Nepal's overall UN EGDI ranking has improved but remains below the global average. Each step a Provincial and Local government Office takes toward Stage 3–4 directly contributes to Nepal's national digital governance targets.

The Role of DPI and DPG in Reaching Digital Maturity To successfully progress from Stage 2 (Interaction) to Stage 4 (Transformation), local governments must leverage foundational digital assets rather than building isolated systems from scratch :

- **Digital Public Infrastructure (DPI) / डिजिटल सार्वजनिक पूर्वाधार:** The core, shared digital systems that enable basic public services across all sectors. In Nepal, the primary DPIs include the National Identity (NID) system for authentication, national digital payment gateways (like ConnectIPS), and the secure Data Exchange Platform. LG systems must integrate with these DPIs rather than creating redundant local IDs or payment portals.
- **Digital Public Goods (DPG) / डिजिटल सार्वजनिक वस्तु:** Open-source software, data models, standards, and building blocks that can be freely used and adapted. The e-Governance Blueprint 2082 mandates the creation of a "building blocks repository" (सफ्टवेयर निर्माणका विकास ब्लक रिपोजिटरी) so LGs can reuse standardized code for common services rather than paying vendors to build them repeated

1.6 Artificial Intelligence and Machine Learning in Government ICT / सरकारी ICT मा कृत्रिम बुद्धिमत्ता र मेसिन लर्निङ

The National AI Policy 2025 establishes clear obligations for government bodies adopting AI. Every AI application used in government service delivery must be: explainable (citizens can understand how decisions affecting them are made); auditable (AI decisions can be reviewed by authorized personnel); non-discriminatory (tested for bias before deployment and monitored for bias in operation); and accountable (human officials remain responsible for decisions made with AI assistance).

AI Application / AI प्रयोग	Practical Benefit for LG	Key Requirement Before Use
Citizen Query Chatbot (नागरिक प्रश्न च्याटबोट)	Automated 24/7 responses to common citizen questions about service fees, office hours, required documents, permit status. Reduces counter queue.	Clean, updated knowledge base in Nepali. Human escalation path for complex queries. Test for accuracy before go-live.
Revenue and Tax Analytics (राजस्व विश्लेषण)	ML analysis of tax payment patterns to identify arrears, forecast revenue, and target reminder campaigns.	Bias testing on historical data. Human review of all model outputs before action. Privacy Act 2075 compliance.
Document Completeness Check (कागजात पूर्णता जाँच)	Automated preliminary verification of submitted application documents for completeness before human review.	Thorough testing. Clear appeal mechanism. Avoid storing documents beyond stated purpose.
Infrastructure Prediction (पूर्वाधार पूर्वानुमान)	ML analysis of maintenance records to predict infrastructure failures before they occur.	Sufficient historical data. Human engineer reviews all predictions before scheduling maintenance.

Complete before procuring or deploying any AI/ML capability; designated authority sign-off required.

F 1.3 | AI/ML Adoption Readiness Checklist — complete before any AI or ML system is procured or deployed	
Check	**Status**
Documented use case exists with a clear, specific public benefit (not speculative)	[ ] Yes [ ] No
Legal basis under the National AI Policy 2025 confirmed and recorded	[ ] Yes [ ] No
No fully automated decision-making on matters affecting a citizen's rights or entitlements without human review	[ ] Yes [ ] No
Bias/fairness check completed for any citizen-facing AI use	[ ] Yes [ ] No
Training/operating data complies with the Privacy Act 2075 (Module 3, Section 3.3.2)	[ ] Yes [ ] No
Vendor contract includes explainability, audit-log, and data-residency requirements	[ ] Yes [ ] No
Designated authority sign-off obtained before procurement or deployment	[ ] Yes [ ] No — STOP

Before any AI system is procured or deployed: complete the AI/ML Adoption Readiness Checklist (F 1.3) and obtain authority sign-off. Ensure: documented use case; legal basis for citizen data use; bias testing; human oversight mechanism; explainability to citizens. AI must never be the sole decision-maker in government processes affecting citizen rights.

See Also (📌):

AI Readiness Checklist (F 1.3) : full checklist provided above in this section. AI Policy legal requirements: Module 3 Section 3.3.10.

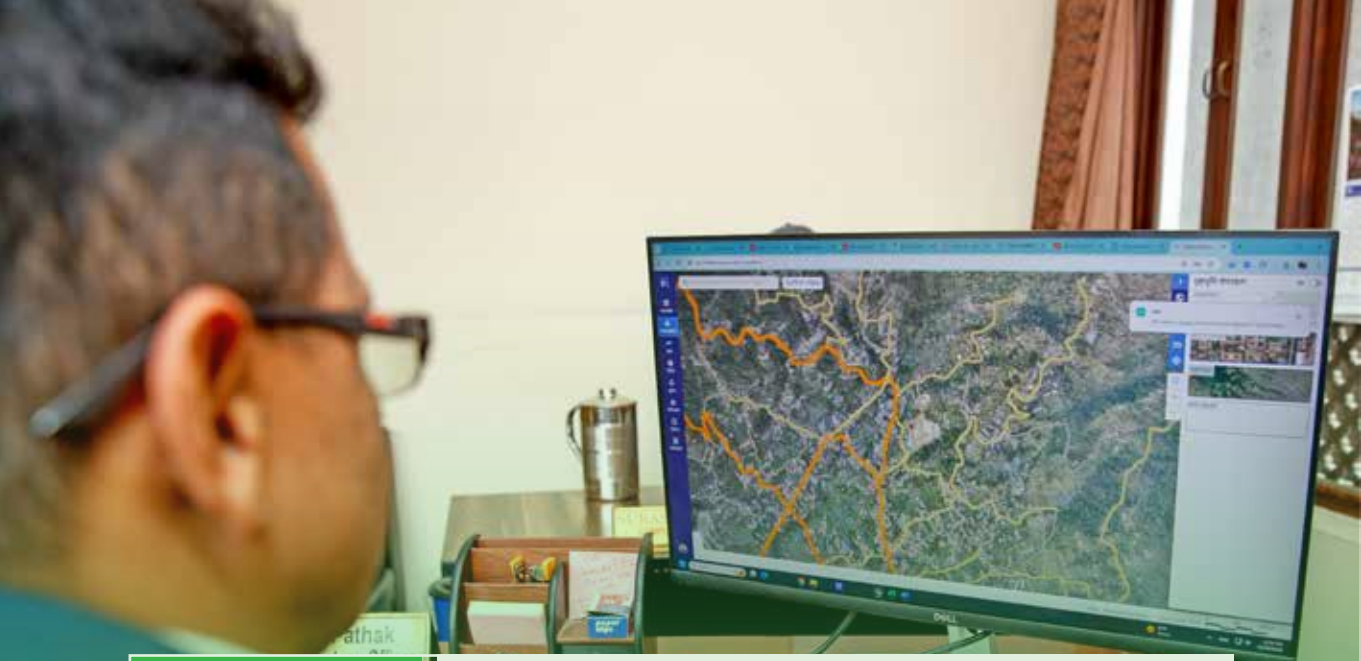
1.7 Data Protection Basics / डेटा संरक्षणका आधारभूत कुराहरू

Protecting citizen data is both a legal obligation and a cornerstone of public trust. Every local and provincial government office that delivers digital services collects, processes, and stores citizen personal information — including names, NID numbers, addresses, family details, land records, tax data, and financial information. A data breach in any of these systems can cause direct citizen harm, legal liability under the Privacy Act 2075, and lasting damage to public trust in digital government.

ISO/IEC 27001:2022 (covered in detail in Module 2, Section 2.5) provides the international framework for implementing an Information Security Management System (ISMS). This module provides the foundational data protection concepts; Module 4 provides the operational security procedures; and Module 3 provides the detailed legal compliance requirements.

Core Data Protection Principles

Principle	Definition	Practical Implication for ICT Officials
Lawfulness and Purpose Limitation	Data may only be collected for a specific, documented, lawful purpose — and may not be used for any other purpose without separate consent or legal basis.	Document the purpose of every data collection activity. Civil registration data may not be repurposed for voter list compilation without a separate legal basis.
Data Minimization	Only the minimum personal data necessary for the stated purpose should be collected. Collecting data 'just in case' is not permitted.	Review all citizen data collection forms. Remove any fields that are not strictly necessary for the service being delivered.
Accuracy	Personal data must be accurate, kept up to date, and corrected when errors are identified.	Implement data correction mechanisms in citizen portals. Provide citizens with a way to flag and request correction of their records.
Storage Limitation	Personal data must not be retained longer than necessary for its stated purpose.	Implement and enforce a data retention policy. Securely delete data that has exceeded its retention period.
Security (Integrity and Confidentiality)	Personal data must be protected against unauthorized access, alteration, disclosure, or destruction.	Implement encryption at rest and in transit. Apply least-privilege access controls. Maintain audit logs. Conduct VAPT before go-live.
Accountability	The organization collecting data is responsible for demonstrating compliance with data protection principles.	Maintain a data inventory. Complete Privacy Act compliance checklist (Module 3, F 3.2). Designate data protection responsibilities to the IT Official.

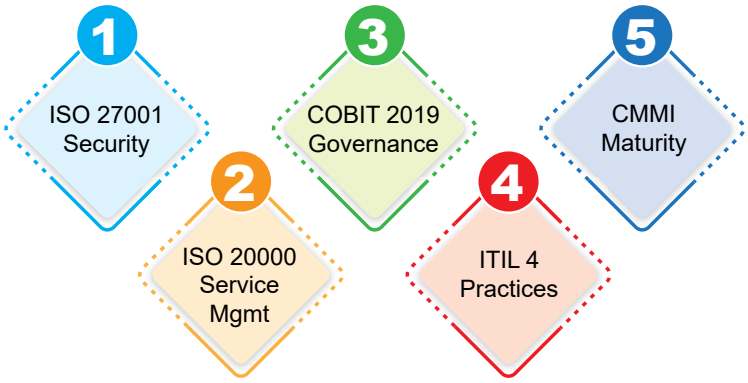


MODULE 2 INTERNATIONAL STANDARDS AND BEST PRACTICES

ISO 27001	ISO 20000	COBIT 2019	ITIL 4	CMMI

This module provides ICT officials with a practical, implementation-oriented introduction to the five internationally recognized standards and frameworks that underpin the entire ICT Technical Handbook. Understanding these frameworks is not merely an academic exercise — it is a prerequisite for conducting compliant, efficient, and accountable ICT operations. Each standard described here is directly linked to the operational guidance in Modules 3 through 7.

Five International Frameworks



2.1 Five Frameworks — At a Glance / पाँच ढाँचाहरू — संक्षिप्त परिचय

These five internationally recognized frameworks provide the professional foundations for ICT governance. They are not independent — they complement each other. IT officials do not need to implement all five at once: start with ISO 27001 (security) and ITIL 4 (service management) as the highest-priority foundations, then build toward the others over 2-3 years.

Framework	Purpose / उद्देश्य	Primary Benefit for LG	Nepal Policy Link	Priority
ISO 27001:2022 (ISMS)	Information Security Management System — framework for protecting government ICT systems and citizen data against threats.	Structured, auditable security — reduces breach risk; demonstrates compliance to OAG and NCSC.	National Cybersecurity Policy 2080; Privacy Act 2075	★★★★★ Start here
ISO 20000-1:2018 (ITSM)	IT Service Management — framework for consistently delivering high-quality ICT services aligned with citizen needs.	Defines what constitutes a managed IT service; supports SLA management with vendors.	GEA 2.0 service delivery; Good Governance Act 2064	★★★★☆ High
COBIT 2019 (IT Governance)	IT Governance framework separating governance (designated authority/ Steering Committee) from management (IT Official).	Clarifies who decides, who advises, and who executes — prevents governance confusion.	Good Governance Act 2064; LGOA 2074	★★★☆☆ Medium
ITIL 4 (Service Value System)	IT Infrastructure Library — best practices for IT Service Management across the service value chain.	Gives IT Officials structured approaches to incident management, change control, and continuous improvement.	GEA 2.0 service value chain; ITIL 4 practices align with Module 4 SOPs	★★★★☆ High
CMMI V2.0 (Process Maturity)	Capability Maturity Model — 5-level maturity framework assessing and improving ICT process capability.	Provides a roadmap for improving ICT processes over time; supports structured self-assessment.	Digital Nepal Framework 2.0 digital transformation stages	★★★☆☆ Medium-term

Note (📌): Practical approach for resource-constrained Offices: Year 1 — Implement ISO 27001 baseline security controls + ITIL 4 incident/change management. Year 2 — Add ISO 20000 service management formalization + COBIT governance structure. Year 3+ — Progress CMMI maturity levels and advanced ITIL practices. Each subsequent section follows this priority order.

2.2 ISO/IEC 27001:2022–Information Security Management / सूचना सुरक्षा व्यवस्थापन

2.2 | ISO/IEC 27001:2022 (22)

सूचना सुरक्षा व्यवस्थापन प्रणाली (ISMS) | International Organization for Standardization

Focus: ISO 27001 is the international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) — a structured, risk-based approach to protecting government information assets and citizen data from security threats.

Key Components / मुख्य अवयवहरु	Nepal/LG Government Adaptation
◆ **ISMS Scope:** Define which systems, data, people, and processes are covered by the security management system. ◆ **Risk Assessment:** Identify threats (unauthorized access, ransomware, insider threats) and vulnerabilities; assess impact and likelihood; prioritize controls. ◆ **Annex A Controls:** 93 security controls in four categories: Organizational (policies), People (training, HR security), Physical (server room, access), Technological (encryption, patching, logging). ◆ **Statement of Applicability:** Document which of the 93 controls are applied and why — the formal compliance record for CIAA Investigation readiness. ◆ **PDCA Cycle:** Plan-Do-Check-Act: set objectives → implement controls → audit effectiveness → improve. Continuous cycle, not a one-time project. ◆ **Internal Audit:** Annual internal review of ISMS effectiveness by IT Official and designated authority; followed by management review for continuous improvement.	→ Security is mandatory by law. Privacy Act 2075 and ETA 2063 require government bodies to protect citizen data. ISO 27001 is the recognized framework for demonstrating this compliance to OAG and NCSC. → Start with the basics. Gandaki Province LGs do not need full ISO 27001 certification immediately. Start with: defined ISMS scope, documented risk register, implemented access controls, incident reporting procedure, and annual review. Module 4 (Section 4.7) contains the operational implementation. → NCSC alignment. ISO 27001 controls align with the National Cybersecurity Policy 2080 requirements. Applying ISO 27001 baseline controls directly supports NCSC VAPT readiness (Module 7, Section 7.3). → Key priority controls for LG IT Officials: Least privilege access (F 4.12), 2FA for admin accounts, encryption at rest and in transit, audit logging, patch management (F 4.13), VAPT before go-live (Module 4, Section 4.8).

Quick Self-Check / द्रुत आत्म-मूल्याङ्कन (Complete annually or when implementing this standard)	
Check Item	**Status**
Is an ISMS scope document defined and approved by the designated authority?	[ ] Yes [ ] No [ ] Partial
Has a risk assessment identified the top 5 information security threats to your office's ICT systems and citizen data?	[ ] Yes [ ] No [ ] Partial
Are the 8 Annex A baseline controls implemented: access control, encryption, patching, logging, physical security, incident management, backup, and staff awareness training?	[ ] Yes [ ] No [ ] Partial
Is there a documented procedure for reporting security incidents to the IT Official, designated authority, and NCSC within required timelines?	[ ] Yes [ ] No [ ] Partial
Has an internal ISMS review been conducted in the last 12 months and findings documented?	[ ] Yes [ ] No [ ] Partial
Reviewed by: _____ Date: _____ Y=Yes / N=No / P=Partial | Detailed checklist: Module 4 (operations) and Module 6 (development).	

Complete annually; present results to the IT Steering Committee.

ISO 27001 ISMS Self-Assessment — annual review of the Information Security Management System	
Check	Status
Information security policy approved by designated authority and published to staff	[ ] Yes [ ] No
Risk assessment conducted and documented within the past 12 months	[ ] Yes [ ] No
Asset inventory (F 4.14) linked to a security classification for each system	[ ] Yes [ ] No
Access control reviewed on a least-privilege basis at least quarterly	[ ] Yes [ ] No
Incident response procedure (Module 4, SOP 4.8.1) tested at least once this year	[ ] Yes [ ] No
Statement of Applicability (which ISO 27001 controls apply and why) is current	[ ] Yes [ ] No

2.3 ISO/IEC 20000-1:2018 — IT Service Management / *IT* सेवा व्यवस्थापन

ISO/IEC 20000-1:2018 (2018)

IT सेवा व्यवस्थापन प्रणाली (ITSMS) | International Organization for Standardization (ISO)

Focus: ISO 20000 provides the international standard for establishing a Service Management System (SMS) — ensuring government ICT services are planned, designed, delivered, and improved systematically to meet agreed citizen and internal service requirements.

Key Components / मुख्य अवयवहरु

- **Service Portfolio:** Define and maintain a catalogue of all IT services delivered to citizens and staff — their scope, responsibilities, and service targets.
- **Service Level Agreements (SLAs):** Documented agreements between the IT team and users specifying service quality targets (uptime, incident response times, resolution times).
- **Service Design and Transition:** Plan and manage new or changed services through testing, training, and handover — preventing disruption when systems change.
- **Incident and Problem Management:** Structured process for logging, classifying, resolving service disruptions (incidents) and eliminating root causes (problems).
- **Change Management:** Controlled evaluation, authorization, and implementation of changes to ICT systems — preventing self-inflicted service outages.
- **Continual Improvement:** Structured review of service performance data to identify and implement service quality improvements over time.

Nepal/LG Government Adaptation

→ **Citizen service quality.** The purpose of government ICT is service delivery. ISO 20000 provides the structure to ensure services meet defined quality standards — not just 'the system is up' but 'citizens can complete their service within defined timeframes.'

→ **Service Catalogue alignment.** Every LG should maintain a Service Catalogue (Module 7, M7-T07) listing all ICT services, their availability targets, and responsible officers. This is the ISO 20000 service portfolio in practice.

→ **Vendor SLA management.** ISO 20000 principles directly inform AMC contract SLA requirements (Module 5, M5-T17) and vendor performance monitoring (Module 5, M5-T22). The monthly SLA Performance Report (M5-T15) implements ISO 20000 service level monitoring.

→ **Module 4 alignment.** The Service Desk (Module 4, Section 4.3), Incident Management (Section 4.2), and Change Management (Section 4.3) SOPs are directly derived from ISO 20000 practices.

Quick Self-Check / द्रुत आत्म-मूल्याङ्कन (Complete annually or when implementing this standard)	
Check Item	**Status**
Is a Service Catalogue (M7-T07) maintained and published on the official website — listing all ICT services, availability, and responsible contacts?	[ ] Yes [ ] No [ ] Partial
Are SLA targets defined in all vendor AMC contracts (Module 5, M5-T17) with documented response and resolution times by priority level?	[ ] Yes [ ] No [ ] Partial
Is the Service Desk Daily Log (Module 4, F 4.8) maintained — logging every IT contact and tracking resolution?	[ ] Yes [ ] No [ ] Partial
Is a Change Request Form (Module 4, F 4.7) required before any change to production ICT systems?	[ ] Yes [ ] No [ ] Partial
Are quarterly service performance reviews conducted and reported to the designated authority — covering incident volumes, SLA compliance, and improvement actions?	[ ] Yes [ ] No [ ] Partial
Reviewed by: _____ Date: _____ Y=Yes / N=No / P=Partial | Detailed checklist: Module 4 (operations) and Module 6 (development).	

Complete quarterly as part of the SLA and service-quality review.

ISO 20000 Service Management Checklist — quarterly IT service management review	
Check	**Status**
Service catalogue maintained and current (what services are offered, to whom)	[ ] Yes [ ] No
SLA targets defined for each service and actually measured	[ ] Yes [ ] No
Incident, problem, and change processes followed per the Module 4 SOPs	[ ] Yes [ ] No
Service performance reviewed at least quarterly	[ ] Yes [ ] No
User/citizen satisfaction with service delivery tracked in some form	[ ] Yes [ ] No

2.4 COBIT 2019 — IT Governance Framework / IT सुशासन ढाँचा

2.4 | COBIT 2019 (2019)

IT सुशासन ढाँचा (COBIT) | ISACA (Information Systems Audit and Control Association)

Focus: COBIT 2019 is the leading international IT governance framework. Its core principle is the clear separation of IT Governance (the designated authority and IT Steering Committee — setting direction, approving policy, evaluating risk) from IT Management (the IT Official — implementing direction and operating systems). This separation is essential for accountability and audit compliance in government ICT.

2.4 | COBIT 2019 (2019)

IT सुशासन ढाँचा (COBIT) | ISACA (Information Systems Audit and Control Association)

Key Components / मुख्य अवयवहरू

- **Governance vs Management:** Governance = Evaluate, Direct, Monitor (EDM) — done by the designated authority/Steering Committee. Management = Align, Plan, Build, Run, Monitor (APBRO) — done by the IT Official. These roles must not be confused.
- **Governance Objectives:** COBIT 2019 defines 40 governance and management objectives covering strategy, risk, resources, performance, and compliance — organized into five domains.
- **Design Factors:** COBIT recognizes that governance needs vary by organization size, risk profile, and sector. A small rural municipality applies a simplified governance model; a large urban municipality applies a more comprehensive one.
- **Performance Management:** Define Key Performance Indicators (KPIs) for ICT services and report them regularly — enabling evidence-based governance decisions by the designated authority.
- **Risk Management:** Maintain an IT Risk Register identifying key risks to ICT services and citizen data; review at every IT Steering Committee meeting.
- **Stakeholder Focus:** IT governance exists to create value for stakeholders — citizens, elected officials, and staff. Every ICT decision should be traceable to a stakeholder benefit.

Nepal/LG Government Adaptation

→ **Governance clarity is critical.** A common failure in LG ICT governance is the IT Official making decisions that should be made by the designated authority (e.g., approving large contracts or major system changes without designated authority involvement). COBIT prevents this by defining clear governance boundaries.

→ **IT Steering Committee.** COBIT's EDM (Evaluate-Direct-Monitor) domain is implemented through the IT Steering Committee: quarterly meetings chaired by the designated authority, reviewing ICT performance, approving major decisions, and monitoring risk. See Module 4, Section 4.1 (IT Governance, F 4.1 Decision Log).

→ **Annual ICT Plan.** COBIT's planning domain is implemented through the Annual ICT Procurement Plan (Module 5, M5-T01) and the Annual Work Plan alignment requirement. The designated authority approves; the IT Official implements.

→ **Audit readiness.** COBIT's monitoring domain aligns with CIAA Investigation requirements — documented decisions, clear approval chains, and performance evidence. Module 4, F 4.2 (IT Governance Self-Assessment) implements the annual COBIT review.

Quick Self-Check / द्रुत आत्म-मूल्याङ्कन *(Complete annually or when implementing this standard)*

Check Item	Status
Does the IT Steering Committee meet at least quarterly with the designated authority chairing and minutes documented?	[ ] Yes [ ] No [ ] Partial
Is there a documented Annual ICT Plan (M5-T01) approved by the designated authority before the fiscal year starts?	[ ] Yes [ ] No [ ] Partial
Is an IT Risk Register maintained and reviewed at each Steering Committee meeting?	[ ] Yes [ ] No [ ] Partial
Are ICT KPIs (incident resolution rate, SLA compliance, backup success, patch compliance) reported to the designated authority at least quarterly?	[ ] Yes [ ] No [ ] Partial

Is the ICT Decision Log (Module 4, F 4.1) maintained — recording all significant ICT decisions with designated authority approval dates?	[ ] Yes [ ] No [ ] Partial
Reviewed by: _____ Date: _____ Y=Yes / N=No / P=Partial | Detailed checklist: Module 4 (operations) and Module 6 (development).	

Complete annually; present results to the IT Steering Committee.

F 2.3 | COBIT IT Governance Self-Assessment — annual governance review	
Check	**Status**
IT Steering Committee (or equivalent) meets regularly with documented minutes	[ ] Yes [ ] No
IT strategy is explicitly aligned to institutional/provincial goals	[ ] Yes [ ] No
Roles and responsibilities for key ICT decisions are defined (who approves what)	[ ] Yes [ ] No
A risk register is maintained and reviewed	[ ] Yes [ ] No
ICT performance metrics are reported to leadership at least annually	[ ] Yes [ ] No

2.5 ITIL 4 — IT Service Value System / IT सेवा मूल्य प्रणाली

ITIL 4

IT सेवा व्यवस्थापन अभ्यासहरू (ITIL 4) | PeopleCert/Axelos (originally CCTA/UK Government)

Focus: ITIL 4 (Information Technology Infrastructure Library) is the world's most widely used IT service management framework. It provides best-practice guidance for managing IT services across the full Service Value Chain — from understanding demand through delivering and improving services. ITIL 4's 34 practices cover every aspect of IT service operations relevant to provincial and local government.

Key Components / मुख्य अवयवहरू

- **Service Value System (SVS):** The overall model: Guiding Principles → Governance → Service Value Chain → Practices → Continual Improvement. Everything connects to creating value for citizens.
- **Guiding Principles:** Focus on value; Start where you are; Progress iteratively; Collaborate and promote visibility; Think and work holistically; Keep it simple and practical; Optimize and automate.
- **Service Value Chain:** 6 activities: Plan → Engage → Design & Transition → Obtain/Build → Deliver & Support → Improve. Each activity adds value toward the citizen service outcome.
- **Key Practices for LG:** Incident Management; Problem Management; Change Enablement; Service Desk; Service Level Management; IT Asset Management — all implemented in Module 4.

Nepal/LG Government Adaptation

→ **Module 4 is ITIL 4.** The ICT operations procedures in Module 4 (Incident Management, Problem Management, Change Management, Service Desk, Asset Management) are directly derived from ITIL 4 practices. Implementing Module 4 SOPs = implementing ITIL 4 foundations.

→ **Seven guiding principles for LG IT Officials:** Keep it simple and practical is the most relevant for resource-constrained LGs. Don't over-engineer; implement what creates actual citizen value. Start where you are — don't redesign from scratch what already works.

→ **Value chain integration with GEA 2.0.** ITIL 4's 'Obtain/Build' activity directly corresponds to the procurement (Module 5) and system development (Module 6) stages in this handbook. The 'Deliver and Support' activity corresponds to Module 4 operations.

◆ **Continual Improvement:** Structured cycle for improving services and practices: What is the vision? Where are we now? Where do we want to be? How do we get there? Did we get there? ◆ **Holistic Thinking:** ITIL 4 emphasizes that people, processes, technology, and partners must all be considered together — not just the technical system in isolation.	→ **SLA management.** ITIL 4's Service Level Management practice is implemented through the vendor SLA framework (Module 5, M5-T15, M5-T17, M5-T22). Service targets are defined in contracts; performance is measured monthly.

Quick Self-Check / द्रुत आत्म-मूल्याङ्कन (Complete annually or when implementing this standard)	
Check Item	**Status**
Are all ICT service incidents logged in the Incident Log (Module 4, F 4.3) regardless of whether they were self-resolved?	[ ] Yes [ ] No [ ] Partial
Is Problem Management (Module 4, SOP 4.2.2, F 4.6) triggered automatically when any incident recurs more than twice?	[ ] Yes [ ] No [ ] Partial
Is a Change Request Form (Module 4, F 4.7) required for every system change before implementation — including security patches?	[ ] Yes [ ] No [ ] Partial
Is the Service Desk the documented Single Point of Contact (SPOC) for all ICT requests — with the Daily Log (F 4.8) as the audit record?	[ ] Yes [ ] No [ ] Partial
Does the IT Official report at least 3 ICT performance metrics to the designated authority every quarter (incident volumes, SLA compliance, backup success rate)?	[ ] Yes [ ] No [ ] Partial
Reviewed by: _____ Date: _____ Y=Yes / N=No / P=Partial | Detailed checklist: Module 4 (operations) and Module 6 (development).	

Complete monthly as part of the service management review.

ITIL 4 Practice Implementation Checklist — monthly practice review	
Check	**Status**
Service desk operates as a single point of contact (SOP 4.3.2)	[ ] Yes [ ] No
Incident, change, and problem management practices are actually being followed, not just documented	[ ] Yes [ ] No
Roles across the service value chain are assigned to named individuals	[ ] Yes [ ] No
A continual-improvement register is maintained and reviewed	[ ] Yes [ ] No

2.6 CMMI V2.0 — Capability Maturity Model / क्षमता परिपक्वता मोडेल

CMMI V2.0

क्षमता परिपक्वता मोडेल एकीकरण | CMMI Institute

Focus: CMMI V2.0 (Capability Maturity Model Integration) is a framework for assessing and improving the maturity and capability of organizational ICT processes across five progressive levels. For Gandaki Province LGs, CMMI provides a structured roadmap for developing ICT process capability over time — from reactive, ad-hoc operations toward proactive, optimized management.

CMMI V2.0

क्षमता परिपक्वता मोडेल एकीकरण | CMMI Institute

Key Components / मुख्य अवयवहरू

- Level 1 — Initial: Processes are ad-hoc and chaotic. Success depends on individual heroics rather than repeatable processes. Most LGs start here.
- Level 2 — Managed: Basic project management practices are in place. Processes are planned, performed, measured, and controlled at the project level. Module 4 SOPs establish Level 2 foundations.
- Level 3 — Defined: Standard organizational processes are defined, documented, and consistently followed across the organization. Handbook implementation achieves Level 3 target.
- Level 4 — Quantitatively Managed: Processes are measured and controlled using quantitative methods. KPIs and data-driven decision-making guide ICT management.
- Level 5 — Optimizing: Continuous process optimization driven by data. Proactive identification and management of process improvements. Long-term target for leading LGs.
- Practice Areas: CMMI covers 20 practice areas across 4 categories: Doing, Managing, Enabling, and Improving — with guidance specific to software development, services, and supplier management.

Nepal/LG Government Adaptation

→ **Where Gandaki Province LGs are now:** Most LGs are at CMMI Level 1 (Initial) — ICT processes are reactive and person-dependent. When the IT Official leaves, institutional knowledge walks out the door.

→ **This handbook targets Level 2-3.** Implementing the SOPs, checklists, and forms in Modules 4, 5, and 6 moves LGs from Level 1 (chaotic) to Level 2 (managed) and toward Level 3 (defined, documented, repeatable). This is achievable within 1-2 fiscal years.

→ **The Staff Handover Procedure (Module 4, Section 4.11)** is the most direct CMMI Level 2 intervention for LGs — it institutionalizes knowledge rather than leaving it with individuals. F 4.24 Technical Handover Checklist + F 4.25 Credentials Register = Level 2 process documentation.

→ **CMMI and Digital Nepal Framework 2.0.** The DNF 2.0 digital transformation stages align with CMMI levels. Moving to Stage 3-4 on the E-Governance Maturity Index (Module 1, Section 1.5) requires CMMI Level 3 process maturity.

Quick Self-Check / द्रुत आत्म-मूल्याङ्कन

Check Item	Status
Are ICT processes documented — can a new IT Official follow SOPs from this handbook without the previous officer's guidance?	[ ] Yes [ ] No [ ] Partial
Is the Annual ICT Plan (M5-T01) prepared before the fiscal year — based on documented needs assessment rather than reactive requests?	[ ] Yes [ ] No [ ] Partial
Is the Staff Handover Checklist (F 4.23/4.24) used for every IT Official departure — ensuring institutional knowledge is captured?	[ ] Yes [ ] No [ ] Partial
Are ICT KPIs measured and reported quarterly — enabling data-informed decisions rather than reactive management?	[ ] Yes [ ] No [ ] Partial
Is a Continual Improvement action tracked from each quarterly review — at least one identified improvement per quarter with a completion date?	[ ] Yes [ ] No [ ] Partial

Reviewed by: _____ Date: _____ Y=Yes / N=No / P=Partial | Detailed checklist: Module 4 (operations) and Module 6 (development).

Complete annually; track maturity progression year over year.

F 2.5 | CMMI Process Maturity Self-Assessment — annual maturity review	
Check	**Status**
Key ICT processes are documented, not purely informal or ad hoc	[ ] Yes [ ] No
Process performance is measured against defined targets	[ ] Yes [ ] No
Lessons learned are captured after every major project or incident	[ ] Yes [ ] No
Identified process improvements are tracked through to closure	[ ] Yes [ ] No
A maturity level (1–5) is self-rated for core processes, with supporting evidence	[ ] Yes [ ] No

2.7 Standards Integration — Nepal Policy Alignment

मानकहरूको एकीकरण र नेपाल नीति समन्वयता

The five frameworks are not independent — they address complementary aspects of ICT governance. The table below shows how they align with Nepal's national ICT policies and with each other. An IT official implementing this handbook is simultaneously applying elements of all five frameworks — aligned with national legal requirements.

Framework	What it contributes	Nepal Policy Alignment	Implemented in this Handbook
ISO 27001 Information Security	Protecting citizen data and government ICT systems. Risk-based security management. Audit-ready controls.	National Cybersecurity Policy 2080 · Privacy Act 2075 · ETA 2063	Module 4: Sections 4.6, 4.7, 4.8 (physical security, InfoSec, VAPT) · Module 3: F 3.2 (Privacy checklist)
ISO 20000 Service Management	Quality ICT service delivery. Defined SLAs. Service catalogue. Structured incident and change management.	Good Governance Act 2064 · GEA 2.0 service delivery principles	Module 4: Sections 4.2, 4.3 (Incident, Change, Service Desk) · Module 5: M5-T15, M5-T17 (SLA management)
COBIT 2019 IT Governance	Clear accountability — governance vs management. IT Steering Committee. Audit trail. Risk management.	Good Governance Act 2064 · LGOA 2074 · CIAA compliance requirements	Module 4: Section 4.1 (IT Governance, F 4.1, F 4.2) · Module 5: M5-T01 (Annual ICT Plan)
ITIL 4 Service Value Chain	End-to-end service delivery lifecycle. 34 best-practice service management practices. Continual improvement.	GEA 2.0 service value chain · Digital Nepal Framework 2.0 service integration	Module 4: All operational sections (4.1–4.11) · Module 6: System Development (6.1–6.4)
CMMI V2.0 Process Maturity	Process documentation and improvement roadmap. Moves LGs from Level 1 (reactive) to Level 3 (defined).	Digital Nepal Framework 2.0 digital maturity targets · DNF 2.0 e-governance stages	Modules 4, 5, 6, 7: All SOPs and documented procedures build CMMI Level 2-3 maturity

Combined Governance Framework:
1. **Set direction** Delegated authority approves ICT policy, budget, and major decisions (Local Government Operation Act 2074). Documented in ICT Decision Log (F 4.1).
2. **Protect information** (ISO 27001 → Privacy Act 2075 + Cybersecurity Policy): An IT Official implements risk-based security controls. Citizen data encrypted, access-controlled, and audit-logged. Reviewed annually.
3. **Deliver services** (ITIL 4 + ISO 20000 → GEA 2.0 + Good Governance): Service Desk, Incident Management, and Change Management operating per Module 4 SOPs. SLAs are monitored monthly.
4. **Build and procure right** (GEA 2.0 + ISO 27001 → VAPT, APIs, source code): All new systems GEA 2.0 compliant, VAPT-cleared, and procured per Module 5. The government retains data and source code ownership.
5. **Improve continuously** (CMMI + ITIL Continual Improvement → DNF 2.0 maturity): Annual ISMS review, quarterly KPI reporting, and staff handover documentation progressively advance process maturity.

See Also (📌):

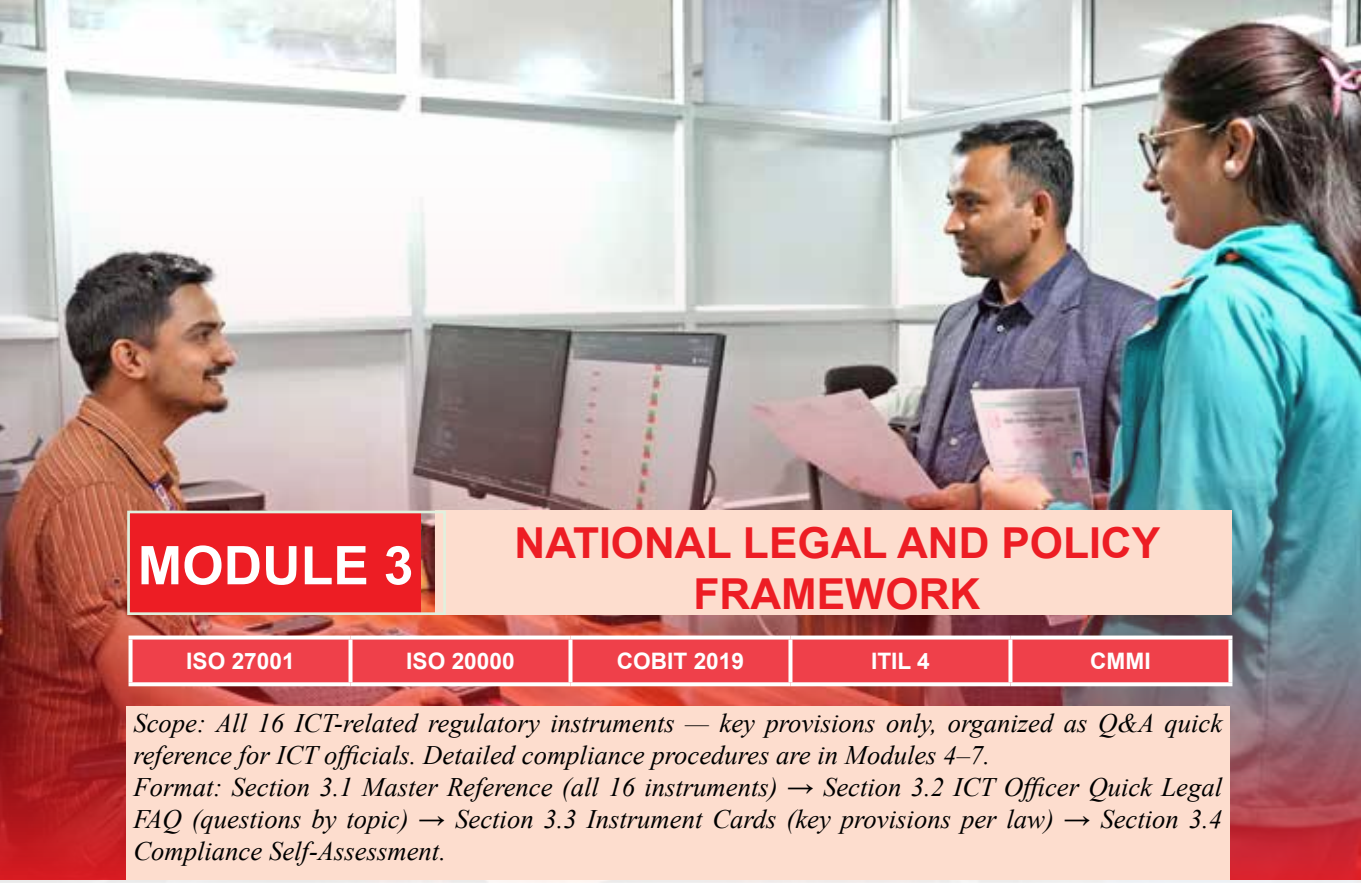
ISO 27001 implementation (security controls): Module 4 Sections 4.6, 4.7, 4.8.

ITIL 4 / ISO 20000 implementation (operations): Module 4 Sections 4.2, 4.3, 4.4.

COBIT 2019 governance (IT Steering Committee): Module 4 Section 4.1.

CMMI maturity (process documentation): All modules — each SOP and checklist in Modules 4-7 contributes to CMMI Level 2-3 maturity.

Nepal legal alignment: Module 3 (Sections 3.3-3.13) provides the national legal framework context for all five standards.



MODULE 3

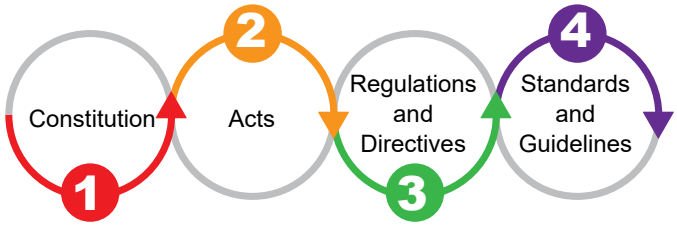
NATIONAL LEGAL AND POLICY FRAMEWORK

ISO 27001	ISO 20000	COBIT 2019	ITIL 4	CMMI

Scope: All 16 ICT-related regulatory instruments — key provisions only, organized as Q&A quick reference for ICT officials. Detailed compliance procedures are in Modules 4–7.
Format: Section 3.1 Master Reference (all 16 instruments) → Section 3.2 ICT Officer Quick Legal FAQ (questions by topic) → Section 3.3 Instrument Cards (key provisions per law) → Section 3.4 Compliance Self-Assessment.

This module provides a concise, navigable reference to Nepal's key national ICT governance instruments. Understanding and complying with these laws and policies is not optional — it is a legal obligation. Every ICT decision made by a official, from procuring a server to launching a citizen portal, must be grounded in the national legal and policy framework described in this module.

Nepal's Legal Hierarchy — What Outranks What



3.1 Master Reference — All Regulatory ICT Instruments / सबै नियमनकारी ICT दस्तावेजहरूको मुख्य सन्दर्भ

Reference list of Relevant ICT legal and policy instruments which every ICT official must be familiar with. Detailed key provisions for each are in Section 3.3.

#	Instrument / दस्तावेज	Type	Year	Primary ICT Relevance for LG Officers
1	Constitution of Nepal नेपालको संविधान	Constitutional Law	2015	Schedules 8 and 9: LG exclusive and concurrent ICT powers. Article 27: RTI. Article 28: Privacy. Article 51(j): State ICT policy.

#	Instrument / दस्तावेज	Type	Year	Primary ICT Relevance for LG Officers
2	Electronic Transactions Act (ETA) विद्युतीय कारोबार ऐन	Primary Law	2063 (2008)	Sections 3-5: Electronic records and digital signatures legally valid. Sections 44-47: Cyber offences and penalties. Foundation for all digital government services.
3	Individual Privacy Act व्यक्तिगत गोपनीयता ऐन	Primary Law	2075 (2018)	Citizen data protection obligations: collection, use, storage, disclosure. Consent requirements. Right to access and correct personal data. Breach reporting obligations.
4	Right to Information Act सूचनाको हकसम्बन्धी ऐन	Primary Law	2064 (2007)	Proactive disclosure mandatory (budget, procurement, decisions). Designate Information Officer. Respond to RTI requests within 15 days. Annual RTI report to NIC.
5	Public Procurement Act (PPA) सार्वजनिक खरिद ऐन	Primary Law	2063 (2007)	Governs ALL ICT procurement. e-GP portal mandatory above threshold. Brand-neutral specifications. QCBS 80:20 for consulting. Conflict of interest prohibition.
6	Public Procurement Regulations (PPR) सार्वजनिक खरिद नियमावली	Regulation	2064 (2008)	Implementing regulation for PPA. Defines all procurement thresholds, methods, timelines, and bidding document requirements. Verify current thresholds at ppmo.gov.np.
7	Good Governance Act सुशासन ऐन	Primary Law	2064 (2008)	Citizen Charter mandatory for all services (include digital services). Grievance mechanism. Equal, efficient, and transparent public service delivery standards.
8	Local Government Operation Act (LGOA) स्थानीय सरकार सञ्चालन ऐन	Primary Law	2074 (2017)	LG mandate for digital service delivery. LG can independently procure ICT services per PPA 2063. Local ICT management responsibilities clearly vested in LG.
9	Nepal GEA 2.0 नेपाल गभर्नमेन्ट इन्टरप्राइज आर्किटेक्चर	Technical Framework	2022	Mandatory for ALL government systems. REST/ JSON APIs. GIDC-first hosting. NID integration. 100% government data and source code ownership. 9 mandatory artifacts. VAPT before go-live.
10	IT Norms 2082 IT दर मापदण्ड	Rate Standard	2082 (2025)	Mandatory monthly rates for all ICT personnel roles. Minimum qualification requirements. Must be used in ALL ICT consulting budget estimates. Verify current rates at mocit.gov.np.
11	Data Center and Cloud Directives 2081 डेटा सेन्टर निर्देशिका	Directive	2081 (2024)	GIDC must be evaluated as first hosting option. Only DoIT-enlisted vendors permitted. All citizen data must remain within Nepal. Audit rights in all hosting contracts.
12	National Cybersecurity Policy राष्ट्रिय साइबर सुरक्षा नीति	Policy	2080 (2023)	Baseline security controls mandatory for all government systems. NCSC VAPT mandatory before go-live. Incident reporting to NCSC mandatory. Minimum encryption: TLS 1.2+, AES-256.

#	Instrument / दस्तावेज	Type	Year	Primary ICT Relevance for LG Officers
13	Digital Nepal Framework 2.0 (DNF 2.0) डिजिटल नेपाल ढाँचा	National Policy	2023	Five pillars including Digital Government. NID integration mandatory. Nagarik App integration. e-GP for procurement. Digital One-Stop Service Delivery target by 2085 BS.
14	National AI Policy राष्ट्रिय AI नीति	National Policy	2082 (2025)	Human oversight mandatory for AI government decisions. Bias testing required before deployment. Privacy Act 2075 applies to all AI using citizen data. designated authority sign-off required.
15	National ICT Policy राष्ट्रिय ICT नीति	National Policy	2015 (2072 BS)	WCAG accessibility mandatory for government portals. E-waste disposal obligations. ICT HR development requirements. Inclusive digital service delivery standards.
16	Financial Procedures and Fiscal Accountability Act आर्थिक कार्यविधि तथा वित्तीय उत्तरदायित्व ऐन	Primary Law	2076 (2019)	ICT budget classification and financial control requirements. ICT assets must be registered in PAMS within 7 working days. Procurement financial documentation standards.
17	e-Governance Blueprint Blueprint ई-गभर्नेन्स ब्लु प्रिन्ट	Strategic Blueprint	2082	A national strategic blueprint designed to transform public service delivery into a seamless digital ecosystem. It establishes the "Once-Only Principle" (OOP), mandates secure data exchange platforms, and enforces digital signatures.
18	Standard for Mobile Apps of Government Bodies सरकारी निकायका मोवाइल एपहरुको मापदण्ड	Standard	2075	Sets mandatory standards for government mobile apps, requiring WCAG accessibility, HTTPS data transfer, and adherence to OWASP security guidelines. Apps must function in poor connectivity or offline modes and require DoIT security clearance before launch.
19	Electronic Correspondence (Email) Management Directives सरकारी निकायमा विद्युतीय पत्राचार (इमेल) व्यवस्थापनसम्बन्धि निर्देशिका	Directive	2075	Mandates the use of the integrated email system (mail.nepal.gov.np) for official correspondence. Requires Two-Factor Authentication (2FA) for security and the archiving of official emails safely for at least 5 years. Prohibits the use of personal email accounts for official government business.
20	Information Technology Bill (Draft) सूचना प्रविधि विधेएक (मस्यौदा)	Bill Draft	2074	(Pending: I will update this row as soon as you import the web search results from the sources panel!)
21	IT System (Management and Operation) Directives सूचना प्रविधि प्रणाली (व्यवस्थापन तथा संचालन) निर्देशिका	Directive	2071	Formulated to ensure uniformity, standardization, and interoperability across all government IT systems. It mandates that systems adhere to the Government Enterprise Architecture (GEA) framework and open standards, and establishes Steering and Technical Committees for IT governance.

#	Instrument / दस्तावेज	Type	Year	Primary ICT Relevance for LG Officers
22	e-Village Operation and Management Procedure ई-भिलेज कार्यक्रम सञ्चालन तथा व्यवस्थापन कार्यविधी	Procedure	2070	Designed to expand ICT access to rural and remote areas to ensure the "digital dividend" reaches marginalized populations. It provides the framework for delivering e-Education, Telemedicine (e-Health), and e-Agriculture to local communities.

All Acts are available free at **lawcommission.gov.np** · *GEA 2.0, IT Norms, AI Policy, DNF 2.0, IT Policy:* **mocit.gov.np** · *DC/Cloud Directives:* **doit.gov.np** · *Cybersecurity Policy:* **ncsc.gov.np** · *Procurement thresholds:* **ppmo.gov.np** *(verify before each procurement — PPR thresholds are updated periodically)*

3.2 ICT Officer Quick Legal Reference — Frequently Asked Questions

ICT अधिकृत कानूनी सन्दर्भ सामाग्री — प्राय:सोधिने प्रश्नहरू

These are the ICT governance and legal questions mostly encountered by ICT officers and administrators. Each answer provides the specific legal source for direct reference and audit defence.

Electronic Records, Digital Signatures, and Data Privacy

इलेक्ट्रोनिक अभिलेख, डिजिटल हस्ताक्षर र गोपनीयता

Question / प्रश्न	Legal Answer / कानूनी उत्तर	Reference
Which law gives digital signatures the same legal validity as physical signatures?	**ETA 2063, Section 4**: Digital signatures authenticated by an OCC-registered Certifying Authority (CA) are legally equivalent to handwritten signatures for all government transactions and services.	ETA 2063 §4
Which law makes government-issued electronic records legally valid?	**ETA 2063, Section 3**: Electronic records produced by or for government offices are legally equivalent to paper records.	ETA 2063 §3
Which directive/policy mandates government services be delivered electronically?	**ETA 2063, Section 5** permits government service delivery electronically. **GEA 2.0** and **DNF 2.0** make digital service delivery mandatory for specified services.	ETA 2063 §5; GEA 2.0
Which law defines cyber crimes against government systems and their penalties?	**ETA 2063, Sections 44–47**: Unauthorized access (§44), data theft/alteration (§45), system damage/ sabotage (§46), and publishing harmful content (§47) are all criminal offences with fines and imprisonment.	ETA 2063 §44-47
Which law requires government offices to protect citizen personal data?	**Individual Privacy Act 2075**: Government bodies must collect only minimum necessary PII, use it only for the stated purpose, protect it with adequate security measures, and disclose it only to authorized parties.	Privacy Act 2075
Which law gives citizens the right to access their own personal data held by the government?	**Individual Privacy Act 2075**: Citizens have the right to access, review, and request correction of personal data held by government bodies.	Privacy Act 2075

Question / प्रश्न	Legal Answer / कानूनी उत्तर	Reference
Which law requires an ICT vendor to keep citizen data confidential?	**Privacy Act 2075 + NDA (Module 5, M5-T16)**: The Privacy Act requires all data processors (including vendors) to protect citizen data. NDA enforces this contractually.	Privacy Act 2075; ETA 2063
Which law prohibits storing citizen data outside Nepal?	**Data Center and Cloud Directives 2081**: All government citizen data must be stored in data centers within Nepal. **GEA 2.0** further mandates Nepal data residency for all government systems.	DC Directives 2081; GEA 2.0

ICT Procurement and Source Code / ICT खरिद तथा स्रोत कोड

Question / प्रश्न	Legal Answer / कानूनी उत्तर	Reference
Which framework mandates that the government retains 100% ownership of source code?	GEA 2.0: Government retains full ownership of all source code developed under government contracts. Vendors must hand over complete, documented source code upon contract completion.	GEA 2.0
Which law prohibits brand-specific ICT specifications in procurement?	PPA 2063 and PPR 2064: Procurement specifications must be performance-based and brand-neutral. Naming specific products or vendors in ToR violates PPA — creates a CIAA Investigation finding.	PPA 2063; PPR 2064
Which standard sets the rates for ICT consultants and personnel in government contracts?	IT Norms 2082 (MoCIT): Mandatory monthly rate benchmarks for all ICT roles. Must be applied to all ICT consulting ToR cost estimates. Verify current rates at mocit.gov.np before each procurement.	IT Norms 2082
Which directive requires the government to evaluate GIDC hosting before commercial cloud?	Data Center and Cloud Directives 2081: GIDC (Government Integrated Data Center, operated by IDMC) must be evaluated as the first hosting option before any commercial hosting decision.	DC Directives 2081
Which law mandates QCBS 80:20 for ICT consulting procurement?	PPR 2064: Quality and Cost-Based Selection (QCBS) at 80% technical + 20% financial is the mandatory method for all government ICT consulting evaluations.	PPR 2064
Who audits ICT procurement spending — OAG or CIAA?	OAG (Constitution Art. 240/241; Audit Act 2075): conducts the annual FINANCIAL audit of all federal, provincial, and local government ICT expenditure. CIAA (Art. 238–239; CIAA Act 2048): investigates procurement IRREGULARITIES and corruption (brand-specific specs, threshold splitting). CIAA maintains a Pokhara-Kaski outreach office serving Gandaki Province directly.	Constitution Art. 240/241; Audit Act 2075; CIAA Act 2048
What is required before designing and developing a new IT system to ensure it meets government standards?	IT System (Management and Operation) Directives 2071, Section 4: Before a government body develops a new IT system for service delivery, it must prepare the system-related requirement and design documents. These must be submitted to the Department of Information Technology (DoIT) through the central body to verify that the system conforms to standard norms.	IT System Directives 2071

Question / प्रश्न	Legal Answer / कानूनी उत्तर	Reference
Can a government body procure consultants to prepare or modify IT system standards?	IT System (Management and Operation) Directives 2071, Section 19: Yes, the Department can appoint a consultant in accordance with prevailing procurement laws to prepare or modify the necessary standards for the IT systems of government bodies.	IT System Directives 2071

Access to Information and Citizen Rights / सूचना पहुँच र नागरिक अधिकार

Question / प्रश्न	Legal Answer / कानूनी उत्तर	Reference
Which law requires the government to proactively publish information online?	RTI Act 2064, Section 5: Government bodies must proactively publish: organizational details, functions, budget, procurement decisions, and service information. A designated Information Officer is mandatory.	RTI Act 2064 §5
Which law requires all government websites to be accessible to persons with disabilities?	National ICT Policy 2015: WCAG 2.1 Level AA accessibility is mandatory for all government web portals and applications.	IT Policy 2015; WCAG 2.1
Which law mandates a Citizen Charter for government services?	Good Governance Act 2064, Section 19: Every government body must publish a Citizen Charter specifying service names, required documents, fees, timeframes, and responsible officers — including digital services.	Good Governance Act 2064 §19
Which law empowers local governments to independently deliver ICT services?	LGOA 2074, Schedule 8: Local governments have the constitutional mandate and operational authority to deliver ICT-enabled public services independently, subject to national standards (GEA 2.0, PPA 2063).	LGOA 2074; Constitution 2015
What are the mandatory standards for developing and managing a government office website?	Government Office Website Construction and Management Directives (सरकारी कार्यालयको वेबसाइट निर्माण तथा व्यवस्थापन निर्देशिका): Mandates the use of an official .gov.np domain and standardized platforms like GIWMS to maintain the website. The website must feature a mobile-first design, prioritize the Nepali language, meet WCAG 2.1 Level AA accessibility standards, and ensure proactive RTI disclosures and the Citizen Charter are regularly updated.	Website Directives

Security, AI, and Emerging Technologies /सुरक्षा, AI र उदीयमान प्रविधि

Question / प्रश्न	Legal Answer / कानूनी उत्तर	Reference
Which policy makes NCSC VAPT mandatory before go-live for government systems?	National Cybersecurity Policy 2080 + GEA 2.0: All internet-facing government systems must obtain NCSC VAPT clearance before going live. VAPT is free for government bodies (NCSC: +977-1-4200144).	Cybersecurity Policy 2080; GEA 2.0

Question / प्रश्न	Legal Answer / कानूनी उत्तर	Reference
Which policy requires human oversight for all government AI decisions affecting citizens?	National AI Policy 2025 (2082 BS): AI systems used in government must have human oversight. Citizens must have the right to request human review of any AI-assisted government decision.	AI Policy 2025
Which law requires security incident reporting to NCSC?	National Cybersecurity Policy 2080: All government bodies must report cyber security incidents to NCSC within specified timelines. Critical incidents must be reported immediately.	Cybersecurity Policy 2080
Which policy requires NID integration for citizen-facing government portals?	Digital Nepal Framework 2.0 (DNF 2.0) + GEA 2.0: NID (National Identity Card) authentication must be integrated into all new citizen-facing government portals.	DNF 2.0; GEA 2.0

3.3 Key Provisions by Instrument / उपकरण अनुसार मुख्य व्यवस्थाहरू

Electronic Transactions Act 2063 (ETA) विद्युतीय कारोबार ऐन २०६३ | Primary Law

Purpose: Provides the primary legal foundation for electronic governance in Nepal by legally validating electronic records and communications. It officially enables government bodies to deliver public services electronically and recognizes digital signatures authenticated by an OCC-registered Certifying Authority as legally equivalent to handwritten signatures. Furthermore, the Act provides the statutory framework for defining and prosecuting cybercrimes—such as unauthorized system access, data theft, and system sabotage—making it the essential bedrock for accountability and security in Nepal's digital ecosystem

Question IT Officials Ask	Key Provision / Legal Answer
Q: Which provision validates electronic government records?	A: Section 3: Electronic records have the same legal validity as paper records for all purposes.
Q: Which provision validates digital signatures?	A: Section 4: Digital signatures by OCC-registered CAs are legally equivalent to handwritten signatures.
Q: Which provision enables electronic government services?	A: Section 5: Government services may be delivered electronically. Electronic applications, submissions, and communications are legally valid.
Q: What is the penalty for unauthorized system access (hacking)?	A: Section 44: Unauthorized access is punishable — fine up to NPR 1,00,000 and/or imprisonment up to 5 years.
Q: What are the penalties for data theft/ alteration and system damage?	A: Sections 45-47: Data theft/alteration (§45), system sabotage (§46), and harmful content publication (§47) — fines and imprisonment up to 5 years.

IT Official Action: Report ALL cyber incidents to NCSC (+977-1-4200144). Only use OCC-registered CAs for government digital signatures (currently: Radiant InfoTech Nepal). Verify at occ.gov.np.

Individual Privacy Act 2075 व्यक्तिगत गोपनीयता ऐन २०७५ | Primary Law

Purpose: Establishes citizen data protection obligations for all government bodies — covering collection, use, storage, and disclosure of personal information, with the right to privacy as a constitutional guarantee (Article 28).

Question IT Officials Ask	Key Provision / Legal Answer
Q: What is the legal basis for collecting citizen personal data?	**A:** Must have a specific, documented, lawful purpose. Collect only minimum data necessary (data minimization principle). Informed consent or legal mandate required.
Q: Can the government use citizen data collected for one service for another purpose?	**A:** No. Purpose limitation applies — data collected for birth registration cannot be used for tax campaigns without separate legal basis or explicit consent.
Q: What must the government do when citizen data is breached?	**A:** Immediately investigate, contain the breach, notify affected citizens, and report to relevant authorities. IT Official logs in F 4.17 (Security Incident Report). For significant breaches, notify NCSC.
Q: Can vendors access citizen PII without restriction?	**A:** No. All vendors must sign NDA (M5-T16) BEFORE any system access. Contracts must include Privacy Act compliance clauses and data residency requirements.
Q: What rights do citizens have over their personal data?	**A:** Right to know what data is held, why, and by whom. Right to access their own data. Right to request correction of inaccurate data. Right to complain about unauthorized use.

Display privacy notices at ALL data collection points (online and physical). Complete Privacy Act Compliance Checklist (Module 4, F 4.12) annually. All vendors must sign M5-T16 NDA before any access.

Complete annually, and before every new system go-live.

Privacy Act 2075 Compliance Checklist — annual review and pre-go-live check	
Check	**Status**
Lawful purpose documented for every category of personal data collected	[ ] Yes [ ] No
Data minimization applied — no fields collected beyond what the service needs	[ ] Yes [ ] No
Data subject consent or notice given where the Act requires it	[ ] Yes [ ] No
Data retention period defined and not exceeded	[ ] Yes [ ] No
Security measures in place — encryption at rest/in transit, access control	[ ] Yes [ ] No
Data breach response procedure exists and is known to staff (Module 4, SOP 4.8.1)	[ ] Yes [ ] No

Right to Information Act 2064 सूचनाको हकसम्बन्धी ऐन २०६४ | Primary Law

Purpose: Guarantees citizens the right to access government information and mandates proactive disclosure of specified information — including budget, procurement decisions, and service information — without waiting for citizen requests.

Question IT Officials Ask	Key Provision / Legal Answer
Q: What information must be proactively published without a citizen request?	**A:** Organizational structure, functions, budget, sources of income, details of officers, procurement decisions, and project information. Must be updated at least quarterly and published on the official website.

Q: Who is the Information Officer and what is their legal obligation?	**A:** Every government body must designate an Information Officer. The Officer must respond to RTI requests within 15 days and manage all proactive disclosure requirements.
Q: What is the penalty for refusing a lawful RTI request?	**A:** The RTI Act provides for complaint mechanisms and penalties against officers who refuse legitimate RTI requests without valid legal grounds.
Q: Does RTI apply to information stored in ICT systems?	**A:** Yes. Electronic records, databases, and digital files are subject to RTI. Electronic records cannot be withheld simply because they are digital.
Q: How does RTI interact with the Privacy Act?	**A:** The two laws must be balanced. Personal citizen data (PII) is exempt from RTI disclosure under the Privacy Act 2075. Procurement decisions and policy information must be disclosed per RTI, even if submitted digitally.
IT Official Action: Designate an Information Officer if not yet done. Publish proactive disclosure items on GIWMS website quarterly. Include all required disclosures in the Citizen Charter. Reference Module 4 F 4.22 (website management).	

Complete quarterly as part of the portal content compliance review.

RTI and Proactive Disclosure Checklist — quarterly compliance review	
Check	**Status**
22-point proactive disclosure checklist published and current on the official website	[ ] Yes [ ] No
An Information Officer is designated and their contact details are published	[ ] Yes [ ] No
RTI request log is maintained	[ ] Yes [ ] No
Requests are responded to within the statutory 21-day timeframe	[ ] Yes [ ] No
Annual RTI report submitted to the National Information Commission	[ ] Yes [ ] No

3.4 Public Procurement Act 2063 + Regulations 2064 (PPA + PPR) (2063 + 2064)

सार्वजनिक खरिद ऐन + नियमावली | Primary Law + Regulation

Purpose: Governs ALL government procurement including ICT — establishing mandatory competitive processes, prohibiting brand-specific specifications, and setting thresholds for different procurement methods. CIAA investigates procurement irregularities against these laws.

Question IT Officials Ask	Key Provision / Legal Answer
Q: Can we specify a particular brand (e.g., HP, Cisco, Microsoft) in ICT procurement?	**A:** No. PPA 2063 requires brand-neutral, performance-based specifications. Naming brands is a PPA violation and creates CIAA Investigation findings. Specify technical standards (e.g., 'quad-core processor, min 3.0 GHz') not brands.
Q: Is competitive bidding always required for ICT hardware?	**A:** Thresholds determine the method — verify current amounts at ppmo.gov.np before each procurement. Below NPR 5 lakhs: direct purchase permitted. Above threshold: quotation or open bidding required.

Q: Is the e-GP portal mandatory for all ICT procurement?	**A:** e-GP (bolpoatra.gov.np) is mandatory above specified thresholds. Using e-GP below the mandatory threshold is optional but recommended for transparency.
Q: Which PPMO document must be used for ICT goods bidding?	**A:** PPMO Standard Bidding Document (SBD) for goods — mandatory for ICT hardware procurement above threshold. Free download at ppmo.gov.np.
Q: What is the penalty for awarding a contract to a blacklisted vendor?	**A:** CIAA investigation finding, void contract, personal liability for the approving officer. Always verify vendor status at PPMO blacklist (ppmo.gov.np) before award — Template 1 (M5-T10) includes this check.

IT Official Action: ALWAYS check: (1) Is the vendor blacklisted? (ppmo.gov.np) (2) Is specification brand-neutral? (3) Is the methodcorrect for the value? (4) Is SBD used? (5) Is e-GP used if it is abovethe threshold? All five checks = Module 5, M5-T24 Red Flag Checklist.

Nepal Government Enterprise Architecture 2.0 (GEA 2.0)

नेपाल गभर्नमेन्ट इन्टरप्राइज आर्किटेक्चर | Technical Framework

Purpose: Mandatory blueprint for ALL government ICT systems — covering interoperability standards, hosting requirements, data ownership, security clearance, mandatory artifacts, and source code ownership. Non-compliance blocks IDMC VM provisioning.

Question IT Officials Ask	Key Provision / Legal Answer
Q: Which technical standard does GEA 2.0 mandate for inter-system communication?	**A:** REST/JSON APIs are mandatory for all data exchange between government systems. Proprietary, closed API standards are prohibited.
Q: Which framework mandates source code handover from vendors?	**A:** GEA 2.0: Government retains 100% ownership of all source code. Vendor must provide complete, documented source code and all build tools upon contract completion — or acceptance payment is withheld.
Q: Which framework requires GIDC hosting evaluation before commercial cloud?	**A:** GEA 2.0 + Data Center Directives 2081: GIDC (IDMC) hosting must be evaluated first. External hosting requires documented justification. Nepal data residency is mandatory.
Q: How many mandatory artifacts does GEA 2.0 require for every software project?	**A:** 9 artifacts: SRS, FRS, System Architecture, Database Design, API Specification, Test Plan, User Manual, Training Material, and Security Assessment — plus the VAPT Clearance Letter from NCSC.
Q: What is the pre-condition for IDMC VM/VPS provisioning?	**A:** GEA 2.0 Compliance Certificate from DoIT + NCSC VAPT Clearance Letter — both required before IDMC will provision VM/VPS hosting for any government system. (Module 7, Section 7.2)

IT Official Action: Include GEA 2.0 compliance checklist (F 3.1) in every procurement ToR. Verify GEA compliance at each payment milestone using Module 6, F 6.1. All systems must have a DoIT GEA Certificate before IDMC hosting.

Complete before any software procurement or deployment.

GEA 2.0 Compliance Checklist — verify architecture compliance before procurement or deployment	
Check	**Status**
System uses REST/JSON APIs, not a proprietary or closed format	[ ] Yes [ ] No
Hosted on GIDC/IDMC or a DoIT-approved facility — citizen data resides in Nepal	[ ] Yes [ ] No
Integrates with National ID (NID) for citizen authentication where the service requires identity verification	[ ] Yes [ ] No
WCAG 2.1 Level AA accessibility compliance verified	[ ] Yes [ ] No
All 9 GEA 2.0 mandatory artifacts (Module 6, Section 6.2) completed and on file	[ ] Yes [ ] No
DoIT GEA Certificate obtained before go-live	[ ] Yes [ ] No — STOP

IT Norms 2082 — ICT Rate Standards (MoCIT)

IT दर मापदण्ड २०८२ | Rate Standard / Regulation

Purpose: Mandatory monthly rate benchmarks for all ICT personnel roles used in government contracts. Also sets minimum qualification requirements. Must be applied to ALL ICT consulting budget estimates — verified cost estimates are the first anti-corruption gate in consulting procurement.

Question IT Officials Ask	Key Provision / Legal Answer
Q: Is IT Norms 2082 compliance mandatory or optional?	**A:** Mandatory for ALL government ICT consulting procurement. Using rates above IT Norms without written designated authority justification is a PPA violation and CIAA Investigation finding.
Q: What happens if we award a consulting contract above IT Norms rates?	**A:** CIAA Investigation finding. The contract may be declared void. The approving officer faces personal liability. Always document IT Norms rate comparison in the cost estimate (M5-T09 Worksheet).
Q: How do we find the current IT Norms rates for a specific ICT role?	**A:** Current rates are published at **mocit.gov.np**. VERIFY rates before each procurement — IT Norms are updated and new versions replace previous ones. Never rely on rates from a previous procurement year.
Q: Do IT Norms apply to equipment/ hardware procurement or only to consulting?	**A:** IT Norms apply to consulting/human resource roles only (Project Manager, Software Developer, Database Administrator, Systems Analyst, etc.). Hardware is procured under PPA goods thresholds.
Q: Which document must use IT Norms rates in the calculation?	**A:** M5-T09: IT Consulting Cost Estimation Worksheet — mandatory for every TCN (Technical Concept Note) involving consulting. Filed with the TCN before designated authority approval.

IT Official Action: BEFORE every consulting TCN: download current IT Norms from mocit.gov.np → complete M5-T09 worksheet → attach to TCN. Keep the rate download date-stamped as audit documentation.

Data Center and Cloud Services Directives 2081 डेटा सेन्टर तथा क्लाउड सेवा निर्देशिका २०८१ | Directive	
Purpose: Regulates where government data may be hosted and which vendors may provide hosting services — establishing GIDC-first policy, Nepal data residency requirements, and a mandatory DoIT vendor enlistment process.	
Question IT Officials Ask	**Key Provision / Legal Answer**
Q: Is GIDC/IDMC hosting mandatory for all new government systems?	**A:** GIDC must be evaluated as the first option. If GIDC capacity or technical suitability is insufficient, commercial hosting from DoIT-enlisted vendors is permitted — with documented justification.
Q: Can government data be hosted on international cloud services (AWS, Azure, GCP)?	**A:** Only if DoIT-enlisted to serve Nepal government AND data residency within Nepal is maintained. Hosting citizen data on international servers without Nepal data copies is prohibited.
Q: Which agency maintains the list of approved/enlisted data center vendors?	**A:** DoIT (Department of Information Technology) — doit.gov.np. Verify vendor enlistment status before any hosting contract. Non-enlisted vendors cannot be engaged.
Q: What must all hosting contracts include per the Directives?	**A:** Audit rights for government, Nepal data residency confirmation, security standards compliance, data portability clause (exit rights), and no vendor data use for any purpose other than hosting.
Q: What is the penalty for using non-enlisted hosting providers?	**A:** Void contract, CIAA Investigation finding, and personal liability. Always check DoIT enlistment list before procurement and include it in the Module 5 Red Flag Checklist (M5-T24).
IT Official Action: Before any hosting procurement: (1) Check IDMC/GIDC availability — Module 7 Section 7.2 (2) If GIDC not suitable, check DoIT enlisted vendors list at doit.gov.np (3) Include data residency clause in all hosting contracts.	

Complete before any data center or cloud hosting procurement.

Data Center Enlistment Checklist — pre-procurement compliance check	
Check	**Status**
Data center / cloud provider is enlisted with DoIT per the Data Center and Cloud Services Directives 2081	[ ] Yes [ ] No
Citizen data is hosted only within Nepal (data residency confirmed)	[ ] Yes [ ] No
Provider's current ISO 27001 / facility-tier certification is on file	[ ] Yes [ ] No
Contract SLA includes uptime, backup, and incident-response commitments	[ ] Yes [ ] No
Contract includes an exit/migration clause to avoid vendor lock-in	[ ] Yes [ ] No

National Cybersecurity Policy 2080

राष्ट्रिय साइबर सुरक्षा नीति २०८० | National Policy

Purpose: Establishes mandatory minimum security standards for all government ICT systems, requires NCSC VAPT before go-live for internet-facing systems, and mandates incident reporting to NCSC for all government cyber incidents.

Question IT Officials Ask	Key Provision / Legal Answer
Q: Which systems must undergo NCSC VAPT before going live?	**A:** All internet-facing government systems — citizen portals, web applications, APIs, and government websites. Also mandatory annually thereafter. VAPT is free for government bodies.
Q: What are the mandatory minimum encryption standards?	**A:** TLS 1.2 minimum for data in transit (all government websites must use HTTPS). AES-256 minimum for data at rest (encrypted databases for all PII). 2FA mandatory for administrator accounts.
Q: How quickly must cyber incidents be reported to NCSC?	**A:** Immediately for critical incidents (system compromises, ransomware, data breaches). Non-critical incidents within 72 hours. NCSC 24/7 hotline: +977-1-4200144.
Q: What constitutes a mandatory security incident report?	**A:** Any: unauthorized system access, data breach or exfiltration, ransomware or malware compromise, denial of service on government services, or social media account compromise.
Q: Does the Policy apply to social media accounts and SMS gateways?	**A:** Yes. Official government social media accounts and SMS gateway usage are covered. 2FA is mandatory on all official accounts. SMS gateway must be used only for official government notifications.

IT Official Action: VAPT before every go-live — contact NCSC at +977-1-4200144 and submit F 7.18 Annex I (Module 7). Post NCSC IP 202.45.145.183 in the server room — must be whitelisted before VAPT. Report all incidents within 72 hours.

Digital Nepal Framework 2.0 (DNF 2.0)

डिजिटल नेपाल ढाँचा २.० | National Policy/Framework

Purpose: Nepal's national digital transformation strategy establishing five pillars — Digital Government, Digital Infrastructure, Digital Economy, Digital Society, and Digital Public Infrastructure (DPI) — with specific targets for provincial and local government by 2085 BS.

Question IT Officials Ask	Key Provision / Legal Answer
Q: What is the DNF 2.0 digital government target for LGs by 2085 BS?	**A:** All citizen services available digitally through a single integrated platform (Nagarik App / one-stop portal) with NID authentication. Citizens should be able to access all government services without visiting an office.

Q: What is 'Digital Public Infrastructure (DPI)' per DNF 2.0?	**A:** The three foundational DPIs: National ID (NID) for citizen authentication, government digital payment systems (ConnectIPS), and unified data exchange infrastructure. All new LG systems must integrate with these DPIs.
Q: Does DNF 2.0 mandate Nagarik App integration for all LG services?	**A:** Yes. Priority citizen services (birth certificates, property tax, building permits) must be available via the Nagarik App . LGs register for integration through DoIT (Module 7, Section 7.1 Service 3).
Q: What is the DNF 2.0 requirement for data interoperability?	**A:** GEA 2.0 REST/JSON API compliance is mandatory to enable DNF 2.0 data exchange between government systems. No new system can be an isolated data silo.
Q: How does DNF 2.0 align with the E-Governance Maturity Index?	**A:** DNF 2.0 targets E-Governance Maturity Stage 4 (Transformation) by 2085 BS — integrated services, proactive delivery, and NID-based one-stop service access for all citizens.

IT Official Action: Integrate priority services with Nagarik App (Module 7, Section 7.1 Service 3). Include NID integration requirement in ALL new citizen portal ToRs. Register .gov.np domain and maintain GIWMS website per DNF 2.0.

National Artificial Intelligence Policy 2025 (2082 BS)

राष्ट्रिय कृत्रिम बुद्धिमत्ता नीति २०८२ | National Policy

Purpose: Establishes Nepal's framework for responsible AI adoption in government — with mandatory human oversight, bias testing, explainability requirements, Privacy Act 2075 compliance for citizen data, and designated authority sign-off for all government AI deployments.

Question IT Officials Ask	Key Provision / Legal Answer
Q: Can AI systems make final government decisions affecting citizens?	**A:** No. Human oversight is mandatory for all AI-assisted government decisions. Citizens must have the right to request human review of any AI-assisted decision (human-in-the-loop principle).
Q: Is bias testing required before deploying AI in government?	**A:** Yes. AI systems must be tested for demographic and algorithmic bias before deployment. Bias testing results must be documented and reviewed by the IT Official and designated authority.
Q: Does the Privacy Act 2075 apply to AI systems using citizen data?	**A:** Yes. AI systems processing citizen PII are fully subject to Privacy Act 2075 — requiring legal basis for data use, purpose limitation, data minimization, and security protection.
Q: Who must approve government AI deployments?	**A:** The designated authority must sign off before any AI system is procured or deployed (Module 1, Section 1.6 / Module 1, Section 1.6, F 1.3 AI Readiness Checklist). No AI deployment without documented designated authorization.

Q: Can commercial AI tools (ChatGPT, etc.) be used for government work?	**A:** With strict restrictions. Never input citizen PII, classified information, or sensitive government data into commercial AI tools — this would violate Privacy Act 2075 and potentially ETA 2063.

IT Official Action: Complete AI Readiness Checklist (F 1.3 / Module 1, Section 1.6) before any AI procurement. Document designated authority sign-off. Include AI Policy obligations in all AI vendor contracts: audit rights, bias testing, human oversight, data ownership.

e-Governance Blueprint 2082 (2025)

ई-गभर्नेन्स ब्लु प्रिन्ट २०८२| National Strategic Blueprint

Purpose: A national strategic blueprint designed to transform public service delivery into a seamless, transparent, and responsive digital ecosystem across all levels of government. It relies on seven strategic pillars, prioritizing shared digital public infrastructure, unified digital identity, the "Once-Only Principle", and secure data exchange platforms

Question IT Officials Ask	Key Provision / Legal Answer
Q: What is the "Once-Only Principle" (OOP) and how must local governments apply it??	**A:** Pillar 2 (Section 3.2.2): Citizens and businesses should not have to repeatedly provide demographic or personal data that the government has already collected. LGs must utilize data exchange platforms to reuse verified data, eliminating the need for citizens to submit physical copies repeatedly.
Q: How does the Blueprint structure IT governance implementation at the local level?	**A:** Pillar 1 (Section 3.1.1): It establishes a structured implementation framework across all three tiers of government. For local levels, this includes a Local Implementation Committee and a Local Project Management Office to ensure local projects align with national digital transformation directives.
Q: Are digital signatures going to be mandatory for government staff?	**A:** Pillar 3 (Section 3.3.4): Yes. To expand the scope of digital service delivery, the blueprint makes digital signatures mandatory for government employees and ensures they are provided free of cost as an integrated part of the National Identity Card (NID).
Q: How should LGs handle aging hardware and software systems?	**A:** Pillar 2 (Section 3.2.3): LGs must adhere to a Digital Life Cycle Policy combined with Legacy Management. This requires a defined lifecycle for hardware and software to ensure timely renewals, preventing cybersecurity vulnerabilities and maintaining service quality.
Q: How does the Blueprint address citizens who lack digital skills to use online LG portals?	**A:** Pillar 4 (Section 3.4.2): It mandates the establishment of Citizen Service Centers (नागरिकसेवाकेन्द्र) in partnership with provincial and local governments. These centers aim to boost digital literacy, reduce service costs, and ensure equitable access to digital governance.

Q: What is the legal standard for sharing data between different government systems?	A: Pillar 3 (Section 3.3.3): A secure Data Exchange Platform will be established within the bounds of privacy laws. It ensures non-repudiation, strict access management, and limits centralized access, ensuring data transfers between agencies are secure, authentic, and trackable.

IT Official Action: Align the Annual ICT Procurement Plan with the Blueprint's 7 pillars. Actively design new systems using the "Once-Only Principle", avoiding unnecessary redundant data collection. Prepare LG portals to interface with the national Data Exchange Platform and mandate digital signatures for internal approvals. Facilitate the creation of a Local Implementation Committee and coordinate with the E-Governance Board for major ICT initiatives.

3.5 Annual Legal Compliance Self-Assessment

वार्षिक कानूनी अनुपालन आत्म-मूल्याङ्कन

Complete this self-assessment annually — at the start of each fiscal year. Present results to the designated authority and IT Steering Committee if applicable. For any 'No' or 'Partial' result, create an action plan with a completion date.

#	Compliance Check / अनुपालन जाँच	Law / Instrument	Status	Action if No/Partial
1	Is an Information Officer formally designated and RTI proactive disclosures published on the GIWMS website (quarterly updates)?	RTI Act 2064	[ ] Yes [ ] No [ ] Partial	Designate officer; publish disclosures within 30 days
2	Are privacy notices displayed at ALL citizen data collection points (online forms and physical counters)?	Privacy Act 2075	[ ] Yes [ ] No [ ] Partial	Update all portals and counter signage within 14 days
3	Does the Citizen Charter include digital services with timeframes and is it published on the website?	Good Governance Act 2064	[ ] Yes [ ] No [ ] Partial	Update Citizen Charter to include all digital services
4	Is IT Norms 2082 applied to ALL ICT consulting budget estimates (M5-T09 completed and filed)?	IT Norms 2082	[ ] Yes [ ] No [ ] Partial	File M5-T09 worksheets retrospectively; apply going forward
5	Do all ICT procurement specifications use brand-neutral, performance-based requirements (no brand names)?	PPA 2063	[ ] Yes [ ] No [ ] Partial	Review all active ToRs; remove brand-specific requirements
6	Have all internet-facing government systems received NCSC VAPT clearance before go-live and within the last 12 months?	Cybersecurity Policy 2080; GEA 2.0	[ ] Yes [ ] No [ ] Partial	Schedule VAPT with NCSC (+977-1-4200144) for non-compliant systems
7	Does every ICT vendor with access to citizen data have a signed NDA (M5-T16) on file?	Privacy Act 2075	[ ] Yes [ ] No [ ] Partial	Obtain signed NDAs from all vendors before next access
8	Has the data center/hosting vendor for all government systems been verified as DoIT-enlisted?	DC Directives 2081	[ ] Yes [ ] No [ ] Partial	Verify all hosting vendors at doit.gov.np; exit non-compliant vendors

#	Compliance Check / अनुपालन जाँच	Law / Instrument	Status	Action if No/Partial
9	Is citizen data of all systems hosted within Nepal (no international-only storage)?	DC Directives 2081; GEA 2.0	[ ] Yes [ ] No [ ] Partial	Migrate non-compliant systems to IDMC/GIDC or DoIT-enlisted Nepal data centers
10	Do all new system procurement ToRs include GEA 2.0 compliance and source code ownership requirements?	GEA 2.0	[ ] Yes [ ] No [ ] Partial	Update ToR templates to include GEA 2.0 requirements (Module 6, F 6.1)
11	Does the Citizen Charter and website comply with WCAG 2.1 Level AA accessibility standards?	IT Policy 2015	[ ] Yes [ ] No [ ] Partial	Schedule WCAG accessibility audit; add to next system UAT checklist
12	Has any AI system been deployed without documented designated authority approval and F 1.3 AI Readiness Checklist?	AI Policy 2025	[ ] Yes [ ] No [ ] Partial	Obtain retroactive designated authority approval; complete F 1.3 for all deployed AI tools

Self-Assessment Completed by (IT Official): _____ Date: _____ Fiscal Year: _____	Reviewed by (designated authority): _____ Date: _____ Signature: _____

See Also (📌):

All Acts: lawcommission.gov.np · IT Norms, AI Policy, DNF 2.0: mocit.gov.np · DC Directives: doit.gov.np · Cybersecurity Policy: ncsc.gov.np · Procurement thresholds: ppmo.gov.np · DoIT Enlistment: doit.gov.np · Detailed compliance procedures: Module 4 (operations), Module 5 (procurement), Module 6 (system development), Module 7 (government agency coordination).

MODULE 4 ICT OPERATIONS, SECURITY, AND BUSINESS CONTINUITY

IT Governance · Incident & Problem · Change & Service Desk · Operations Rhythm · Asset Management · Physical Security · Information Security · Security Incident & VAPT · Backup & BC/DR · Social Media · Staff Handover

Incident/Problem	Change/Service Desk	Asset/Security	Backup/BCP

Scope: Day-to-day operational procedures — incident and problem management, change control, asset lifecycle, security, backup, and business continuity — covering Sections 4.1–4.11.

Target: IT Officials running daily ICT operations at the provincial and local government level.

: IT Governance · ITSM (Incident, Problem, Change, Service Desk) · Daily/Weekly/Monthly Operations · Asset Management · Physical and Environmental Security · Information Security Controls · Security Incident Response · VAPT · Backup · Business Continuity/DR · Social Media · Staff Handover

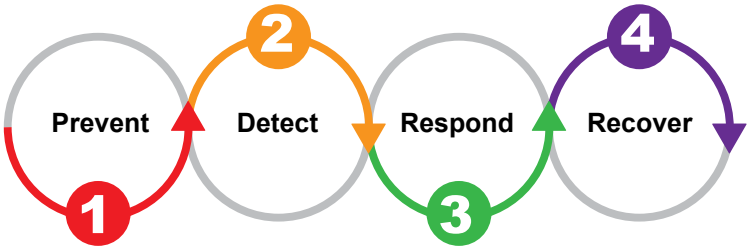
Tools: 28 operational tools — F 4.1 through F 4.12.3. All forms are ready to print and use. Condensed per government feedback: redundancies removed, similar sections grouped.

Legal basis: ISO/IEC 27001:2022 · ITIL 4 · National Cybersecurity Policy 2080 · Individual Privacy Act 2075 · Good Governance Act 2064 · ETA 2063

Cross-references: Module 3 — Legal basis for each obligation. Module 5 — Procurement of security services, VAPT contracts. Module 6 — Security requirements in system development. Module 7 — NCSC, IDMC, DoIT coordination.

Module 4 is the operational core of the ICT Technical Handbook — the module that ICT officials will reference most frequently in their day-to-day work. It translates the governance frameworks of Module 2 and the legal requirements of Module 3 into concrete, step-by-step procedures for managing ICT operations, protecting information assets, maintaining service continuity, and ensuring accountability in staff transitions. Every SOP, checklist, and template in this module is designed to be immediately usable by ICT Officials.

The Operations, Security, and Continuity Cycle



4.1 IT Governance / IT सुशासन

IT Governance is the framework through which the designated authority (for eg: designated authority in the case of LGs) directs and monitors ICT — setting direction, approving budgets, and holding the IT Official accountable for results. The designated authority governs; the IT Official manages. This distinction protects both: the designated authority has documented oversight; the IT Official has documented authority.

Governance Layer	Role	Key Actions
Govern (LGs Scenario: designated authority)	Sets direction — approves ICT policy, budget, and major procurement decisions	Chair quarterly IT Governance review. Approve Annual ICT Plan. Review KPI report. Approve significant changes.
Manage (LGs Scenario: IT Official)	Implements direction — operates systems, manages incidents, executes procurement	Implement approved SOPs. Report incidents, performance, and compliance to designated authority. Prepare IT Governance Self-Assessment (F 4.2) annually.

ICT Decision Log — Record all significant ICT decisions for governance and audit

Date	Decision Reference No.	Decision / Action Approved	Approved By	IT Official Action	Status
[Date]	DL-[Year]-[Seq]	[Describe the decision — e.g., 'Approved Annual ICT Budget FY 2082/83']	[Designated Authority/ designated authority / IT Steering Committee]	[Action to be taken]	[ ] Open [ ] Done
[Date]	DL-[Year]-[Seq]				[ ] Open [ ] Done
[Date]	DL-[Year]-[Seq]				[ ] Open [ ] Done

Completed by: _____ Designation: _____ Date: _____

IT Governance Self-Assessment — Conduct annually; present results to IT Steering Committee	
Governance Check	Status
Is a quarterly IT Steering Committee meeting conducted with documented minutes?	[ ] Y [ ] N [ ] P
Is an Annual ICT Plan prepared and approved by the designated authority before the fiscal year starts?	[ ] Y [ ] N [ ] P
Are all significant ICT decisions recorded in the ICT Decision Log (F 4.1)?	[ ] Y [ ] N [ ] P
Are ICT KPIs (incident resolution rate, SLA compliance, backup success rate) tracked and reported to designated authority quarterly?	[ ] Y [ ] N [ ] P
Is an IT risk register maintained and reviewed at each Steering Committee meeting?	[ ] Y [ ] N [ ] P
Are all ICT expenditures aligned with the approved Annual ICT Plan and procurement procedures?	[ ] Y [ ] N [ ] P
Is the Information Security Policy current, designated auhtority-approved, and communicated to all staff?	[ ] Y [ ] N [ ] P
Has an annual ISMS internal review (Module 2, F 2.1) been conducted and documented?	[ ] Y [ ] N [ ] P
Are all ICT contracts and procurement records audit-ready and available to CIAA/ OAG?	[ ] Y [ ] N [ ] P
Is the Business Continuity Plan current, tested, and known to key staff?	[ ] Y [ ] N [ ] P
Completed by: _____ Designation: _____ Date: _____	

4.2 Incident and Problem Management / घटना तथा समस्या व्यवस्थापन

Incident Management restores normal service as quickly as possible. Problem Management finds and fixes the root cause so the incident does not recur. Every incident is logged — without exception. Incidents recurring more than twice automatically trigger a Problem Record.

Incident Priority Matrix

Priority	Definition	Examples in Province/LG Context	Response Target	Resolution Target
P1 — Critical	Core citizen service or critical government system completely offline — no workaround available	Civil registration system down; SUTRA/financial system offline; ransomware detected; complete internet loss; server room fire/ flood	IT Official on-site or remote response: 15 minutes	Service restored or DR activated: 4 hours
P2 — High	Major service degraded or key system offline — workaround available or partial service only	Revenue portal slow or intermittent; backup failure; network switch down affecting several users; GIOMS inaccessible	Response: 1 hour	Resolution: 8 hours
P3 — Medium	Single user or single function affected — non-critical to citizen services	Single staff member cannot log in; one printer offline; email attachment issue; minor display error	Response: 4 business hours	Resolution: 2 business days

Priority	Definition	Examples in Province/LG Context	Response Target	Resolution Target
P4 — Low	Service request or information query — no service disruption	New user account creation request; software installation query; training request; information request	Response: 1 business day	Resolution: 5 business days

SOP 4.2.1 | Incident Management

SOP 4.2.1 | Incident Management	
Purpose	Restore normal ICT service after an unplanned interruption. All incidents logged without exception — including self-resolved ones. P1/P2 incidents notified to designated authority.
Steps	1. **Detect and log:** As soon as any incident is identified — by IT Official or reported by any staff — open a new row in the Incident Log (F 4.3). Record: date/time; reported by; system affected; description. Assign a sequential Incident Number. 2. **Categorize and prioritize:** Use the Priority Matrix above to assign P1/P4. If in doubt between two levels, assign the higher (more urgent) level. 3. **Notify:** P1 and P2: Notify the designated authority immediately by phone. P3/P4: Log only — notify designated authority in weekly summary. For all P1 incidents affecting citizen services: notify PPSU ICT Unit (Module 7, Section 7.5). 4. **Diagnose and respond:** Identify cause. Apply a workaround if available to restore partial service. For P1: Escalate to vendor/IDMC/PPSU if not resolved within 1 hour. For security incidents: execute SOP 4.8.1 simultaneously. 5. **Resolve and verify:** Confirm service is fully restored and functioning. Test with affected users before closing the incident. Record: cause; action taken; resolved by; resolution date/time in F 4.3. 6. **Review for recurrence:** If this incident has occurred before for the same system or cause: raise a Problem Record (F 4.6) immediately. Do not wait for a third occurrence. 7. **Close and update SLA:** Close the Incident Log row. Calculate actual response and resolution times. Flag any SLA breach for designated authority reporting and vendor SLA penalty deduction (if applicable).

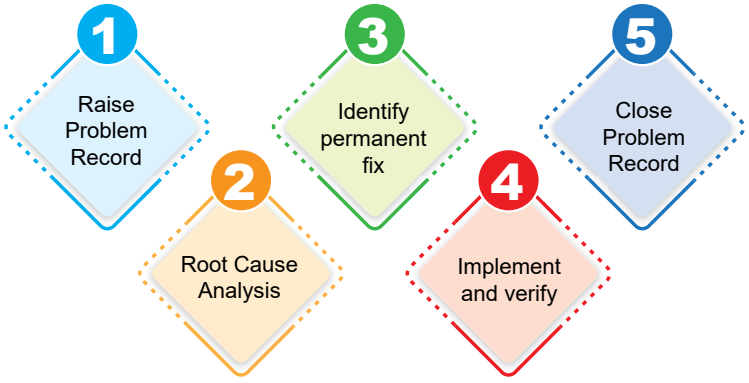
F 4.3 |Incident Log — Log ALL incidents immediately. Review open incidents daily.

Inc. No.	Date/ Time	Reported By	System / Service	Priority	Description	Action Taken	Resolved By	Resolution Time	Status
INC-[Yr]-001	[Date/ Time]	[Name]	[System]	[ ] P1 [ ] P2 [ ] P3 [ ] P4	[Brief description of issue]	[Action taken / workaround applied]	[IT Official / Vendor]	[Date/Time]	[ ] Open [ ] Resolved

F 4.3 |Incident Log — Log ALL incidents immediately. Review open incidents daily.									
INC-[Yr]-002				[ ] P1 [ ] P2 [ ] P3 [ ] P4					[ ] Open [ ] Resolved
INC-[Yr]-003				[ ] P1 [ ] P2 [ ] P3 [ ] P4					[ ] Open [ ] Resolved
Completed by: _____ Designation: _____ Date: _____									

F 4.4 | Incident Priority Quick Reference Card — Print, laminate, and post at IT Official workstation				
Priority	Criteria	First Action	Who to Notify	Response Target
P1 CRITICAL	Core service offline; ransomware; complete connectivity loss; no workaround	Isolate the affected system. Phone designated authority NOW. Start DR if needed.	Designated Authority immediately + PPSU ICT Unit + NCSC if cyber incident	15 min response / 4 hr resolution
P2 HIGH	Major service degraded; key backup failure; multiple users affected; workaround available	Log incident. Phone designated authority. Engage vendor/IDMC if not resolving.	Designated Authority by phone within 30 min	1 hr response / 8 hr resolution
P3 MEDIUM	Single user or function affected; non-critical; workaround possible	Log incident. Investigate. Schedule fix.	Include in weekly Designated Authoritysummary	4 hr response / 2 days resolution
P4 LOW	Service request; query; no disruption	Log as service request. Schedule action.	Include in monthly Designated Authority report	1 day response / 5 days resolution
Completed by: _____ Designation: _____ Date: _____				

SOP 4.2.2 | Problem Management



Problem Management	
Purpose	Identify and eliminate the root cause of recurring incidents. A Problem Record is raised when: (a) any incident recurs more than twice; or (b) a single P1 incident occurs and root cause is unknown.

Steps	
	1. **Raise Problem Record:** Open F 4.6 (Problem Record). Link to all related Incident numbers from F 4.3. Record: affected system; first occurrence date; frequency of recurrence; citizen impact. 2. **Root Cause Analysis:** Apply the 5 Whys technique (F 4.5). Ask 'Why did this happen?' five times. Do not stop at the surface-level cause. Record each 'Why' in F 4.5. The 5th answer is usually the root cause. 3. **Identify permanent fix:** Document the specific technical or procedural change that will prevent recurrence. If the fix requires a system change: raise a Change Request (SOP 4.3.1). If training is the fix: schedule immediately. 4. **Implement and verify:** Implement the fix. Monitor for 30 days to confirm the incident does not recur. If it recurs: repeat from Step 2 — the root cause was not correctly identified. 5. **Close Problem Record:** When 30 days have elapsed with no recurrence: close F 4.4. Update the ISMS Risk Register if the problem revealed a systemic security weakness.

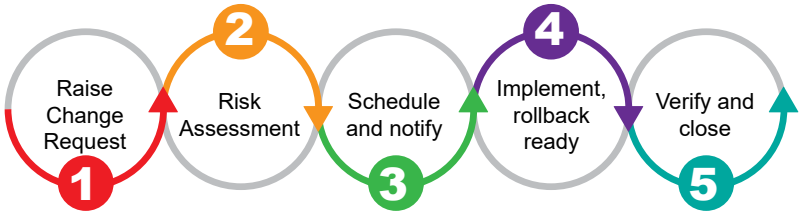
F 4.6 | Problem Record — Raise when any incident recurs more than twice	
Field	**Details**
Problem Record No.:	PRB-[Year]-[Seq]
Raised by IT Official:	[Name] Date: [Date] Linked Incident Nos.:
Affected System/Service:	[System name and description]
Frequency of Recurrence:	[Number of times in past [Period]] First Occurrence: [Date]
Citizen/User Impact:	[Describe operational impact — who is affected and how]
Root Cause (5 Whys result):	[Attach F 4.5 — 5 Whys Worksheet]
Permanent Fix Identified:	[ ] System change (raise Change Request F 4.7) [ ] Training [ ] Procedure update [ ] Vendor action
Target Fix Date:	[Date] Responsible Person: [Name]
Verification (30 days post-fix):	[ ] Incident did NOT recur in 30 days — CLOSE [ ] Incident recurred — REOPEN and repeat RCA
Problem Record Status:	[ ] Open [ ] Under Investigation [ ] Fix Implemented [ ] Closed
Completed by: _____ Designation: _____ Date: _____	

F 4.5 | Root Cause Analysis Worksheet (5 Whys) — Complete for every Problem Record		
Step	**Question**	**Answer (What you observed)**
Problem Statement	Describe the incident/problem in one clear sentence:	
Why 1	Why did [problem statement] happen?	[Answer 1]
Why 2	Why did [Answer 1] happen?	[Answer 2]
Why 3	Why did [Answer 2] happen?	[Answer 3]
Why 4	Why did [Answer 3] happen?	[Answer 4]
Why 5 — ROOT CAUSE	Why did [Answer 4] happen?	[ROOT CAUSE — this is what the permanent fix must address]
Permanent Fix	What specific action will prevent the root cause from occurring again?	[Describe the fix: system change / training / vendor action / procedure update]
Completed by: _____ Designation: _____ Date: _____		

4.3 Change Management and Service Desk / परिवर्तन व्यवस्थापन तथा सेवा डेस्क

Change Management ensures every modification to an ICT system is assessed, approved, and scheduled before implementation — preventing the most common cause of self-inflicted service outages. The Service Desk is the single point of contact for all IT requests and incidents — it creates the audit trail and ensures nothing is missed.

SOP 4.3.1 | Change Enablement

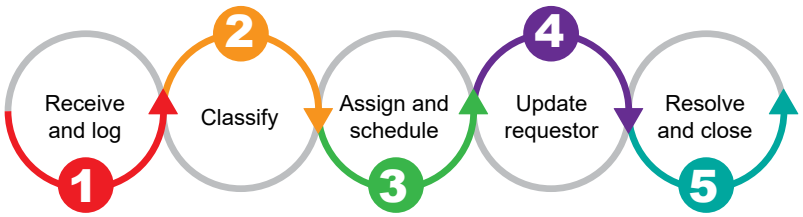


SOP 4.3.1 | Change Enablement — ICT Change Management	
Purpose	Assess, authorize, and safely implement all changes to ICT systems and services. All changes — however minor — require a Change Request. Emergency patches follow an expedited procedure.
Steps	1. **Raise Change Request:** IT Official completes F 4.7 (Change Request Form) for any proposed change to a system, configuration, software, or infrastructure. Classify: Standard (routine, pre-approved), Normal (requires review), or Emergency (critical security patch). 2. **Risk Assessment:** For Normal and Emergency changes: assess the risk — What could go wrong? What is the rollback plan if the change fails? Document in F 4.7. Changes with High or Critical risk require designated authority sign-off. 3. **Schedule and notify:** Schedule the change during the designated maintenance window (Sunday night or public holiday — outside government business hours where possible). Notify all affected users at least 24 hours in advance. 4. **Test in non-production (if available):** If a test or staging environment exists, implement and test the change there first. Verify the change achieves the intended outcome without side effects. 5. **Implement with rollback plan ready:** Implement the change. Have the rollback plan actively prepared — if the change fails, the IT Official must be able to restore previous state within the maintenance window. 6. **Verify and close:** After implementation: verify all affected services are functioning. Test with at least one end user. Close the Change Request in F 4.7. If the change caused an incident: raise F 4.3 immediately.

Change Request Form — Complete BEFORE implementing any system change	
Field	Details
Change Request No.:	CHG-[Year]-[Seq] Submitted by: [Name] Date: [Date]
Change Title:	[Brief descriptive title — e.g., 'Apply Windows security patch KB xxxxxx to all staff PCs']
Affected System/ Service:	[Name of system(s) affected]

Change Request Form — Complete BEFORE implementing any system change	
Change Type:	[ ] Standard (routine, pre-approved procedure) [ ] Normal (requires review and approval) [ ] Emergency (critical security patch — expedited)
Description of Change:	[Describe what will be done, how, and by whom]
Reason / Business Justification:	[Why is this change needed? What risk does it address or benefit does it deliver?]
Risk Assessment:	Impact if change fails: [ ] Low [ ] Medium [ ] High [ ] Critical Rollback plan: [Describe exactly how to restore previous state if change fails]
Implementation Date/ Time:	[Date] Maintenance window: [Time from] to [Time to]
User Notification:	[ ] Affected users notified at least 24 hours in advance Method: [Email / Notice / Verbal]
Post-Implementation Verification:	[ ] All services verified functioning after change [ ] End-user test confirmed [ ] Change caused incident → CHG-[Seq] linked to INC-[Seq]
IT Official Approval:	Signature: _____ Date: _____
Designated authority Approval (High/Critical risk):	Signature: _____ Date: _____
Completed by: _____ Designation: _____ Date: _____	

SOP 4.3.2 | Service Desk Operation



Service Desk Operation — Single Point of Contact	
Purpose	The Service Desk is the designated single point of contact (SPOC) for all IT-related requests and incident reports from all staff. Its purpose is to ensure every request is logged, assigned, tracked, and resolved — creating the audit record for OAG compliance.
Steps	1. **Receive and log:** Every IT contact (incident report, service request, query) received by the IT Official — by phone, email, in-person, or written note — is logged in the Service Desk Daily Log (F 4.8) on the same day it is received. No exceptions. 2. **Classify:** Is this an Incident (unplanned service disruption) → log in Incident Log (F 4.3) and apply SOP 4.2.1. Or a Service Request (planned action — new account, new software, information) → log in F 4.8 and schedule. 3. **Assign and schedule:** Assign a target resolution date based on priority (P1–P4 for incidents; agreed service levels for requests). For requests requiring procurement or vendor action: link to the relevant process.

Steps	4. **Update requestor:** For P1/P2 incidents: update affected users proactively at least every 2 hours until resolved. For service requests: confirm receipt within 1 business day and provide expected completion date. 5. **Resolve and close:** On completion: confirm with the requestor that the incident is resolved or service request is fulfilled. Record completion date and resolution details in F 4.8. Close the log entry.

F 4.8 | Service Desk Daily Log — Log EVERY IT contact on the day it is received

Ref No.	Date	Contact (Name/Dept)	Type	Description	Assigned To	Target Date	Status
SD-[Yr]-001			[ ] Incident [ ] Request				[ ] Open [ ] Done
SD-[Yr]-002			[ ] Incident [ ] Request				[ ] Open [ ] Done
SD-[Yr]-003			[ ] Incident [ ] Request				[ ] Open [ ] Done
SD-[Yr]-004			[ ] Incident [ ] Request				[ ] Open [ ] Done
SD-[Yr]-005			[ ] Incident [ ] Request				[ ] Open [ ] Done

Completed by: _____ Designation: _____ Date: _____

4.4 ICT Operations Rhythm — Daily, Weekly, and Monthly Checklists

ICT सञ्चालन तालमेल — दैनिक, साप्ताहिक र मासिक जाँच सूचीहरू

The three checklists below replace three separate documents in the submitted draft. They cover the same content, grouped by frequency for easier day-to-day use. The IT Official signs each checklist on completion. Signed copies are filed monthly for OAG audit readiness.

F 4.9 | Combined ICT Operations Checklist — Daily, Weekly, and Monthly Tasks

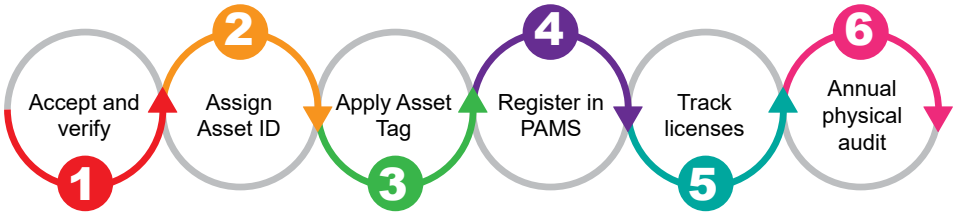
DAILY CHECKS (Complete every working day — Sunday–Friday)	Status
Check all critical servers are online and responding (ping or dashboard). Record any anomaly in Incident Log (F 4.3).	[ ] Done [ ] Issue — see INC-
Verify backup jobs from the previous night completed successfully. Check backup software logs.	[ ] Done [ ] Failed — see INC-
Check UPS battery status and network connectivity. Verify the internet link is active and stable.	[ ] Done [ ] Issue — see INC-
Review the Service Desk Daily Log (F 4.8) for any open P1 or P2 incidents from the previous day.	[ ] Done [ ] Issue — see INC-
Verify power supply, CCTV, and server room temperature are within normal range.	[ ] Done [ ] Issue — see INC-

F 4.9 | Combined ICT Operations Checklist — Daily, Weekly, and Monthly Tasks	
DAILY CHECKS (Complete every working day — Sunday–Friday)	Status
Check for new NCSC cybersecurity alerts or advisories at ncsc.gov.np.	[ ] Done [ ] Issue — see INC-
WEEKLY CHECKS (Complete every Sunday morning before office hours)	Status
Review all open incidents in Incident Log (F 4.3). Escalate any unresolved P1/P2. Identify recurring incidents for Problem Record (F 4.6).	[ ] Done [ ] Escalation needed
Verify all user accounts are active and appropriate. Check for any accounts of departed staff that have not been disabled.	[ ] Done [ ] Action taken:
Test at least one backup restoration — restore a single file from the previous day's backup. Log results in F 4.11.	[ ] Done [ ] Failed — see INC-
Check software patch status. Apply any Critical or High patches released in the past 7 days after completing Change Request (F 4.7).	[ ] Done [ ] Pending patches:
Update the Service Catalogue or System Inventory if any system changes occurred during the week.	[ ] Done [ ] No changes
Review the Service Desk Daily Log (F 4.8) for the week. Prepare a brief weekly ICT summary for designated authority if required.	[ ] Done
MONTHLY CHECKS (Complete in the first week of each month)	Status
Complete Physical Security Checklist (F 4.10). File signed copy.	[ ] Done
Complete User Account Management Checklist (F 4.12). Disable any accounts identified as unnecessary.	[ ] Done [ ] Accounts disabled:
Review the Patch Management Schedule (F 4.13). Verify all patches rated Medium and above have been applied.	[ ] Done [ ] Outstanding:
Review Asset Register (F 4.14) for accuracy. Check for new assets not yet registered or tagged.	[ ] Done [ ] New items added:
Review Software License Tracker (F 4.15). Flag any licenses expiring within 90 days for renewal planning.	[ ] Done [ ] Expiring soon:
Conduct Social Media Account Security Review (F 4.22) for all official government social media accounts.	[ ] Done
Prepare and submit monthly SLA Performance Report to designated authority: Incident volumes · Resolution rates · Backup success rate · Patch compliance rate.	[ ] Done
Review BCP/DR Emergency Contact List (F 4.21) for accuracy — update any changed contact details.	[ ] Done [ ] Updates made
Completed by: _____ Designation: _____ Date: _____	

4.5 ICT Asset Management / ICT सम्पत्ति व्यवस्थापन

Every government-owned ICT device, software license, and peripheral must be registered in the ICT Asset Register (F 4.14) and tagged before it enters service. Unregistered assets cannot be insured, maintained under AMC, or properly decommissioned — and create OAG audit findings. PAMS registration within 7 working days of acceptance is mandatory (Module 3, Section 3.3.7).

SOP 4.5.1 | ICT Asset Registration



ICT Asset Registration and Tracking	
Purpose	Register and track all government ICT assets from procurement to disposal. No ICT asset enters service without an Asset Register entry and a physical asset tag.
Steps	1. **Accept and verify:** On delivery of any ICT asset, complete the System Acceptance Testing procedure (Module 5, Section 5.8). Verify COA stickers, quantities, and specifications before signing the Acceptance Certificate. 2. **Assign Asset ID:** Assign a unique Asset ID in the format: LG/[Office Code]/[Category]/[Year]/[Seq] — e.g., WMN/PC/2082/001 for the first computer at Waling Municipality in 2082. Record in F 4.14. 3. **Apply Asset Tag:** Affix a physical asset tag (F 4.14-T) with the Asset ID to the device in a visible location. For computers: attach to the side of the case. For monitors: attach to the back panel. 4. **Register in PAMS:** Register all accepted hardware in PAMS (Property and Asset Management System) within 7 working days of acceptance. Record the PAMS entry reference number in F 4.14. 5. **Track software licenses:** Add all software licenses, subscriptions, and annual maintenance contracts to the Software License Tracker (F 4.15). Set calendar reminders for renewal 90 days before expiry. 6. **Annual physical audit:** Every Shrawan (July–August), conduct a physical inventory check — verify every item in F 4.14 is present, tagged, and in the recorded location. Update status for items that have been relocated, damaged, or disposed of.

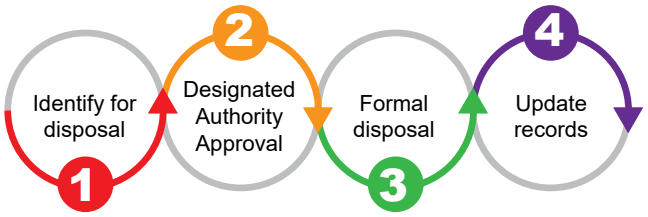
ICT Asset Register — Maintain for ALL government ICT assets

Asset ID	Item Description	Make/ Model	Serial No.	Location	Procurement Date	Warranty Expiry	PAMS No.	Condition	Status
Asset ID	[e.g., Desktop Computer]	Make/ Model	[S/N]	[Office/ Room]	[Date]	[Date]	PAMS No.	[ ] Good [ ] Repair [ ] Poor	[ ] Active [ ] Disposed [ ] Lost
Asset ID								[ ] Good [ ] Repair [ ] Poor	[ ] Active [ ] Disposed [ ] Lost
Asset ID								[ ] Good [ ] Repair [ ] Poor	[ ] Active [ ] Disposed [ ] Lost

Completed by: _____ Designation: _____ Date: _____

Software License Tracker — Update when any license is purchased, renewed, or expires								
Software Name	License Type	No. of Seats/Users	Vendor	License Key / Ref	Purchase Date	Expiry Date	Renewal Cost (NPR)	Action
Software	[ ] Perpetual [ ] Annual [ ] Monthly	[No.]	Vendor	[Key/Ref]	[Date]	[Date]	NPR [Amount]	[ ] Renew [ ] Replace [ ] OK
[Software]	[ ] Perpetual [ ] Annual [ ] Monthly							[ ] Renew [ ] Replace [ ] OK
[Software]	[ ] Perpetual [ ] Annual [ ] Monthly							[ ] Renew [ ] Replace [ ] OK
Completed by: _____ Designation: _____ Date: _____								

SOP 4.5.2 | ICT Asset Disposal



SOP 4.5.2 | ICT Asset Disposal and Secure Decommissioning	
Purpose	Securely decommission ICT assets at end of life. Informal disposal of ICT equipment containing citizen data is a Privacy Act 2075 violation and an OAG audit finding.
Steps	1. **Identify for disposal:** IT Official identifies assets for disposal based on: age (computers >5 years); irreparable damage; end of warranty and uneconomic to repair; replaced by newer procurement. Record in F 4.16 Disposal Checklist. 2. **Data sanitization — MANDATORY FIRST STEP:** Before any physical disposal: wipe all storage devices using approved methods (NIST 800-88 standard where possible). For HDDs: minimum 3-pass overwrite using free tools (DBAN, Eraser). For SSDs: secure erase command. For smartphones/tablets: factory reset + verified account removal. Generate a written wiping certificate signed by an IT Official. 3. **Designated Authority Approval:** Submit the Disposal Checklist (F 4.16) with the wiping certificate to the designated authority for approval. No asset may leave government premises without written designated authority approval. 4. **Formal disposal:** Options in order of preference: (1) Transfer to another government office via official handover; (2) Public auction through PPMO-compliant process; (3) Responsible e-waste disposal through registered local vendors. Document the disposal method and obtain receipt. 5. **Update records:** Remove the disposed asset from F 4.14 (Asset Register). Mark as 'Disposed' with disposal date and method. Update PAMS. File the completed F 4.16 with the wiping certificate in the asset disposal record.

Asset Disposal Checklist — Complete for every asset disposal. Designated authority sign-off required.	
Field	Details
Asset ID(s):	[List all Asset IDs being disposed]
Item Description:	[Description of each item]
Reason for Disposal:	[ ] Age/Obsolescence [ ] Beyond Economic Repair [ ] Replaced by New Asset [ ] Other: ___
MANDATORY — Data Sanitization:	[ ] Storage device wiped (3-pass overwrite / secure erase) [ ] Wiping Certificate generated and attached
[ ] Factory reset completed (mobile devices)	[ ] All government accounts removed from device
Disposal Method:	[ ] Transfer to another government office (Office: _____) [ ] Public auction [ ] E-waste disposal (Vendor: _____)
Disposal Date:	[Date] Disposed by: [IT Official Name]
Designated Authority Approval:	Signature: _____ Date: _____ (MANDATORY — no disposal without this)
PAMS / Asset Register Updated:	[ ] Asset marked 'Disposed' in F 4.14 [ ] PAMS record updated [ ] Disposal record filed
Completed by: _____ Designation: _____ Date: _____	

F 4.17 | Infrastructure Catalogue — Servers, Network Devices, and Software Systems Inventory (annual update)				
Item	Type	Location/Hosting	Owner/Vendor	Last Verified
[Server name]	Physical / VM / GIDC	[Server room / GIDC]	[IT Official / Vendor]	[Date]
[Network device]	Switch / Router / Firewall	[Location]	[Owner]	[Date]
[Software system]	Application / Database	[Hosting location]	[Vendor/in-house]	[Date]

4.6 Physical and Environmental Security / भौतिक तथा वातावरणीय सुरक्षा

The server room is the single highest-risk physical location in any LG office — it contains the systems and data that underpin all citizen services. Physical security prevents the most common non-cyber threats: unauthorized access, power failure, fire, and environmental damage. The monthly physical security checklist (F 4.10) is an OAG audit compliance document.

Physical Security Checklist — Complete monthly. Filed signed copy kept for audit.	
SERVER ROOM AND ICT INFRASTRUCTURE	Status
Is the server room door locked at all times? Is the key/access card held by the IT Official and one named backup holder only?	[ ] Yes [ ] No — Action:
Is the Server Room Entry Log (F 4.11) in place and has every visitor signed in and out since last month?	[ ] Yes [ ] No — Action:

Physical Security Checklist — Complete monthly. Filed signed copy kept for audit.	
SERVER ROOM AND ICT INFRASTRUCTURE	Status
Is the server room temperature within the safe operating range (18–27°C)? Record: ___°C	[ ] Yes [ ] No — Action:
Is the server room free from water leaks, flooding risk, or moisture above 70% relative humidity?	[ ] Yes [ ] No — Action:
Is the CCTV camera in the server room operational and recording to a separate secured location?	[ ] Yes [ ] No — Action:
Is the UPS functional, battery health verified, and estimated backup duration confirmed adequate for controlled shutdown?	[ ] Yes [ ] No — Action:
Is the fire suppression equipment (extinguisher or suppression system) present, inspected, and within its service date?	[ ] Yes [ ] No — Action:
Are all server rack cables managed and labelled? Is there no obstruction to airflow within the rack?	[ ] Yes [ ] No — Action:
Is the generator (if present) tested within the last 3 months and fuel supply adequate for 72-hour operation?	[ ] Yes [ ] No — Action:
OFFICE AND WORKSTATION SECURITY	Status
Are all staff workstations set to auto-lock after a maximumof 10 minutes of inactivity?	[ ] Yes [ ] No — Action:
Are any staff workstations left unlocked or unattended with sensitive data visible? (Conduct spot check)	[ ] None observed [ ] Issues found — Action:
Are printed documents containing citizen PII properly secured in locked cabinets — not left on desks?	[ ] Yes [ ] No — Action:
Is the office CCTV (if installed) operational and recording? Is footage stored for a minimumof 30 days?	[ ] Yes [ ] N/A [ ] No — Action:
Are visitor access procedures in place for office areas handling citizen data? Are visitors escorted?	[ ] Yes [ ] No — Action:
Completed by: _____ Designation: _____ Date: _____	

F 4.11 |Server Room Entry Log — Every entry and exit must be recorded. Leave in the server room.

Date	Name	Organization / Dept.	Purpose of Visit	Authorised By	Time In	Time Out	IT Official Supervised?
[Date]	[Name]	[Org]	[Purpose]	[IT Official Name]	[HH:MM]	[HH:MM]	[ ] Yes [ ] No
							[ ] Yes [ ] No
							[ ] Yes [ ] No
							[ ] Yes [ ] No
Completed by: _____ Designation: _____ Date: _____							

4.7 Information Security Operations / सूचनासुरक्षासञ्चालन

Information security operations translate the ISO 27001 ISMS (Module 2, Section 2.2) and the Information Security Policy into daily actions. The three tools in this section — User Account Management, Patch Management, and the Baseline Security Controls table — are the primary defences against the most common threats in Gandaki Province LG offices.

Baseline Security Controls — Minimum Required Government Offices

Control	Requirement	Frequency	Evidence for Audit
Least Privilege Access	Each staff member has access only to the systems and data required for their specific role. No shared or generic admin accounts.	Review monthly (F 4.12). Revoke excess access immediately.	Signed F 4.12 User Account Review on file
Two-Factor Authentication (2FA)	2FA mandatory for: all administrator accounts; all remote access (VPN); all accounts with access to citizen PII.	Verify at each new account creation and monthly review.	2FA configuration screenshot or vendor confirmation
Password Policy	Minimum 12 characters; mixture of upper/lower case, numbers, and symbols; no reuse of last 12 passwords; change required every 90 days.	Enforce through system policy where possible. Manual check in F 4.12 monthly.	System password policy settings documented
Malware Protection	Antivirus/anti-malware installed, active, and set to auto-update daily on all devices. No manual update dependency.	Verify auto-update status weekly in F 4.9 (Operations Checklist).	Antivirus dashboard showing update status
Encryption	All citizen PII: encrypted in transit (HTTPS/TLS 1.2+) and at rest (AES-256 or equivalent) on all servers and portable devices.	Verify in all new system deployments and at each VAPT.	System configuration documentation; VAPT report
Audit Logging	All administrator actions, system access events, and data modification events logged. Logs retained for a minimumof 1 year. Tamper-evident.	Review logs monthly for anomalies.	Log access records; log retention policy
Session Timeout	All workstations and systems auto-lock after a maximum 10 minutes of inactivity.	Verify monthly in F 4.10 Physical Security Checklist.	Group policy setting or individual configuration screenshots
Access Revocation	All system access for any departing or transferring staff member is revoked within 24 hours of departure. Credentials register updated.	Execute SOP 4.11.1 (Handover) and disable accounts the same day.	F 4.26/F 4.27/F 4.28 completed and filed

User Account Management Checklist — Complete monthly. Disable inactive or unauthorised accounts immediately.	
Account Management Check	Status
Are the number of active user accounts in all systems reviewed and compared against the current staff list?	[ ] Yes [ ] No — Action:
Are there any accounts for staff who have departed, transferred, or changed roles? (If yes: disable immediately)	[ ] None found [ ] Accounts disabled — IDs:
Do any accounts have administrator/elevated privileges that are not strictly required for the role?	[ ] None found [ ] Access reduced — IDs:
Are all administrator accounts protected by Two-Factor Authentication (2FA)?	[ ] Yes [ ] No — Action:
Are all system passwords meeting the current password policy (minimum 12 characters; complexity; not reused)?	[ ] Yes [ ] Non-compliant accounts:
Are any accounts showing login activity from unusual times (nights, public holidays) or unusual locations?	[ ] None found [ ] Suspicious activity — see INC-
Are all shared or generic accounts (e.g., 'admin') either disabled or assigned to a named individual?	[ ] Yes [ ] No — Action:
Are service accounts (used by systems, not humans) documented, password-protected, and not used for interactive logins?	[ ] Yes [ ] No — Action:
Have all accounts with access to citizen PII been reviewed and confirmed as still appropriate?	[ ] Yes [ ] Changes made — IDs:
Have any temporary access grants from the previous month been reviewed and revoked if no longer needed?	[ ] None outstanding [ ] Revoked — IDs:
Completed by: _____ Designation: _____ Date: _____	

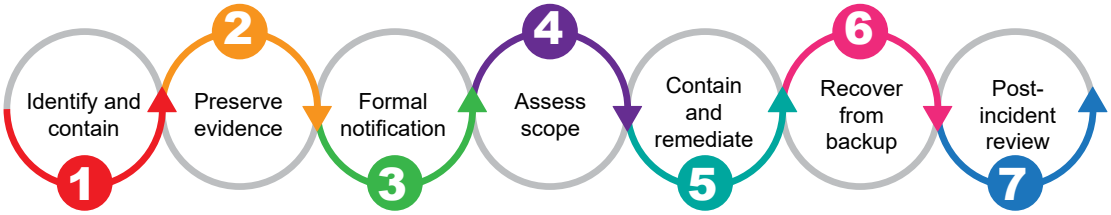
Patch Management Schedule — Update weekly. Apply Critical and High patches within 7 days of release.								
System / Software	Current Version	Patch / Update Available	Severity	Release Date	Target Apply Date	Applied Date	Change Ref (F 4.7)	Status
[OS / Software name]	[Version]	[Patch ID/ Name]	[ ] Critical [ ] High [ ] Med [ ] Low	[Date]	[Date — within 7 days for Critical/ High]	[Date]	CHG-[Yr]-[Seq]	[ ] Pending [ ] Applied [ ] Deferred
			[ ] Critical [ ] High [ ] Med [ ] Low					[ ] Pending [ ] Applied [ ] Deferred

Patch Management Schedule — Update weekly. Apply Critical and High patches within 7 days of release.								
			[ ] Critical [ ] High [ ] Med [ ] Low					[ ] Pending [ ] Applied [ ] Deferred
Completed by: _____ Designation: _____ Date: _____								

4.8 Security Incident Response and VAPT / साइबर सुरक्षा घटना प्रतिक्रिया तथा VAPT

A security incident is any actual or suspected unauthorized access to, disclosure of, modification of, or destruction of government ICT systems or citizen data. Security incidents are simultaneously a P1 operational incident (SOP 4.2.1) and a legal obligation under ETA 2063. The IT Official must execute both procedures in parallel.

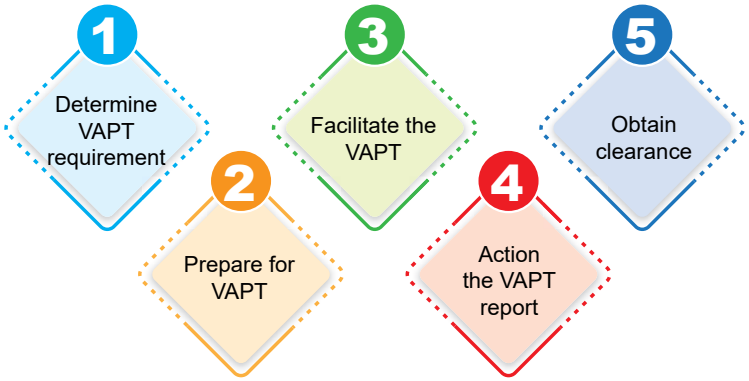
SOP 4.8.1 | Security Incident Response



Security Incident Response	
Purpose	Respond to, contain, and recover from security incidents — including cyberattacks, data breaches, ransomware, and unauthorized access. Simultaneously raises as P1 incident in SOP 4.2.1.
Steps	1. **Identify and contain:** Upon detecting or being notified of a security incident: immediately isolate affected systems from the network (disconnect network cable; disable Wi-Fi). Do NOT switch off — preserve evidence. Inform designated authority immediately by phone. Log in F 4.3 as P1. 2. **Preserve evidence:** Do not alter, delete, or attempt to clean the affected system. Photograph error messages, alerts, and unusual system behaviour. Download and preserve system event logs, security logs, and access logs to a separate storage device. 3. **Formal notification:** Report to: (1) **Nepal Police Cyber Bureau: +977-1-4412523** — file formal complaint; (2) **NCSC: +977-1-4200144** — mandatory notification for government systems under National Cybersecurity Policy. Record complaint reference numbers. 4. **Assess scope:** Determine: which systems are affected; what data may have been accessed, modified, or exfiltrated; how long the incident has been occurring; and whether citizen PII has been compromised (Privacy Act 2075 breach notification obligation). 5. **Contain and remediate:** With NCSC/vendor guidance: remove malware; close exploited vulnerabilities; reset all credentials on affected systems; rebuild compromised systems from clean backups if necessary. 6. **Recover from backup:** Restore services from the most recent clean backup (F 4.11). Verify integrity of restored data before returning to production. Test all critical services before resuming citizen-facing operations. 7. **Post-incident review:** Complete F 4.17 (Security Incident Report). Update ISMS Risk Register. Schedule VAPT to verify the exploited vulnerability has been remediated. Brief designated authority and relevant staff on lessons learned.

Security Incident Report — Complete for every security incident within 48 hours of detection	
Field	Details
Incident Reference:	INC-[Year]-[Seq] (from F 4.3) Date/Time Detected: [Date/Time]
Incident Type:	[ ] Ransomware [ ] Unauthorized Access [ ] Data Breach/Exfiltration [ ] Phishing [ ] DDoS [ ] System Defacement [ ] Other: ___
Systems Affected:	[List all affected systems, servers, and devices]
Data Potentially Compromised:	[ ] No citizen PII affected [ ] Citizen PII potentially exposed (Privacy Act breach notification required) Type of data: [Describe] Estimated records affected: [Number]
How Detected:	[ ] NCSC Alert [ ] Antivirus alert [ ] User report [ ] Routine log review [ ] External notification [ ] Other: ___
Immediate Containment Actions:	[Describe isolation steps taken and time of action]
Notification Record:	Nepal Police Cyber Bureau: Complaint No.: ___ Date: ___ NCSC: Reference No.: ___ Date: ___ Phone: +977-1-4200144
Root Cause (5 Whys if recurring):	[Identified root cause or 'Under investigation' if not yet determined]
Remediation Actions Taken:	[List all remediation steps completed]
VAPT Scheduled:	[ ] Yes — Date: ___ [ ] Not required (explain)
IT Official Signature:	_____ Date: _____
Designated Authority Review Signature:	_____ Date: _____
Completed by: _____ Designation: _____ Date: _____	

SOP 4.8.2 | VAPT Coordination



VAPT — Vulnerability Assessment and Penetration Testing from NCSC	
Purpose	Request and facilitate the NCSC VAPT for all internet-facing government systems before go-live and annually thereafter. VAPT clearance is a mandatory GEA 2.0 requirement before any citizen-facing system goes live.

Steps	1. **Determine VAPT requirement:** VAPT is required: (a) before any internet-facing citizen service goes live; (b) annually for all live internet-facing systems; (c) after any significant security incident; (d) after major system changes. Contact NCSC at +977-1-4200144 to schedule. 2. **Prepare for VAPT:** Complete F 4.18 VAPT Checklist. Whitelist the NCSC scanning IP address (202.45.145.183) in all firewalls, web application firewalls, and intrusion detection systems before the test date. 3. **Facilitate the VAPT:** Provide NCSC with: system scope (URLs, IP ranges, API endpoints); system architecture documentation; test user credentials if required. Ensure IT Official is available throughout the VAPT window.
Steps	4. **Receive and action the VAPT report:** Upon receiving the NCSC VAPT report: Critical findings must be remediated within 7 days; High findings within 30 days; Medium findings within 90 days. For each finding: raise a Change Request (F 4.7). No internet-facing system may go live if any Critical or High findings are unresolved. 5. **Obtain clearance:** Request NCSC VAPT Clearance Letter after all Critical and High findings are remediated. Retain clearance letter as a mandatory GEA 2.0 artifact (Module 6) and file with the system acceptance record.

F 4.18 | VAPT Planning and Preparation Checklist — Complete before NCSC VAPT date	
VAPT Preparation Check	Status
Is the scope of the VAPT defined? (List all URLs, IP addresses, APIs, and mobile app endpoints to be tested)	[ ] Defined — attached scope document
Is the NCSC test IP address (202.45.145.183) whitelisted in all firewalls and WAFs?	[ ] Whitelisted [ ] Not done — Action:
Is the system architecture documentation (GEA 2.0 artifact) available to share with NCSC?	[ ] Ready [ ] Not available — Action:
Have test user accounts (if required by NCSC) been created for authenticated testing?	[ ] Ready [ ] N/A
Is the IT Official available and on standby throughout the entire VAPT window?	[ ] Confirmed: [Date/Time]
Is a rollback / emergency shutdown plan in place if VAPT causes unintended system disruption?	[ ] Yes [ ] No — Action:
Is the NCSC formal request letter submitted and VAPT date confirmed with NCSC?	[ ] Confirmed: [Date] NCSC Contact: ___
POST-VAPT: Have all Critical findings been remediated within 7 days?	[ ] Yes [ ] N/A [ ] In progress — Due: ___
POST-VAPT: Have all High findings been remediated within 30 days?	[ ] Yes [ ] N/A [ ] In progress — Due: ___
POST-VAPT: NCSC VAPT Clearance Letter received?	[ ] Received — Date: ___ [ ] Awaiting — for final acceptance
Completed by: _____ Designation: _____ Date: _____	

4.9 Data Backup, Business Continuity, and Disaster Recovery / डेटा ब्याकअप, व्यापार निरन्तरता तथा विपद् पुनर्प्राप्ति

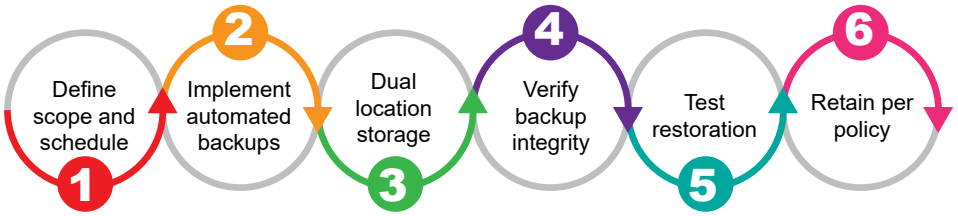
Backup, Business Continuity, and Disaster Recovery address the same question from three angles: Can we get critical citizen services back online quickly if something goes seriously wrong? Backup is the

technical mechanism. BCP is the organizational plan. DR is the technical procedure. All three must be in place and tested before they are needed — not after.

A Business Continuity Plan (BCP) ensures that critical government services remain accessible to citizens during ICT disruptions — whether from power failure, cyber incident, hardware failure, or natural disaster. A Disaster Recovery Plan (DR Plan) defines how ICT systems are restored after a major disruption. Both must be documented, tested bi-annually, and updated annually

IMPORTANT (⚠): UNTESTED BACKUP = NO BACKUP: A backup that has never been tested cannot be trusted. The Weekly Operations Checklist (F 4.9) requires a file restoration test every week. The Monthly Checklist requires a full system restoration test quarterly. Document every test in F 4.20 (Backup Test Log).

SOP 4.9.1 | Data Backup Procedure



SOP 4.9.1 | Data Backup Procedure	
Purpose	Protect all critical government and citizen data through a documented, automated, and regularly tested backup schedule aligned with the RTO/RPO requirements in F 4.19.
Steps	1. **Define backup scope and schedule:** Complete F 4.19 (Backup Schedule Template). For each critical system: specify what data is backed up; the backup frequency; the backup method (full/incremental/differential); and the storage location (local + off-site/ GIDC replication). 2. **Implement automated backups:** Configure backup jobs to run automatically — do not rely on manual daily backups. Financial and civil registration systems: daily incremental + weekly full backup minimum. Other systems: weekly full minimum. Verify each automated job completes with a success status. 3. **Dual location storage:** Every backup must be stored in at least two locations: (1) local NAS or backup server on-site; and (2) off-site — GIDC replication (preferred) or verified cloud with Nepal data residency. Off-site copy protects against fire, flood, and physical theft. 4. **Verify backup integrity:** Review backup job logs daily (F 4.9 Daily Checklist). Any failed backup job is a P2 incident — log in F 4.3 and investigate immediately. A backup job showing 'success' does not guarantee data integrity — run periodic restoration tests. 5. **Test restoration regularly:** Weekly: restore a single test file from the previous day's backup. Quarterly: perform a full system restoration test on a non-production system. Document results in F 4.20 (Backup Test Log). Failed tests = P1 incident. 6. **Retain backups per policy:** Financial data: minimum 7 years. Civil registration data: minimum 10 years. General operational data: minimum 3 years. Verify retention settings match these requirements in backup software configuration.

F 4.19 | Backup Schedule Template — Define backup policy for every critical system

System / Data	Criticality	Backup Frequency	Method	Local Storage	Off-site Storage	Retention	RPO Target
[Civil Registration System]	P1 — Critical	Daily incremental + Weekly full	Automated — scheduled	On-site NAS	GIDC replication	10 years	4 hours
[Financial / SUTRA data]	P1 — Critical	Daily incremental + Weekly full	Automated — scheduled	On-site NAS	GIDC replication	7 years	4 hours
[Staff records / HR data]	P2 — High	Weekly full	Automated — scheduled	On-site NAS	External HDD (locked storage)	5 years	24 hours
[Website / Portal]	P2 — High	Weekly full	Automated — scheduled	On-site NAS	GIDC / Cloud (Nepal)	3 years	24 hours
[Add additional systems as needed]							

Completed by: _____ Designation: _____ Date: _____

F 4.20 |Backup Test and Restoration Log — Record every backup test. Quarterly: full restoration test.

Test Date	System Tested	Backup Date Restored	Test Type	Test Result	Time to Restore	IT Official
[Date]	[System name]	[Date of backup used]	[ ] File [ ] Full system	[ ] Success [ ] Partial [ ] Failed — see INC-	[HH:MM]	[Name]
			[ ] File [ ] Full system	[ ] Success [ ] Partial [ ] Failed — see INC-		
			[ ] File [ ] Full system	[ ] Success [ ] Partial [ ] Failed — see INC-		

Completed by: _____ Designation: _____ Date: _____

RTO and RPO Targets — F 4.19 Reference

Recovery Time Objective (RTO): The maximum acceptable time from incident to service restoration.

Recovery Point Objective (RPO): The maximum acceptable data loss — how far back in time you may need to restore from.

System / Service	Priority	RTO (max time to restore)	RPO (max data loss)	DR Strategy
Civil registration / vital records	P1 — Critical	4 hours	4 hours (last backup)	GIDC replication; DR site activation; manual operation procedures for interim period
Financial / accounting systems (SUTRA, PAMS)	P1 — Critical	4 hours	4 hours	GIDC replication; manual payment recording during restoration window

System / Service	Priority	RTO (max time to restore)	RPO (max data loss)	DR Strategy
Email / office communication	P2 — High	8 hours	24 hours	Backup server restore; manual communication during outage
Staff HR / leave management	P2 — High	24 hours	24 hours	Weekly backup restore from local or off-site storage
Municipal website / citizen portal	P2 — High	8 hours	24 hours	Backup restore; static 'maintenance' page during outage
General office productivity (shared drives)	P3 — Medium	2 business days	1 week	Weekly full backup restore; users switch to local working files

SOP 4.9.2 | BCP Development

SOP 4.9.2 | BCP Development Guide — Five Steps for LG IT Officials BCP विकासमार्गदर्शन — पाँचचरणहरू	
Purpose	Protect all critical government and citizen data through a documented, automated, and regularly tested backup schedule aligned with the RTO/RPO requirements in F 4.19.
Steps	1. **सेवा पहिचान:** Identify which government services are most critical — which would cause greatest harm to citizens if interrupted? Prioritize by citizen impact, legal mandate, and revenue sensitivity. Priority list: P1 (Civil Registration, Revenue) · P2 (Property services, Permits) · P3 (Internal admin) 2. **ICT निर्भरता:** Map each critical service to its ICT dependencies: server, software, network, power, data, vendor. Every dependency is a potential failure point. Service-ICT dependency matrix for all P1/P2 systems 3. **RTO/RPO निर्धारण**: Define Recovery Time Objective (RTO — how quickly must service be restored?) and Recovery Point Objective (RPO — how much data loss is acceptable?) per system. Document in F 4.21 RTO/RPO Register. Signed F 4.21 with RTO/RPO targets per system 4. **पुनर्प्राप्ति प्रक्रिया**: Document step-by-step recovery procedures for each P1/P2 system. Who does what? In what order. Contact details for every vendor and agency needed.Recovery runbooks per system + F 4.21 Emergency Contacts 5. **परीक्षण र अद्यावधिक:** Test the BCP bi-annually. Document results in F 4.23 DR Test Report. Update the BCP annually or after any major incident or system change. Bi-annual DR test completed · Annual BCP update

F 4.21 |Application RTO/RPO Register — Maintain for all government systems. Review at every DR test.

Item / विवरण	Details / विवरण	Status / स्थिति	Reference			
System Name	Priority (P1/P2/P3)	RTO Target (max restoration time)	RPO Target (max data loss period)	Recovery Method	Last DR Test Date	RTO/RPO Met?
Civil Registration / GIOMS	P1	4 hours	4 hours	Restore from GIDC backup to standby VM	[Date]	[ ] Yes [ ] No
Revenue / Property Tax	P1	4 hours	4 hours	[Define recovery method]	[Date]	[ ] Yes [ ] No
GIWMS Website	P2	8 hours	24 hours	[Define]	[Date]	[ ] Yes [ ] No
[Add system]						

Authorized IT Official: _____ Date: _____

Designated Authority (if required): _____

F 4.22 | BCP/DR Readiness Checklist — Complete annually and after major system changes

Check Item	Status
Is an RTO/RPO Register (F 6.9) maintained and current for all P1 and P2 systems?	[ ] Yes [ ] No [ ] Partial
Are current backups verified daily and stored in GIDC offsite backup (IDMC Service I4 — Module 7)?	[ ] Yes [ ] No [ ] Partial
Has a restoration test been conducted for all P1 systems within the last 6 months (restore and verify)?	[ ] Yes [ ] No [ ] Partial
Is a step-by-step recovery runbook documented for each P1/P2 system — can a different staff member follow it?	[ ] Yes [ ] No [ ] Partial
Is the Emergency Contact List (Module 4 F 4.21) current — verified within last month?	[ ] Yes [ ] No [ ] Partial
Are all vendor AMC contracts active with escalation contacts confirmed reachable?	[ ] Yes [ ] No [ ] Partial
Has staff been trained on BCP procedures — do front-desk staff know what to do during system outage?	[ ] Yes [ ] No [ ] Partial
Has the BCP been reviewed and updated in the last 12 months or after any major incident?	[ ] Yes [ ] No [ ] Partial
Are critical government service alternatives documented (manual workaround procedures during ICT outage)?	[ ] Yes [ ] No [ ] Partial

Is the DR test result from the last bi-annual test documented in F 4.23 DR Test Report and presented to designated authority?	[ ] Yes [ ] No [ ] Partial
Reviewed by IT Official: _____ Date: _____	

F 4.23 | DR Test Report — Complete after every bi-annual DR test

Item / विवरण	Details / विवरण	Status / स्थिति	Reference		
Test Date		System Tested		Test Lead (IT Official)	
Test Type	[ ] Tabletop (discussion)· [ ] Simulation· [ ] Full restoration test				
RTO Target (from F 4.21)		Actual restoration time		[ ] Met [ ] Not met	
RPO Target (from F 4.21)		Actual data loss period		[ ] Met [ ] Not met	
Issues Identified	[Describe any problems encountered during restoration]				
Improvement Actions	[Actions to address gaps — with responsible officer and completion date]				
Designated Authority Briefed on Results	[ ] Yes Date: _____	Next DR Test Scheduled	[ ] 6 months Date: _____		

Authorized IT Official: _____ Date: _____

Designated Authority (if required): _____

F 4.24 | BCP/DRP Emergency Contact List — Print and keep physical copy in server room and with designated authority

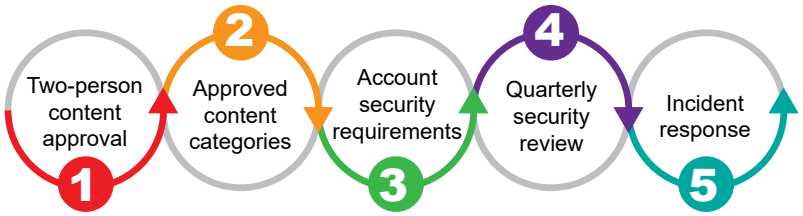
Role / Agency	Name	Primary Phone	Secondary Phone	Email	24/7?
Designated Authority/ Administration Chief (Designated Authority)	[Name]	[Phone]	[Phone]	[Email]	[ ] Yes [ ] No
IT Official	[Name]	[Phone]	[Phone]	[Email]	[ ] Yes [ ] No
Province Government, Support Unit/ Personnel	[Name]	[Phone]	[Phone]	[Email]	[ ] Yes [ ] No
NCSC (National Cyber Security Centre)	NCSC Duty Officer	+977-1-4200144		ncsc@nepal.gov.np	[ ] 24/7

F 4.24 | BCP/DRP Emergency Contact List — Print and keep physical copy in server room and with designated authority					
Nepal Police Cyber Bureau	Cyber Duty Officer	+977-1-4412523			[ ] 24/7
IDMC (Govt Data Center)	IDMC Helpdesk	Verify at idmc.gov.np		Verify at idmc.gov.np	[ ] Yes [ ] No
Primary ICT Vendor / AMC Provider	[Vendor Name]	[Phone]	[Phone]	[Email]	[ ] Yes [ ] No
Backup Power / Generator Technician	[Name]	[Phone]	[Phone]	[Email]	[ ] Yes [ ] No
Internet Service Provider (NTC / other)	[Provider]	[Account No.: ___]	[NOC Phone]	[Email]	[ ] 24/7
Completed by: _____ Designation: _____ Date: _____					

4.10 Social Media Management / सामाजिक सञ्जाल व्यवस्थापन

Official government social media accounts (Facebook, YouTube, and official portal) are public-facing communication channels subject to the RTI Act (proactive disclosure), the Good Governance Act (accuracy and decorum), and the ETA 2063 (account security). Compromised social media accounts can rapidly spread misinformation about government services — creating public trust crises.

SOP 4.10.1 | Social Media Approval



SOP 4.10.1 | Social Media Content Approval and Security	
Purpose	Manage all official government social media accounts with documented content approval, two-person control, and quarterly security reviews. Combined procedure covering both content publication and security management.
Steps	1. **Two-person content approval:** No government social media post is published without approval from both the IT Official(technical review) and the designated authority or designated Communication Officer (content and policy review). Emergency public notices (disasters, service outages): IT Official publishes with simultaneous designated authority verbal approval and documents the approval in F 4.22 within 24 hours. 2. **Approved content categories:** Published without additional review: official government announcements; service disruption notices; approved public event notifications; proactive disclosure updates (RTI Act compliance). NEVER publish: political content; personal opinions; content about pending legal matters; content provided by unknown external parties.

Steps	
	3. **Account security requirements:** All official social media accounts must have: (a) 2FA enabled with authentication app — never SMS-only; (b) account access restricted to named individuals only — no shared passwords; (c) administrator access recorded in F 4.23; (d) recovery email/phone registered to a government institutional address — not a personal address. 4. **Quarterly security review:** Complete F 4.22 (Social Media Security Checklist) quarterly. Remove access for any departed or changed-role staff. Verify 2FA is active on all accounts. Change account passwords if any security concern has arisen. 5. **Incident response:** If an official social media account is compromised or suspected compromised: immediately change the account password; revoke access for all users; re-enable 2FA; post a correction notice from the restored account; report to NCSC (+977-1-4200144); complete F 4.17 Security Incident Report.

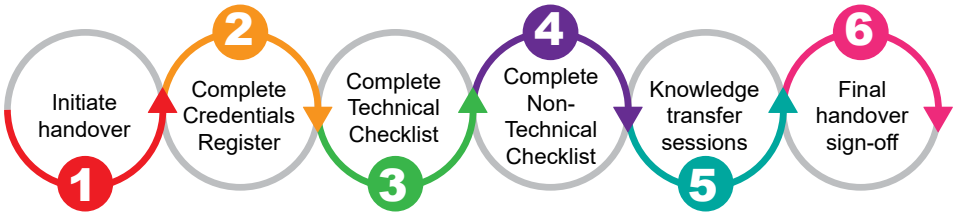
F 4.25 | Social Media Management Checklist — Content Approval (each post) + Security Review (quarterly)	
CONTENT APPROVAL — Complete for every post before publication	Status
Is the content factually accurate and sourced from an official government document or decision?	[ ] Yes [ ] No — do not publish
Has the IT Official reviewed the content for technical accuracy and security implications (no sensitive system info, no PII)?	[ ] Approved [ ] Changes required
Has the designated Communication Officer approved the content for policy and tone?	[ ] Approved by: ___ Date: ___
Does the post comply with the Government Communication Guidelines (no political content, no personal opinions)?	[ ] Yes [ ] No — do not publish
Is the post in Nepali as the primary language (or bilingual where appropriate)?	[ ] Yes [ ] No — translate first
ACCOUNT SECURITY REVIEW — Complete quarterly for every official account	Status
Is Two-Factor Authentication (2FA) enabled on all official social media accounts (app-based, not SMS-only)?	[ ] Yes [ ] No — enable immediately
Are all accounts using an institutional email address (not a personal address) for recovery?	[ ] Yes [ ] No — update immediately
Is the list of current account administrators current and reviewed (no departed staff with access)?	[ ] Yes [ ] Access removed for: ___
Are all account passwords current, complex, and not shared verbally or via messaging apps?	[ ] Yes [ ] No — change immediately
Has account activity been reviewed for any unusual posts, login attempts, or access from unfamiliar devices?	[ ] Nothing unusual [ ] Suspicious — see INC-
Completed by: _____ Designation: _____ Date: _____	

4.11 Staff Handover Procedures / कर्मचारी हस्तान्तरण प्रक्रियाहरु

Inadequate ICT handover when an IT Official departs is the single most disruptive and risk-creating event for a government ICT operation. Within 24 hours of a departure, system credentials may be unknown, vendor contacts lost, and critical operational knowledge in the departing officer's head only. The 14-day structured handover process below prevents this — and creates the documented proof required for OAG audit compliance.

IMPORTANT (⚠): CREDENTIALS REGISTER (F 4.25) IS A SECURITY DOCUMENT: The Credentials Register must be stored in a sealed envelope signed across the seal by the IT Official and designated authority. The envelope can be stored in the designated authority's personal secure cabinet — not in an accessible office file. It is opened ONLY when a staff member departs or when a P1 system access emergency requires it. Photographing or copying the register in other circumstances is a security breach.

SOP 4.11.1 | ICT Handover



SOP 4.11.1 | ICT Handover for Departing IT Official or ICT-Responsible Staff	
Purpose	Execute a structured 14-day handover when any IT Official or ICT-responsible staff member departs. Zero tolerance for undocumented departures — the designated auhtorityis personally accountable for ensuring this SOP is completed.
Steps	1. **Initiate handover immediately on notice of departure:** As soon as departure is known — regardless of the notice period — the IT Official begins the handover documentation. Minimum 14 calendar days is required for IT Officials; 7 days for non-technical staff with ICT responsibilities. The designated authority must confirm the handover plan in writing within 48 hours. 2. **Complete Credentials Register (F 4.25):** The departing IT Official documents ALL system credentials, admin passwords, vendor account logins, ISP account details, social media admin access, and backup encryption keys in F 4.25. This is completed within the first 3 days of the handover period. The IT Official and designated authority both verify the register is complete before signing. 3. **Complete Technical Handover Checklist (F 4.24):** Document all systems, their current status, pending issues, ongoing vendor contracts, and known vulnerabilities. The receiving officer must confirm each item is understood and verified. For each item in F 4.24: the receiving officer counter-signs confirming receipt. 4. **Complete Non-Technical Handover Checklist (F 4.23):** Hand over all physical items: laptops, keys, ID cards, server room access tokens, official SIM cards, government devices. Each item is signed for by the receiving officer.

Steps	
	5. **Knowledge transfer sessions:** The departing IT Official conducts formal knowledge transfer sessions with the receiving officer: (a) System tour — demonstrating each system's administration console; (b) Vendor contacts — introducing vendors and reviewing AMC contract terms; (c) Open issues — walking through all open incidents in F 4.3 and open change requests in F 4.7. 6. **Final handover sign-off:** On the last working day: (a) Change all admin passwords and 2FA tokens to new values known only to the receiving officer; (b) Remove departed staff's access from all systems immediately; (c) Update the Credentials Register with new values; (d) Designated authority, departing officer, and receiving officer all sign the Technical Handover Checklist (F 4.24).

Non-Technical / Physical Handover Checklist

Item	Description	Received By	Status
Government-issued laptop/ computer	[Asset ID: ___]	[Signature]	[ ] Received in good condition [ ] Damaged — noted
Server room physical key(s)	[Number of keys: ___]	[Signature]	[ ] Received
Network equipment access key(s)	[Location: ___]	[Signature]	[ ] Received [ ] N/A
Government SIM card(s)	[Number: ___ Networks: ___]	[Signature]	[ ] Received [ ] N/A
Government ID card / access token	[Description: ___]	[Signature]	[ ] Received
Official stamp / seal	[Description: ___]	[Signature]	[ ] Received [ ] N/A
Physical documentation files (ICT records)	[Box/folder list attached]	[Signature]	[ ] Received
All government-issued portable storage devices	[Number of USB drives / external HDDs: ___]	[Signature]	[ ] Received [ ] None issued

Completed by: _____ Designation: _____ Date: _____

F 4.27 | Technical Handover Checklist — Departing IT Official completes; Receiving Officer counter-signs each item

Category	Item	Status / Notes	Receiving Officer Sign
Systems Status	Current operational status of all systems (list separately — see Incident Log F 4.3 for open issues)	[ ] Briefed [ ] Outstanding issues: ___	
Open Incidents	All open incidents in F 4.3 — receiving officer briefed on each	[ ] Briefed No. of open: ___	
Open Changes	All open change requests in F 4.7 — receiving officer briefed on each	[ ] Briefed No. of open: ___	
Backup Status	Current backup schedule (F 4.19) explained; last successful backup verified; restoration procedure demonstrated	[ ] Demonstrated Last backup: ___	

F 4.27 | Technical Handover Checklist — Departing IT Official completes; Receiving Officer counter-signs each item			
Vendor Contacts	All AMC vendors, ISP, and support contacts introduced; current contract status reviewed	[ ] Briefed Contracts reviewed: ___	
Security Alerts	Any known vulnerabilities, pending VAPT, or NCSC advisories outstanding	[ ] Briefed Outstanding: ___	
Upcoming Deadlines	Any procurement, license renewals, or compliance deadlines in the next 90 days	[ ] Briefed Dates: ___	
Credentials Register (F 4.25)	Credentials Register verified as complete; stored in sealed envelope in designated authority's secure cabinet	[ ] Verified [ ] Sealed and filed	
Training Provided	Departing officer has conducted minimum [__] hours of formal knowledge transfer sessions	[ ] Completed Dates: ___	
FINAL SIGN-OFF	All items above verified complete and received		
Departing IT Official:	Name: _____ Signature: _____ Date: _____		
Receiving Officer:	Name: _____ Signature: _____ Date: _____		
Designated authority Verification:	Name: _____ Signature: _____ Date: _____		
Completed by: _____ Designation: _____ Date: _____			

F 4.28 | System Credentials and Access Handover Register — CONFIDENTIAL: Store sealed in designated official's cabinet

System / Service	Account Type	Username / Login ID	Password / Access Method	2FA Device/ App	Recovery Email/ Phone
[Civil Registration System]	[ ] Admin [ ] Service	[Username]	[Password — update on departure]	[App/ Device]	[Recovery contact]
[Financial System / SUTRA]	[ ] Admin [ ] Service				
[Municipal Website Admin]	[ ] Admin [ ] Service				
[Email admin account]	[ ] Admin [ ] Service				
[Server root/admin account]	[ ] Admin [ ] Service				

F 4.28 | System Credentials and Access Handover Register — CONFIDENTIAL: Store sealed in designated official's cabinet					
[Firewall / Router admin]	[ ] Admin [ ] Service				
[Internet account (ISP)]	[ ] Admin [ ] Service				
[Social media accounts]	[ ] Admin [ ] Manager				
[GIOMS admin]	[ ] Admin [ ] Service				
[Backup software admin]	[ ] Admin [ ] Service				
[Add additional systems as needed]					
Verified complete and accurate — Departing IT Official:	_____ Date: _____ Designated authority:	_____ Date: _____	SEALED AND STORED: Date: _____		

MODULE 5

PROCUREMENT AND VENDOR MANAGEMENT

Annual Plan · TCN · ToR · Specs · Cost Estimation · QCBS · Anti-Corruption Templates · NDA · AMC · Acceptance · Vendor Management · Scenario Navigator · Red Flag Checklist

Planning	ToR/Specs	Bidding	Evaluation	Contract

Scope: The complete ICT procurement lifecycle from planning through vendor management, covering Sections 5.1–5.10, aligned to the Public Procurement Act 2063 and IT Norms 2082.

Target: IT Officials and procurement committees running any ICT goods, software, or consulting procurement.

Coverage: Procurement planning → TCN → ToR/Specs → Cost estimation → Bidding → QCBS evaluation → Contract → Vendor performance → Acceptance → Handover. All procurement types: Goods, Consulting/Software, AMC.

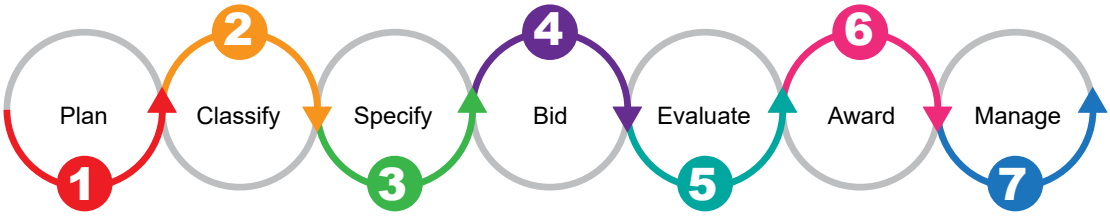
Legal basis: Public Procurement Act 2063 · PPR 2064 (14th Amendment) · MoCIT IT Norms 2082 · PPMO Standard Bidding Documents. See Module 3, Sections 3.9-3.10 for full legal framework.

Key tools: M5-T01 Annual Plan · M5-T03 TCN · M5-T04/05 ToR · M5-T07/08 Specs · M5-T09 Cost Worksheet · M5-T11 QCBS Matrix · Anti-Corruption Templates 1-3 · M5-T13 Contract Clauses · M5-T16 NDA · M5-T17 AMC · M5-T20 Acceptance · M5-T21 Vendor Risk · M5-T22 Scorecard · M5-T23 Scenario Navigator · M5-T24 Red Flag Checklist

Cross-references: Module 3 (legal framework) · Module 4 (SLA monitoring F 4.21, asset registration F 4.14) · Module 6 (GEA 2.0 artifacts in software contracts) · Module 7 (IDMC/DoIT vendor services, e-GP portal)

This module covers the complete ICT procurement lifecycle — from initial needs assessment and budget preparation through bid document preparation, e-GP publication, evaluation, contract award, vendor risk assessment, ongoing performance management, technical evaluation and exit management. All procedures are aligned with the Public Procurement Act 2063 (including the 2nd Amendment ordinance, 2083), Public Procurement Regulation 2064 (14th Amendment, 2082), the Electronic Government Procurement System Guidelines, and PPMO Standard Bidding Documents.

The ICT Procurement Lifecycle



5.1 Procurement Planning / खरिद योजना

Every ICT procurement must: (1) be included in the Annual ICT Procurement Plan (M5-T01) approved by the designated authority before the fiscal year starts; and (2) begin with an approved Technical Concept Note (M5-T03).

Legal Basis (⚖):

PPA 2063 requires all procurement to be included in the Master Procurement Plan (Schedule-2). IT Norms 2082 rates are mandatory for all ICT consulting and software development cost estimates. Thresholds listed in this module are indicative — verify current values at ppmo.gov.np before each procurement.

M5-T01 | Annual ICT Procurement Plan — Prepare before fiscal year start; Designated Authority approval required

Item	Description	Qty	Est. Cost (NPR)	Method	Quarter	Budget Status
[ICT item 1]	[Description]	[n]	NPR [Amount]	[Direct/SQ/ NCB/RFP]	Q[1-4]	[ ] Approved [ ] Pending
[ICT item 2]					Q[1-4]	[ ] Approved [ ] Pending
[Additional rows as needed]						
TOTAL ICT BUDGET:			NPR [Total]			

Completed by: _____ Designation: _____ Date: _____

5.1.1 Procurement Lifecycle at a Glance / खरिद चक्र — एक झलक

SOP 5.1.1 | ICT Procurement Lifecycle at a Glance				
1 Needs Assessment	**2** Draft Specs/ToR	**3** Cost Estimation	**4** Determine Method	**5** Prepare Bid Doc
6 Executive Approval	**7** e-GP Publication	**8** Pre-Bid Meeting	**9** Receive Bids	**10** Technical Evaluation
11 Financial Evaluation	**12** Bid Evaluation Report	**13** Contract Award	**14** Kick-off and Monitoring	**15** Contract Close-out

SOP 5.1.1: ICT Procurement Process (Goods, Software, and Consultancy)	
1	NEEDS ASSESSMENT AND BUDGET ALIGNMENT: The IT Official drafts a Technical Concept Note (M5-T03) clearly identifying the operational problem, proposed solution, GEA 2.0 alignment, and estimated budget. Confirm that the procurement is included in the approved Annual Program and Budget before proceeding. Procurement not in the approved budget requires a budget transfer or supplementary approval.
2	DRAFT SPECIFICATIONS OR TOR: For hardware/goods procurement, prepare brand-neutral Technical Specifications (M5-T07/M5-T08) describing required performance and functionality — not specific brands or models. For software/consultancy, prepare a detailed Terms of Reference (M5-T05/M5-T06) with defined deliverables, timelines, and key expert qualifications aligned with MoCIT IT Norms 2082.
3	IT NORMS-COMPLIANT COST ESTIMATION: For all consultancy/software assignments, calculate the budget estimate using the IT Consulting Cost Estimation Worksheet (M5-T09). Multiply required person-days per role by the applicable IT Norms daily rate. Attach this calculation to the financial clearance request. This document is the primary defence against CIAA budget queries.
4	DETERMINE PROCUREMENT METHOD: Based on the total estimated cost and procurement type (goods vs consultancy), select the correct procurement method from the threshold tables in Section 5.2. If in doubt, apply the higher-threshold method — never the lower. Document the method selection with the cost estimate.
5	PREPARE BID DOCUMENT: Use only PPMO Standard Bidding Documents — available at ppmo.gov.np. For goods: select the appropriate Standard Bidding Document (SQ, 1S1E, or 1S2E). For consultancy: use the Standard Request for Proposal (RFP) template. Complete all sections including minimum eligibility criteria, evaluation criteria, and contract conditions.
6	EXECUTIVE APPROVAL: Submit the bid document package (Concept Note, Specifications/ToR, cost estimate, draft bid document) to the designated authority for approval before publication. Record approval in the ICT Decision Log (F 4.1, Module 4).
7	e-GP PUBLICATION: Publish the procurement notice on the PPMO e-GP portal (bolpoatra.gov.np) for all qualifying procurements. Publication must include the bid document, submission deadline, and evaluation criteria. Simultaneously published in a national daily newspaper for 1S1E and above.
8	PRE-BID MEETING (if applicable): For complex procurements (1S2E, major software), hold a pre-bid meeting to clarify the bid document. Issue written minutes of the pre-bid meeting to all interested bidders and publish on e-GP within 5 working days.

9	RECEIVE BIDS: Receive bids through e-GP or in physical sealed envelopes as specified. Never accept a bid after the submission deadline. For consultancy RFPs, confirm technical and financial proposals are in separate sealed envelopes before opening. Log all received bids with date, time, and bidder details.
10	TECHNICAL EVALUATION: For goods (1S1E): evaluate against minimum eligibility criteria; eligible bidders proceed to price comparison. For goods (1S2E): evaluate against eligibility AND qualification criteria; qualified eligible bidders proceed to price. For consultancy: evaluate technical proposals using the QCBS Technical Evaluation Matrix (M5-T11) scoring firm experience, methodology, and key expert qualifications. Only firms scoring above the minimum technical threshold (typically 70/100) proceed to financial evaluation.
11	FINANCIAL EVALUATION: For goods: the lowest evaluated bid price among eligible/qualified bidders wins. For consultancy: open financial envelopes only of technically qualified firms. Apply QCBS formula: Combined Score = (Technical Score × 0.80) + (Financial Score × 0.20). The highest combined score wins.
12	BID EVALUATION REPORT: Prepare a formal Bid Evaluation Report signed by all evaluation committee members. The report must document: all bids received, evaluation criteria applied, scores awarded, and recommended awardee with justification. This report is a mandatory procurement record.
13	CONTRACT AWARD AND SIGNING: Issue Letter of Acceptance to the successful bidder. Execute the contract within the statutory period. Attach the signed NDA (M5-T16) as a contract annex for all software and data-handling assignments. Notify unsuccessful bidders per PPA requirements.
14	PROJECT KICK-OFF AND MONITORING: Conduct a formal project kick-off meeting. Establish monitoring milestones aligned with the payment schedule. Assign the IT Official as contract administrator responsible for verifying deliverables before authorizing payments.
15	CONTRACT CLOSE-OUT: Upon completion, verify all deliverables against the ToR/Technical Specifications and sign the System Acceptance Certificate (M5-T20). Obtain UAT sign-off. Process final payment only after all deliverables are accepted. Update the ICT Asset Register (Module 4). File all procurement records for OAG audit readiness.

Market Price Survey (Mandatory for All Goods Procurement)

Before preparing the cost estimate for any goods procurement, obtain minimum **3 written quotations** from different suppliers for equivalent specifications. Formula: **Total Cost = (Unit Price × Qty) + Taxes (VAT 13%) + Delivery + Contingency (max 10%)**. Attach the completed M5-T25 survey to the TCN before designated authority approval.

M5-T25 | Market Price Survey Record — Attach to TCN M5-T03. Mandatory for all goods procurement.					
Supplier Name	Contact	Date of Quote	Quoted Unit Price (NPR)	Warranty / Service Terms	Notes
[Supplier 1]	[Contact]	[Date]	NPR [Amount]	[Terms]	
[Supplier 2]	[Contact]	[Date]	NPR [Amount]	[Terms]	
[Supplier 3]	[Contact]	[Date]	NPR [Amount]	[Terms]	
Selected Cost Estimate:	NPR [Amount/ unit] × [Qty] = NPR [Sub]	+ VAT 13%: NPR [Amount]	+ Delivery/Install: NPR [Amount]	+ Contingency (max 10%): NPR [Amount]	TOTAL: NPR [Grand Total]

M5-T25 | Market Price Survey Record — Attach to TCN M5-T03. Mandatory for all goods procurement.					
Justification if not lowest:	[Explain]				

IT Official Signature:	_____ Date: _____ Designated Authority Approval:	_____ Date: _____

5.2 Procurement Classification and Thresholds / खरिद वर्गीकरण र सीमाहरू

Correctly classifying the procurement type determines the method, timeline, and evaluation approach. Apply goods thresholds for hardware and off-the-shelf software; consulting thresholds for custom software development, advisory, and AMC services.

IMPORTANT (⚠):

THRESHOLD VERIFICATION: Values below are indicative based on PPA 2063 and PPR 2064 (14th Amendment). Thresholds change by PPMO gazette notification. ALWAYS verify current thresholds at ppmo.gov.np before initiating any procurement. Do not rely on printed values alone.

Method — ICT GOODS	Threshold (NPR) [Verify at ppmo.gov.np]	Notice	e-GP Mandatory?	Typical Gandaki LG Use
Direct Purchase	Up to NPR 1,00,000	Immediate — negotiated	No	Accessories, cables, emergency peripherals, minor hardware repairs
Sealed Quotation (SQ) — ask with firms among Standing List	NPR 1,00,000 to NPR 10,00,000	7 days	No	Standard peripherals, UPS batteries, minor hardware upgrades
Open IFQ — Published (open for all firms)	NPR 10,00,000 to NPR 20,00,000	15 days	Recommended	Standard computers (5-10 units), basic networking equipment
NCB 1S1E — Open Bidding	Above NPR 20,00,000 to NPR 2,00,00,000	30 days	Mandatory	Server procurement, bulk computer refresh, structured cabling
NCB 1S2E — Open Bidding	Above NPR 2,00,00,000 to NPR 15,00,00,000	30 days	Mandatory	Server procurement, bulk computer refresh, structured cabling
ICB — International	Above NPR 15,00,00,000	45 days	Mandatory	Rare at LG level — verify with PPMO before initiating

Method — ICT CONSULTING / SOFTWARE / AMC	Threshold (NPR) [Verify at ppmo.gov.np]	Notice	Evaluation Method	IT Norms 2082 Required?
Direct Selection	Up to NPR 1,00,000	Immediate	1 qualified firm, negotiated	Yes — for cost estimate baseline
Sealed Quotation (SQ)	NPR 1,00,000 to NPR 5,00,000	7 days	Lowest eligible	Yes — mandatory for ToR

Method — ICT CONSULTING / SOFTWARE / AMC	Threshold (NPR) [Verify at ppmo.gov.np]	Notice	Evaluation Method	IT Norms 2082 Required?
RFP — Shortlisted firms	NPR 5,00,000 to NPR 20,00,000	15 days	QCBS 80:20	Yes — mandatory
EOI + RFP (NCB) — Open	Above NPR 20,00,000	15 days EOI + 30 days RFP (e-GP)	QCBS 80:20	Yes — mandatory

Method - Special Goods Procurement	When to Use	Key Conditions	Approx. Timeline
Catalog Shopping	Procurement of standard equipment directly from manufacturer or authorized dealer. Valid for a single fiscal year only.	Must be from authorized dealer list; competitive price from at least 3 catalogs/quotations. designated authority approval required.	10–20 working days
Limited Tendering	When only a limited number (3 or fewer) of manufacturers/ authorized dealers supply the required item.	Must document why full competition is not possible. designated authority approval required. Competitive quotes from all known suppliers.	15–25 working days
Buy-Back Method	Upgrading/replacing existing equipment by negotiating with the original supplier.	Must be the same vendor who supplied the original equipment; negotiated price must demonstrate value for money. designated authority approval required.	10–20 working days
Item Rate Procurement	When procuring multiple items of the same type at a unit rate for use as needed throughout a period.	Applicable to SQ, 1S1E, 1S2E methods. Useful for consumables and maintenance materials.	Same as parent method

In addition to the standard methods above, PPR 2064 provides the following special methods applicable to specific ICT goods procurement situations:

e-GP Portal (bolpoatra.com.np): All procurement above the e-GP mandatory threshold must be published on the PPMO portal. Failure to publish when required is a stand-alone irregularity regardless of other compliance. Verify the current e-GP threshold at ppmo.gov.np.

5.3 Technical Concept Note (TCN) / प्राविधिक अवधारणा नोट (TCN)

The TCN is the mandatory internal business case document that justifies an ICT investment. It must be approved by the designated authority before any procurement activity commences.

M5-T03 | Technical Concept Note (TCN) — Designated authority approval required before any procurement commences	
Section	Content
TCN Reference No.:	TCN-[Office Code]-[Year]-[Seq] — e.g., TCN-WMN-2082-003 Date: [Date]

M5-T03 | Technical Concept Note (TCN) — Designated authority approval required before any procurement commences	
1. Problem / Need:	[Describe the specific operational problem or service gap this procurement addresses — 2-4 sentences. Which system is failing, how many users are affected, what citizen service is impacted, since when?]
2. Proposed Solution:	[ ] Goods/Hardware [ ] Software/Consulting [ ] AMC [ ] Others[Describe the proposed procurement and why it addresses the problem above.]
3. GEA 2.0 Compliance (for software):	[ ] REST/JSON APIs planned [ ] GIDC hosting evaluate [ ] NID integration considered [ ] Source code ownership in ToR [ ] N/A (goods)
4.Expected Outcomes:	[List 2-4 specific, measurable outcomes — e.g., 'All 12 staff will have functional workstations'; 'Civil registration system restored with 99.5% uptime SLA']
5. Cost Estimate:	NPR [Insert total][ ] Market Price Survey (M5-T25) attached — mandatory for goods[ ] IT Norms 2082 Cost Worksheet (M5-T09) attached — mandatory for consulting
6. Procurement Method:	[Insert method — verify with Threshold Tables in Section 5.2]
7. Budget:	[ ] Included in Annual ICT Procurement Plan (M5-T01) [ ] Supplementary amendment required — attach approval
8. Alternatives Considered:	[Briefly state alternatives considered and why this solution is preferred]
Designated Authority Approval:	This TCN authorizes the IT Official to proceed with procurement planning only. It does NOT authorize commitment of funds.Signature: _____ Name: _____ Date: _____
Completed by: _____ Designation: _____ Date: _____	

5.4 Terms of Reference and Technical Specifications

सन्दर्भ सर्तहरू तथा प्राविधिक विशिष्टताहरू

A well-written ToR defines exactly what will be delivered, the acceptance criteria, Key Expert qualifications (per IT Norms 2082), and GEA 2.0 compliance requirements. A poorly written ToR is the single most common root cause of procurement failure and CIAA findings in ICT consultancy procurement.

5.4.1 Terms of Reference (ToR) — Consulting and Software Development

कार्य सन्दर्भहरुको सूची — परामर्श र सफ्टवेयर विकास

Purpose: Defines the scope, deliverables, timelines, and key expert requirements for consultancy and custom software development assignments.

Section	Required Content
1. Background and Context	Institutional context of the local/provincial government; rationale for the assignment; connection to the approved Annual Work Plan and ICT Strategic Plan.
2. Objectives	Primary objective (what the assignment must achieve) and specific sub-objectives (what the consultant must deliver).
3. Scope of Work	Explicitly list all tasks in scope (e.g., Technical Specifications: Software System, system requirements analysis, design, coding, testing, UAT support, deployment, training, documentation). List OUT-OF-SCOPE activities to prevent scope creep.
4. Deliverables and Timelines	Table format: Deliverable | Description | Due Date | Acceptance Criteria Minimum required: Inception Report; SRS/FRS; System Architecture; UAT Plan; Deployment; User Manual; Admin Manual; Source Code (GEA 2.0 mandatory artifacts).
5. Key Expert Requirements	Title | Minimum Degree | Minimum Experience (Years) | Specific Skills Required — must align with MoCIT IT Norms 2082 categories. Do not specify qualifications significantly above IT Norms minimums without documented justification.
6. Data Ownership and Security	State explicitly: (a) 100% ownership of all source code, data, and documentation belongs to the government; (b) all staff must sign NDA; (c) no data to be hosted/ stored outside Nepal; (d) system must pass NCSC VAPT before deployment.
7. Payment Schedule	Tie ALL payments to verified delivery of specific deliverables. No advance payments beyond what PPR permits. Final payment (min. 10%) withheld until successful UAT completion and formal system handover.
8. Reporting Requirements	Frequency and format of progress reports; escalation procedures; change request process.

Technical Specifications: Software System

Use this template as the technical specification outline for Terms of Reference (ToR) — Consulting and Software Development and specification checklist for all custom software development and system deployment procurement. Bidders must complete the Compliance column and return it with their technical proposal.

Requirement	Specification	Bidder Compliance (Y/N/NA)
Web Accessibility	All citizen-facing web interfaces must meet WCAG 2.1 Level AA standards. Verified by automated accessibility scan before UAT.	
Mobile Responsiveness	All citizen-facing interfaces must be fully functional on mobile devices (screen widths 320px–1920px). Tested on Android and iOS browsers.	
Nepali Language	Citizen-facing content must be available in Nepali. All form labels, error messages, and instructions must be in Nepali Unicode.	
Low-Bandwidth Performance	All citizen-facing pages must fully load in under 5 seconds on a 1 Mbps connection. Verified via Lighthouse or equivalent during UAT.	

Requirement	Specification	Bidder Compliance (Y/N/NA)
API Standards (GEA 2.0)	All inter-system integrations must use REST architecture and JSON data format per GEA 2.0 requirements.	
Authentication	Role-based access control (RBAC); Two-Factor Authentication (2FA) mandatory for all administrator accounts.	
Encryption	HTTPS (TLS 1.2 minimum) for all web interfaces; all citizen PII encrypted at rest (AES-256 or equivalent).	
Source Code Ownership	Government retains 100% source code ownership; vendor provides full repository access from Day 1 of development. Final payment withheld until repository transfer confirmed.	
VAPT Clearance	No citizen-facing system may go live without NCSC VAPT clearance. All Critical and High findings must be remediated before go-live.	
Data Residency	All citizen and operational data stored, processed, and backed up exclusively within Nepal (GIDC hosting preferred per GEA 2.0).	
Audit Logging	All system access events, data modifications, and administrator actions must be logged with timestamp, user ID, and action. Logs retained minimum 2 years.	
Completed by Bidder:	_____ Designation: _____ Date: _____	

5.4.2 ToR Quality Checklist (M5-CK07) / ToR गुणस्तर जाँचसूची (M5-CK07)

Complete this checklist before any consultancy ToR is included in a bid document.

M5-CK07 | ToR Quality Checklist — Complete before publishing any consultancy RFP	
Check	Status
Is the objective, scope, and expected deliverables described precisely? Is the scope boundary (what is IN and what is OUT) clear?	[ ] Y [ ] N [ ] P
Do all Key Expert requirements comply with MoCIT IT Norms 2082 minimum qualifications? Are qualifications not set lower to favour unqualified bidders?	[ ] Y [ ] N [ ] P
Are all specifications brand-neutral performance benchmarks (no brand names without documented justification)?	[ ] Y [ ] N [ ] P
Are GEA 2.0 requirements specified: REST/JSON APIs; GIDC hosting evaluation; NID integration; source code ownership (government retains 100%)?	[ ] Y [ ] N [ ] P
Are all 9 GEA 2.0 mandatory artifacts listed as deliverables with payment milestones linked to each?	[ ] Y [ ] N [ ] P

M5-CK07 | ToR Quality Checklist — Complete before publishing any consultancy RFP	
Is NCSC VAPT clearance specified as a mandatory requirement before go-live (for all internet-facing systems)?	[ ] Y [ ] N [ ] P
Are QCBS evaluation criteria (with weightings totalling 100%) explicitly stated in the RFP document?	[ ] Y [ ] N [ ] P
Is data ownership clause (100% government) and data residency within Nepal specified?	[ ] Y [ ] N [ ] P
Is the NDA (M5-T16) referenced as a mandatory contract annex?	[ ] Y [ ] N [ ] P
IT Official: _____ Designated Authority: _____ Date: _____ Y=Yes / N=No / P=Partial	

Cross-Reference (🔗): Full ToR templates: M5-T04 (Goods with Installation), M5-T05 (Software Development), M5-T06 (ICT Consulting). Technical specifications: M5-T07 (Desktop/Laptop — includes PassMark score table), M5-T08 (Software System accessibility and security requirements). Full templates for M5-T04 through M5-T08 are provided above in this section.

Terms of Reference: ICT Goods with Installation

Use this ToR template when procuring ICT goods that require installation, configuration, or technical handover — e.g., servers, networking infrastructure, CCTV systems, structured cabling. This is different from the consulting ToR (M5-T05/M5-T06) used for software and advisory services.

ToR Section	Content Required
Contract Title:	[Insert — e.g., 'Supply and Installation of Desktop Computers and Network Switch — [LG Name] FY 2082/83']
Estimated Value:	NPR [Insert] (based on Market Price Survey M5-T25 attached to TCN M5-T03)
Procurement Method:	[Direct/SQ/NCB — verify with Threshold Tables in Section 5.2]
1. SCOPE OF SUPPLY	
Items to be supplied and installed:	[List all items from Technical Specifications — M5-T07/T08 — with quantities]
Installation requirements:	[Describe installation location, network integration, configuration required]
2. TECHNICAL SPECIFICATIONS	
Specifications reference:	Technical Specifications (M5-T07 for computers/laptops; M5-T08 for software systems; or custom spec attached as Annex). All specifications are brand-neutral and performance-based.
3. ACCEPTANCE AND WARRANTY	

Acceptance testing:	Supplier must participate in System Acceptance Testing (SAT — see Section 5.8). All items must pass SAT before final payment is released. SAT must be documented in M5-T20.
Warranty minimum standards:	Desktops/Laptops/Servers: Minimum 3 years on-site warranty. Authorized service center must be located in Gandaki Province or Pokhara. Peripherals: Minimum 1 year.
4. PAYMENT TERMS	
Payment milestone:	Minimum 10% of contract value withheld until signed System Acceptance Certificate (M5-T20) is received. No final payment before SAT completion.
5. DATA PROTECTION	
Pre-delivery security:	All default passwords changed before delivery. No pre-installed evaluation software, trial licenses, or bloatware. Vendor to provide written confirmation.

5.4.3 Technical Specifications Templates — ICT Goods and Software Systems
प्राविधिक विशेषता टेम्प्लेटहरू — ICT सामान र सफ्टवेयर प्रणाली

Purpose: Defines the technical requirements for off-the-shelf hardware and software goods procurements. Must be brand-neutral and performance-based.

Section	Required Content
1. General Requirements	State that all specifications are brand-neutral. Bidders may propose any product meeting or exceeding the minimum specifications. Equivalent or better performance to the specification is acceptable.
2. Minimum Technical Specifications Table	Feature | Required Minimum Specification | Bidder's Proposed Specification | Compliance (Y/N) Example for Laptop: Processor: Intel Core i5 12th Gen or equivalent | RAM: 16GB DDR4 | Storage: 512GB SSD | Display: 15.6" FHD | Battery: 6+ hours
3. Warranty and Support Requirements	Minimum warranty period (e.g., 3 years comprehensive onsite warranty). Parts and labor included. Response time for warranty claims. Local service center requirement (district or province level).
4. Energy Efficiency and Environmental Standards	Energy Star certification or equivalent. Power consumption limits. Disposal/recycling compliance (RoHS or equivalent).
5. Delivery and Installation	Maximum delivery period from contract signing date. Installation and commissioning responsibility. Acceptance testing procedure.
6. Documentation	User manual (Nepali or English). Technical/service manual. Software licenses and certificates of authenticity.

Brand-Neutral Specification Principles — Prohibited vs Required Language

CRITICAL: Writing brand-specific specifications is among the most common CIAA findings in ICT procurement. The table below shows exactly what language is prohibited and what is required for audit-safe specifications.

Specification Element	PROHIBITED (Creates CIAA Risk)	REQUIRED (Audit-Safe)
Processor	'Intel Core i7' or 'AMD Ryzen 5'	'Minimum 8 Core, 2.4 GHz clock speed, 25MB L1 Cache, 'Minimum PassMark benchmark score of 15,000 (verified at passmark.com)'
Memory	'Samsung DDR4' or 'Crucial RAM'	'Minimum 16 GB DDR4-3200 MHz or faster'
Storage	'Western Digital SSD' or 'Seagate'	'Minimum 512 GB NVMe PCIe 3.0 SSD (read speed ≥ 2,400 MB/s)'
Network Equipment	'Cisco 24-port switch' or 'HP ProCurve'	'24-port managed Gigabit Ethernet switch, SNMP v3, IEEE 802.3, rack-mountable'
Operating System	'Windows 11 Home'	'Licensed Windows 11 Pro (minimum); genuine COA sticker affixed to device'
Printer	'HP LaserJet' or 'Canon i-SENSYS'	'A4/A3 monochrome laser; minimum 30 ppm; duplex; network-enabled; toner yield ≥ 3,000 pages'
UPS	'APC Smart-UPS'	'Pure sine wave UPS; minimum 1 kVA / 0.6 kW; minimum 30-minute battery runtime at full load'
Server	'Dell PowerEdge'	'2U rack server; minimum 2× CPU sockets; minimum 32 GB ECC RAM; minimum RAID 5 storage'

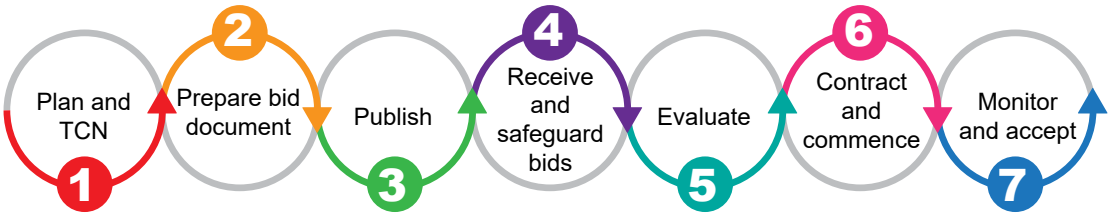
5.5 ICT Procurement Process / ICT खरिद प्रक्रिया

Every ICT procurement — regardless of method or value — follows the same fundamental sequence. This SOP applies to goods, software, consulting, and AMC procurement. Steps cannot be skipped. The designated authority approves at the start (TCN) and the end (contract award). The IT Official manages the process in between.

- **Start gate:** Approved TCN (M5-T03) + item in Annual ICT Plan (M5-T01) — BOTH required before any bid is published
- **Specification gate:** Brand-neutral, performance-based specs — brand names in ToR/specs = PPA violation
- **Anti-corruption gate:** Template 3 Red Flag Checklist (M5-T24) — complete BEFORE publishing bid
- **Evaluation gate:** Template 1 Eligibility Test (M5-T10) BEFORE technical scoring; Template 2 QCBS Matrix (M5-T11) for scoring

- **End gate:** System Acceptance Certificate (M5-T20) — signs off go-live and gates final payment

SOP 5.5 | ICT Procurement Process



SOP 5.5 | ICT Procurement Process — Applies to all procurement types: Goods, Software/Consulting, AMC	
Purpose	Execute PPA 2063-compliant procurement from Annual Plan to contract signing. All types follow this sequence — the evaluation method differs (Goods: lowest compliant bid; Consulting/Software/AMC: QCBS 80:20).
Steps	1. Plan and TCN: Confirm the item is in the Annual ICT Procurement Plan (M5-T01). Prepare TCN (M5-T03) with cost estimate (M5-T25 for goods; M5-T09 for consulting). Obtain designated authority approval on TCN before proceeding. 2. Prepare bid document: Goods: use M5-T04 with brand-neutral specifications (M5-T07/08). Consulting/Software: use M5-T05/06 ToR with IT Norms-compliant Key Expert requirements and QCBS criteria. Complete Anti-Corruption Template 3 Red Flag Checklist (M5-T24 Section 5.7) before publishing. Use PPMO Standard Bidding Documents — do not create from scratch. 3. Publish: Publish on e-GP portal (bolpoatra.com.np) when threshold required. Observe minimum notice periods from Table 5.2. Send RFP to shortlisted firms for consulting. Do not accept bids submitted after the deadline. 4. Receive and safeguard bids: For consulting: keep technical and financial envelopes physically separate and sealed until evaluation. Opening financial envelopes before technical evaluation is a procedural irregularity. 5. Evaluate: Goods — Stage 1: Eligibility (M5-T10 Template 1). Stage 2: Technical specification compliance. Stage 3: Award to lowest compliant bidder.Consulting — Stage 1: Eligibility (Template 1). Stage 2: Technical evaluation using QCBS Mathematical Matrix (M5-T11 Template 2) — minimum 70/100 to open a financial envelope. Stage 3: Financial evaluation formula: Score = (Lowest Bid ÷ This Firm's Bid) × 20. Award to highest combined QCBS score. 6. Contract and commence: Sign Standard Contract + NDA (M5-T16) + SLA (if services) — all three before any work commences or system access is granted. Obtain Performance Security as required by PPA 2063. File complete procurement record for CIAA Investigation. 7. Monitor and accept: Monitor deliverables against milestones. For consulting: link each GEA 2.0 artifact to a payment milestone. Sign System Acceptance Certificate (M5-T20) only after all required tests, UAT, and VAPT are complete. Register assets in PAMS within 7 working days.

For step 6-8

M5-CK01 | Consolidated ICT Procurement Compliance Checklist — Complete at each stage	
Check	**Status**
PRE-PROCUREMENT	

M5-CK01 | Consolidated ICT Procurement Compliance Checklist — Complete at each stage	
Item included in Annual ICT Procurement Plan (M5-T01) for current fiscal year	[ ] Yes [ ] No — supplement required
TCN (M5-T03) approved by designated authroity before procurement commenced	[ ] Yes [ ] No — STOP
Cost estimate: Market Survey (M5-T25) attached (goods) OR IT Norms Worksheet (M5-T09) attached (consulting)	[ ] Yes [ ] No — STOP
Correct procurement method selected based on estimated value (Table 5.2)	[ ] Confirmed: [Method]
BID DOCUMENT AND PUBLICATION	
Specifications are brand-neutral performance benchmarks — no brand names without documented justification	[ ] Yes [ ] No — revise first
PPMO Standard Bidding Document used — not a custom document	[ ] Yes [ ] No — use SBD
ToR Quality Checklist (M5-CK07) completed for consulting/software procurement	[ ] Done [ ] N/A (goods)
Anti-Corruption Red Flag Checklist (M5-T24) completed before bid publication — all items resolved	[ ] Done [ ] Outstanding — resolve first
e-GP portal publication completed when threshold requires	[ ] Done [ ] N/A (below threshold)
Break Table here	
BID EVALUATION	
Evaluation criteria finalized and published in bid document BEFORE bids were received	[ ] Yes [ ] No — serious irregularity
Template 1 (Integrity Eligibility Test) completed for ALL bidders before technical scoring	[ ] Done [ ] N/A (goods)
Technical and financial envelopes kept separate (consulting); financial opened only for firms scoring ≥70/100	[ ] Done [ ] N/A (goods)
Evaluation report signed by all evaluation committee members	[ ] Done
CONTRACT AND POST-AWARD	
NDA (M5-T16) signed by vendor BEFORE any system access or data sharing	[ ] Done — date: ___
Contract includes: data ownership, source code ownership, data residency, SLA (if services) — M5-T13	[ ] Yes [ ] Missing clauses — add before signing
System Acceptance Certificate (M5-T20) signed before final payment released	[ ] Done [ ] Payment withheld pending
Assets registered in PAMS within 7 working days of acceptance	[ ] Done [ ] N/A (consulting)

M5-CK01 | Consolidated ICT Procurement Compliance Checklist — Complete at each stage		
IT Official: _____	designated authority: _____	Date: _____
		Y = Yes / N = No / P = Partial

5.6 IT Consulting Cost Estimation — IT Norms 2082

परामर्श सेवा लागत अनुमान — IT Norms 2082

Using rates higher than IT Norms 2082 without documented designated authority justification is the most common ICT CIAA/OAG Investigation finding in Gandaki Province LG offices. The 5-step procedure below is for all ICT consulting and software development cost estimates.

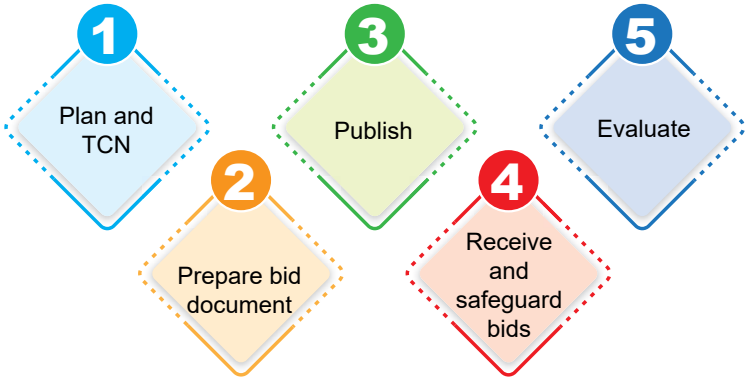
Legal Basis (⚖️):

MoCIT IT Norms 2082: For ALL ICT consulting and software development cost estimates and ToR Key Expert qualifications. Verify current rates at mocit.gov.np on the date of TCN preparation — rates are updated annually. Record the URL and access date in M5-T09.

Applying IT Norms 2082 rates to all consulting cost estimates is under PPA 2063. A worked numerical example of IT Norms rate application is in the Annex. The procedure below specifies the steps; the worksheet (M5-T09) records the calculation.

- Download current rates first — IT Norms are updated annually at mocit.gov.np. Never use rates from a previous procurement without verifying the current version.
- Rate calculation = Person-months × Monthly rate × Role factor — the M5-T09 worksheet automates this
- Above-Norms rates: Require written justification approved by the designated authority — document in the TCN
- Rates apply to all ICT roles: Project Manager, Senior Developer, Junior Developer, Database Admin, Systems Analyst, QA Engineer, Network Engineer, IT Trainer, etc.

SOP 5.6 | Consulting Cost Estimation



SOP 5.6 | ICT Consulting Cost Estimation — 5-Step Procedure (IT Norms 2082)	
Purpose	Produce a legally defensible, IT Norms-compliant cost estimate for all ICT consulting and software development procurements.

Steps	
	1. **Role Identification:** Based on the approved TCN scope, list ONLY roles genuinely required. Map each role to IT Norms 2082 categories. Do not add roles to inflate the budget. 2. **Qualification Check:** Verify minimum academic degree and years of experience per IT Norms for each role. ToR Key Expert requirements must match IT Norms minimums — never set lower. 3. **Rate Application:** Apply current IT Norms 2082 monthly rates. Current indicative rates (verify at mocit.gov.np): Team Leader / PM: NPR 200,000/month · System Architect / Sr. Analyst: NPR 160,000/month · Senior Developer / Database Designer: NPR 140,000/month. 4. **Calculate using the formula:** Total Personnel Cost = Σ (Monthly Rate × Estimated Person-Months) for each role. Add: Reimbursable Costs (travel, workshops, printing, other documented direct costs). Add: Contingency — **maximum 10%** of (Personnel + Reimbursables). Contingency above 10% requires written designated authority justification. 5. **Verify and document:** Check all rates against current mocit.gov.np on the day of TCN preparation. Record URL and access date in M5-T09. Attach M5-T09 to the TCN. designated authority signature on TCN approves the cost estimate — file M5-T09 as a permanent procurement record.

M5-T09 | IT Consulting Cost Estimation Worksheet (IT Norms 2082) — Attach to every consulting TCN

Role (per IT Norms 2082)	IT Norms Min. Qualification	Monthly Rate (NPR)[Verify at mocit.gov.np]	Estimated Person-Months	Sub-Total (NPR)
Team Leader / Project Manager	Master's in IT + 5 yrs exp	NPR 200,000	[Months]	NPR [Calc]
System Architect / Senior Analyst	Bachelor's + cert + 5 yrs	NPR 160,000	[Months]	NPR [Calc]
Senior Developer / Database Designer	Bachelor's in IT + 5 yrs	NPR 140,000	[Months]	NPR [Calc]
[Additional role — specify]	[Per IT Norms]	NPR [Verify]	[Months]	NPR [Calc]
A. TOTAL PERSONNEL COST				NPR [Sum]
B. REIMBURSABLE COSTS	Travel: NPR [ ] Workshops: NPR [ ] Printing: NPR [ ] Other: NPR [ ]			NPR [Sum B]
C. CONTINGENCY (MAX 10% of A+B)	(A + B) × [up to 10%] Note: above 10% requires designated authority written justification			NPR [Max 10%]
TOTAL ESTIMATED CONTRACT VALUE (A+B+C)				NPR [Grand Total]
IT Norms version verified:	Date: ___ URL: mocit.gov.np Verified by IT Official: ___ designated authority Approval on TCN: ___			

Completed by: _____ Designation: _____ Date: _____

5.7 Bid Evaluation — Direct Purchase and QCBS Methods
बोलपत्र मूल्याङ्कन — प्रत्यक्ष खरिद र QCBS विधिहरू

5.7.1 Direct Purchase Bid Evaluation (Goods and Services)
प्रत्यक्ष खरिद बोलपत्र मूल्याङ्कन (सामान र सेवा)

For direct purchase of ICT goods and services (Sealed Quotation, Catalog Shopping, Limited Tendering, and similar methods under Section 5.2), evaluation compares the office-specified technical requirements against each supplier's quoted specifications, verifies warranty and authorization documents, and ranks compliant bidders by price.

M5-CK02	Direct Purchase Bid Evaluation Checklist — Complete for goods/services procured by Direct Selection, Sealed Quotation, Catalog Shopping, or Limited Tendering	
Check		Status
Supplied specification meets or exceeds the Technical Specifications (Section 5.4) — item by item		[ ] Compliant [ ] Non-compliant
Warranty terms meet the minimum standards for the item category		[ ] Yes [ ] No — STOP
Manufacturer/Authorized Dealer Certificate provided (where the method requires an authorized dealer)		[ ] Yes [ ] N/A
Quoted price checked against the Market Price Survey (M5-T25)		[ ] Yes [ ] No — STOP
At least 3 quotations obtained and compared (or justification recorded if fewer)		[ ] Yes [ ] No — STOP
Delivery timeline confirmed and stated in the purchase order/contract		[ ] Yes [ ] No
Financial comparative table completed and attached to the procurement file		[ ] Yes [ ] No — STOP

5.7.2 QCBS Evaluation — Consulting and Software
QCBS मूल्याङ्कन — परामर्श र सफ्टवेयर

Three templates must be used in sequence for all consulting and software procurement evaluations. They convert legal requirements into operational tools.

Sequence: Template 1 (Integrity Gateway — before scoring) → Template 2 (QCBS Mathematical Matrix — technical scoring) → Template 3 (Red Flag Checklist — before bid publication). Template 3 is completed first in practice.

QCBS (Quality and Cost-Based Selection) is mandatory for ALL government ICT consulting procurement (PPR 2064). The three templates below must be used in sequence — skipping any template is a PPA violation. A fully-worked QCBS scoring example is in the Annex.

- Template 1 (M5-T10) — Eligibility Gate: Must be completed FIRST. Any bidder who fails any item is immediately disqualified — their technical proposal is not opened.
- Template 2 (M5-T11) — Technical Scoring: Only bidders who PASSED Template 1 proceed here. Technical score = 80% of total. Mathematical scoring only — no subjective scoring ranges.
- Template 3 (M5-T24) — Pre-Publication Red Flag Check: Complete BEFORE publishing the bid document. Any STOP item must be resolved before publication.

- QCBS ratio: 80% technical quality + 20% financial price. The technically strongest proposal usually wins even if not the cheapest.

Template 1 — Integrity-Based Eligibility Test (Mandatory Gateway — Complete Before Technical Scoring)

M5-T10 | Integrity-Based Eligibility Test — Every bidder must PASS ALL items before technical scoring commences					
Eligibility Criterion	Legal Basis	Verification	Bidder A	Bidder B	Bidder C
1. No active corruption case filed in Court against firm or Directors (PPR Rule 65A)	PPR 2064, Rule 65A	Written declaration by firm; verify with CIAA if in doubt	[ ] P [ ] F	[ ] P [ ] F	[ ] P [ ] F
2. Not blacklisted by PPMO or any government body	PPA 2063, Sec 63	Check ppmo.gov.np blacklist; print screenshot with date	[ ] P [ ] F	[ ] P [ ] F	[ ] P [ ] F
3. No conflict of interest — firm did not prepare ToR or specifications	PPA 2063, Sec 61	Written declaration; IT Official verifies from own knowledge	[ ] P [ ] F	[ ] P [ ] F	[ ] P [ ] F
4. Proposed Key Experts meet IT Norms 2082 minimum qualifications	IT Norms 2082	Cross-check CV and certificates against IT Norms minimums	[ ] P [ ] F	[ ] P [ ] F	[ ] P [ ] F
5. Valid registration and current tax clearance	PPA 2063	Physical inspection; verify validity dates	[ ] P [ ] F	[ ] P [ ] F	[ ] P [ ] F
GATEWAY RESULT: ALL 5 must PASS to proceed to Technical Scoring (M5-T11)			P/F	P/F	P/F

Evaluation Committee Members:	1. _____ 2. _____ 3. _____ Date: _____

Template 2 — QCBS Mathematical Evaluation Matrix (Technical 80% + Financial 20%)

M5-T11 | QCBS Technical Evaluation Matrix — Mathematical scoring only. No subjective point ranges.			
Evaluation Category	Max Pts	Scoring Formula (Remove All Subjective Discretion)	Score (Bidder)
1. Firm's Specific Experience	20	Formula: (No. of similar GoN ICT projects completed in last 5 years ÷ 5) × 20. Maximum 20 points. Non-GoN projects score 0 unless ToR specifies otherwise.	/20
2. Methodology and Work Plan	20	Binary scoring (No subjective range):• DNF 2.0/GEA 2.0 compliance plan present and technically coherent: Yes = 10, No = 0• Proposed timeline feasible within contract period with milestones: Yes = 10, No = 0	/20

M5-T11 | QCBS Technical Evaluation Matrix — Mathematical scoring only. No subjective point ranges.			
Evaluation Category	Max Pts	Scoring Formula (Remove All Subjective Discretion)	Score (Bidder)
3. Key Expert: Team Leader	20	IT Norms 2082 baseline (Pass/Fail gate — must meet minimum qualification to score):• Meets IT Norms minimum: PASS (required to score); FAIL = 0 for entire category• Points: 2 points per additional year of experience above IT Norms minimum (max 20 total)	/20
4. Key Expert: Technical Specialist	20	Certification-based binary scoring:• Holds relevant recognized certification (CISA/CISSP/Database/PMP/CISM): Yes = 20, No = 0• Claimed certification must be evidenced by certificate copy in technical proposal	/20
TECHNICAL SUB-TOTAL (min. 70/100 to open financial envelope)	100	Financial envelope opened ONLY if Technical Sub-Total ≥ 70 points.	/100
TECHNICAL WEIGHT (80%)	80	Technical Sub-Total × 0.80	/80
5. Financial Proposal	20	Fixed formula (no discretion):Score = (Lowest Bid Price ÷ This Firm's Bid Price) × 20	/20
COMBINED QCBS SCORE (Technical 80% + Financial 20%)	100	Award to firm with highest combined score. Equal scores: higher technical score takes precedence.	/100
RECOMMENDATION		Firm [ ] with QCBS Score [ ]/100 and proposed cost NPR [ ] — recommended for award. All committee members sign below.	

Evaluation Committee:	1. _____ 2. _____ 3. _____ Designated Authority Approval: _____ Date: _____

Template 3 — Pre-Publication Governance Checklist (Complete BEFORE publishing any bid)

M5-T24 | Red Flag Checklist — IT Official and designated authority both sign. Any STOP item must be resolved before bid publication.	
Check	**Status**
Category: SPECIFICATIONS AND COST ESTIMATE	
Brand-specific names (Cisco, HP, Dell, Microsoft) used without documented technical justification? → STOP: Rewrite using performance benchmarks (PassMark, RAM/ speed minimums).	[ ] OK [ ] STOP
Cost estimate for goods NOT based on 3+ written quotations (M5-T25)? → STOP: Complete market survey first.	[ ] OK [ ] STOP

M5-T24 | Red Flag Checklist — IT Official and designated authority both sign. Any STOP item must be resolved before bid publication.	
Cost estimate for consulting NOT based on IT Norms 2082 rates (M5-T09)? → STOP: Redo using IT Norms.	[ ] OK [ ] STOP
Contingency exceeds 10% without written designated authority justification? → STOP: Cap at 10% or obtain written justification.	[ ] OK [ ] STOP
Category: PROCUREMENT PROCESS	
Procurement NOT in Annual ICT Procurement Plan (M5-T01)? → STOP: Supplementary amendment with designated authority approval required.	[ ] OK [ ] STOP
Project split into smaller contracts to avoid threshold? → STOP: Threshold splitting is a serious irregularity under PPA 2063 Section 38.	[ ] OK [ ] STOP
e-GP publication not arranged when procurement value requires it? → STOP: e-GP publication failure is a stand-alone irregularity.	[ ] OK [ ] STOP
Evaluation criteria NOT yet finalized and documented? → STOP: Criteria must be pre-defined before bid publication.	[ ] OK [ ] STOP
Category: EVALUATION AND CONTRACT	
Any evaluation committee member has personal or financial connection to a known bidder? → STOP: Disqualify conflicted members; appoint replacement.	[ ] OK [ ] STOP
Template 1 (Integrity Gateway) NOT yet completed for all bidders before technical scoring? → STOP: Complete Template 1 first.	[ ] OK [ ] STOP
Contract does NOT include: data ownership, source code ownership, data residency, Step-in Rights clauses (M5-T13)? → STOP: Add mandatory clauses before signing.	[ ] OK [ ] STOP
NDA (M5-T16) NOT yet signed by vendor before any system access or data sharing? → STOP: NDA must be signed before any access.	[ ] OK [ ] STOP
Final payment released before System Acceptance Certificate (M5-T20) signed? → STOP: Payment withheld until M5-T20 signed.	[ ] OK [ ] STOP
NCSC VAPT clearance NOT received before the citizen-facing software system goes live? → STOP: No go-live without VAPT clearance.	[ ] OK [ ] STOP
IT Official: _____ Designated Authority: _____ Date: _____ Y=Yes / N=No / P=Partial	

5.7.3 Bid Evaluation Report / बोलपत्र मूल्याङ्कन प्रतिवेदन

Before contract award, the evaluation committee prepares a formal Bid Evaluation Report, signed by all committee members, documenting: all bids received; the eligibility, technical, and financial results for each bidder; the combined QCBS score where applicable; and the recommended awardee with justification. The report is a mandatory procurement record and the primary evidence produced for OAG/CIAA review of the award decision.

System Acceptance Certificate — M5-T20 (Key Fields)

Field	Details
Contract / Purchase Order Reference	[Insert TCN M5-T03 and contract reference numbers]
Vendor Name	[Insert]
Scope of Acceptance	[ ] Goods [ ] Software/System [ ] Consultancy Deliverable [ ] AMC/ Service
Deliverables Verified Against	ToR/Technical Specifications (Section 5.4) and approved TCN (Section 5.3)
Post-Delivery Inspection (PDI) Completed	[ ] Yes — Date: _____ [ ] No — STOP
UAT Completed (software/ systems only)	[ ] Yes — Date: _____ [ ] N/A
NCSC VAPT Clearance (citizen-facing systems only)	[ ] Yes — Date: _____ [ ] N/A
Outstanding Deficiencies	[ ] None [ ] Listed with remediation deadline: _____
Warranty Start Date	[Insert — commences from this Certificate's date]
Asset Registered in ICT Asset Register (F 4.14)	[ ] Yes — Date: _____ [ ] N/A (services only)
Final Payment Authorized	[ ] Yes — releases remaining contract value [ ] Withheld — reason: _____
IT Official	Signature: _____ Date: _____
Designated Authority	Signature: _____ Date: _____
Vendor Representative	Signature: _____ Date: _____

5.8 Contract Award and Signing / सम्झौता स्वीकृति र हस्ताक्षर

5.8.1 Key Contract Templates / मुख्य सम्झौता टेम्प्लेटहरू

All three documents below must be signed before any work commences, system access is granted, or data is shared with a vendor. The sequence is: (1) NDA signed first. (2) Contract signed (includes mandatory clauses). (3) SLA or AMC signed as mandatory annex. No exceptions.

Mandatory ICT Contract Clauses — M5-T13

The following clauses must appear in every ICT contract, regardless of value. A contract missing any of these clauses creates legal liability for the signing officer.

Clause	Requirement	Why Mandatory
1. Data Ownership	100% of all citizen and operational data is exclusive government property. Vendor has no ownership claim. Data ownership does not transfer under any circumstances including non-payment or contract disputes.	Privacy Act 2075; GEA 2.0; prevents vendor data hostage situations
2. Source Code Ownership	The government retains 100% ownership of all source code, scripts, databases, and documentation. Vendor provides government repository access from Day 1. Upon termination: complete final repository snapshot, build instructions, and documentation.	GEA 2.0; prevents vendor lock-in; protects government investment
3.Data Residency	All citizen and government data stored, processed, backed up, and replicated exclusively within Nepal. Vendors may not store data on servers outside Nepal under any circumstances.	Data Center Directives 2081; Privacy Act 2075
4. Security Obligations	Vendor complies with National Cybersecurity Policy; ISO 27001 principles; all ToR security requirements. Facilitate NCSC VAPT (whitelist 202.45.145.183). Report security incidents within 2 hours.	National Cybersecurity Policy; ETA 2063
5. NDA	NDA (M5-T16) is incorporated by reference. All vendor staff and sub-contractors accessing government systems or data must sign NDA before access.	Privacy Act 2075; ETA 2063
6. Exit Management	On termination: 90-day transition period at contracted rates; data transferred in open machine-readable format; complete documentation and source code; data certified deleted within 30 days.	GEA 2.0; data protection
7. Payment Milestones	No payment released without delivery and IT Official approval of corresponding GEA 2.0 artifact. Final payment (minimum 10%) released only after signing the System Acceptance Certificate (M5-T20).	PPA 2063; GEA 2.0 compliance enforcement
8. Subcontracting	Vendors may not subcontract significant work without prior written approval. All sub-contractors bound by NDA and data protection obligations.	PPA 2063
9. Step-in Rights	If a vendor fails SLA obligations for 3 consecutive months or abandons a critical system, the government may appoint a third party at the vendor's cost. Activated by written notice from designated authority after 30-day Performance Improvement Notice period.	Service continuity protection
10. Dispute Resolution	Good-faith negotiation within 30 days, then Nepal arbitration/judicial authority per PPA 2063.	PPA 2063

Every ICT contract — regardless of value — must include the mandatory clauses in M5-T13. The templates below address the four most critical contract types.

- NDA (M5-T16) — Sign before any system access or citizen data sharing. Non-negotiable. No exceptions.

- AMC (M5-T17) — Annual maintenance and support. Includes SLA targets, escalation matrix, and penalty clauses.
- System Acceptance Certificate (M5-T20) — Signed after successful UAT. Gates the final payment. Cannot be delegated below IT Official level.
- Practical examples of filled contract templates are in the Annex. The mandatory clauses checklist (M5-T13) applies to ALL contracts including those not listed here.

Non-Disclosure Agreement — M5-T16 (Sign BEFORE any system access or data sharing)

M5-T16 | Non-Disclosure Agreement (NDA) — Key Provisions and Signature Block	
NDA Provision	**Obligation on Vendor**
1. Confidential Information Definition	ALL information disclosed by the government: citizen data; system architecture; source code; API credentials; financial data; security configurations; official communications.
2. Permitted Use	Confidential Information may ONLY be used for the specific purpose of this contract. No other use. No sharing with third parties without written approval.
3. Security Standard	Vendor applies security measures no less rigorous than ISO 27001 — minimum AES-256 encryption at rest; TLS 1.2+ in transit.
4. Breach Notification	Report any actual or suspected breach to the IT Official within **2 hours** of detection.
5. Duration	NDA commences before any access is granted. Obligations continue for **3 years** after contract termination.
6. Return of Data	On termination: return all confidentialinformation; certify destruction of all electronic copies in writing within 30 days; confirm revocation of all system access credentials within 24 hours.
7. Consequences of Breach	Civil claim for full damages; report to Nepal Police Cyber Bureau (+977-1-4412523) under ETA 2063; permanent disqualification from government contracts.
Signing:	Date of NDA MUST precede date of first system access. Both dates verifiable by OAG. Government Representative: _____ Date: _____ Vendor Representative: _____ Date: _____Witnesses (2 required): 1. _____ 2. _____
Completed by: _____ Designation: _____ Date: _____	

5.8.2 Project Kick-off and Monitoring / परियोजना सुरुवात र अनुगमन

Within 10 working days of contract signing, the IT Official convenes a formal project kick-off meeting with the vendor, recording attendees, the confirmed delivery schedule, and communication protocol. Monitoring milestones are aligned with the payment schedule and each GEA 2.0 artifact gate (Module 6, Section 6.2); the IT Official acts as contract administrator, verifying deliverables against the ToR/ Technical Specifications before authorizing any payment. For AMC and service contracts, monthly SLA monitoring begins immediately using the SLA Performance Report (M5-T15, Section 5.9).

5.8.3 Contract Close-out and Post-Delivery Inspection / सम्झौता समापन र डेलिभरी पछिको निरीक्षण

On completion, the IT Official and vendor jointly conduct a Post-Delivery Inspection (PDI), checking every deliverable against the ToR/Technical Specifications and recording any deficiencies with a remediation deadline. Once all items pass, and UAT/VAPT clearance is on file where applicable, the IT Official and

designated authority sign the System Acceptance Certificate (M5-T20, below) — this gates release of the final payment. Assets are then registered in the ICT Asset Register (F 4.14, Module 4) within 7 working days, and the warranty period is recorded as commencing from the Certificate date.

Annual Maintenance Contract Template — M5-T17 (Key Provisions)

AMC Provision	Requirement
Scope of Coverage	List covered equipment/systems with Asset IDs (F 4.14). Define: Comprehensive AMC (includes spare parts) vs Non-Comprehensive (labour only). Clearly define what is included and excluded.
Minimum Warranty — Mandatory	Desktops, laptops, servers: minimum 3 years. Printers, UPS, peripherals: minimum 1 year. Network equipment: minimum 2 years. Warranty commences from System Acceptance Certificate date.
Local Service Center	Vendors must maintain an authorized service center in the office geographical location. On-site repair within 3 working days of fault notification. Temporary replacement for P1 failures.
SLA Targets	P1 (completely non-functional): on-site response 4 hours, resolution 24 hours. P2 (degraded): next business day response, 3 days resolution. P3 (minor): 2 business days response, 7 days resolution.
Penalty Clause	P1 breach: minimum 0.5% of monthly AMC fee per hour of excess downtime. P2 breach: minimum 0.1% per breach beyond monthly budget. Maximum monthly deduction cap: 30% of monthly AMC fee.
Monthly SLA Report	Vendor submits SLA Performance Report (M5-T15) with each monthly invoice. IT Official reviews against KPIs before approving payment. Penalties deducted from invoice automatically.
NDA Requirement	NDA (M5-T16) signed before any vendor access to systems or data containing citizen PII. All AMC technicians accessing the server room must sign Server Room Entry Log (F 4.11).
Payment	Monthly equal installments only after the SLAreport is received and reviewed. designated authority must approve any waiver of penalty deduction — not IT Official alone.

Cross-Reference (🔗): System Acceptance Certificate (M5-T20) — used for both goods and software acceptance, linking physical asset registration, VAPT clearance, and GEA 2.0 artifact verification to the final payment trigger. The full M5-T20 template is provided above in Section 5.8.

5.9 Vendor Management / विक्रेता व्यवस्थापन

Vendor management does not end at contract signing. Monthly SLA monitoring, quarterly performance scoring, and documented corrective action when performance falls below threshold — all create the audit record needed to enforce contract penalties and, in the worst case, activate Step-in Rights (M5-T13 Clause 9).

Vendor management extends beyond contract signing. Active monitoring protects citizens from service failures and the government from audit arrears. Three tools manage the full vendor relationship lifecycle.

- **Before award (M5-T21):** Risk assessment — due diligence on financial stability, PPMO blacklist check, technical capacity, and reference verification. For critical/high contracts only.
- **During contract (M5-T22 + M5-T15):** Quarterly performance scorecard + monthly SLA report submitted by vendor with invoice. Scores below 18/30 trigger a formal Performance Improvement Plan.
- **Escalation:** Vendors scoring below threshold two consecutive quarters: withhold payment pending performance improvement or terminate per contract Step-in Rights clause.
- **Blacklist check:** Always verify PPMO blacklist (ppmo.gov.np) BEFORE contract award — Template 1 (M5-T10) includes this check.

Vendor Risk Assessment — M5-T21 (Complete Before Award for Critical/High Vendors)

M5-T21 | Vendor Risk Assessment Checklist — Complete before awarding Critical or High criticality contracts	
Check	Status
MANDATORY CHECKS — Must pass ALL (applies to every vendor)	
No active corruption case (PPR Rule 65A)? Verified with CIAA or written declaration.	[ ] Pass [ ] Fail
Not blacklisted by PPMO? Screenshot with date from ppmo.gov.np.	[ ] Pass [ ] Fail
No conflict of interest — did not prepare ToR/specifications?	[ ] Pass [ ] Fail
All Key Expert qualifications meet IT Norms 2082 minimums? CVs and certificates reviewed.	[ ] Pass [ ] Fail
ADDITIONAL CHECKS — Required for Critical/High vendors	
Financial health: audited accounts for the last 3 years provided (for contracts above RFP threshold)?	[ ] Pass [ ] Fail [ ] N/A
Government project references: minimum 2 similar GoN ICT contracts in last 3 years with verifiable references?	[ ] Pass [ ] Fail [ ] N/A
Local service capability: authorized service center in Gandaki Province or Pokhara?	[ ] Pass [ ] Fail [ ] N/A (consulting)
NDA signed before any government data or system access granted?	[ ] Pass [ ] Fail
Data residency commitment: written guarantee all data within Nepal?	[ ] Pass [ ] Fail
DoIT enlistment verified (for data center/cloud vendors)? Registry at doit.gov.np.	[ ] Pass [ ] Fail [ ] N/A
Sub-contractors disclosed? All bound by NDA and data protection clauses?	[ ] Pass [ ] Fail [ ] N/A
VERDICT:	[ ] LOW RISK — proceed [ ] MEDIUM RISK — additional safeguards [ ] HIGH RISK — designated authority review required before award
IT Official: _____ Designated Authority: _____ Date: _____ Y=Yes / N=No / P=Partial	

Vendor Performance Scorecard — M5-T22 (Complete Quarterly for All Active Vendors)

M5-T22 | Vendor Performance Scorecard — Thresholds: 25-30=Excellent | 18-24=Satisfactory | Below 18=Warning — issue Performance Improvement Plan			
Category	Max	Scoring Criteria (Objective)	Score
1. SLA Compliance — Uptime	10	10: Zero uptime breaches. 8: One minor breach resolved within 4 hrs. 5: One significant breach resolved within 12 hrs. 0: Multiple breaches or unresolved.	/10
2. Incident Response	10	10: 100% P1/P2 responses within SLA targets. 7: One P1/P2 response breach. 4: Two P1/P2 breaches. 0: Three or more P1/P2 breaches.	/10
3. Reporting and Communication	5	5: All monthly SLA reports submitted on time with invoice. 3: One report late. 0: Two or more reports missing or late.	/5
4. Security Compliance	5	5: All patches applied within SLA timelines; NDA maintained; no breaches. 3: One patch delay under 30 days. 0: Critical patch missed; NDA breach; any security incident.	/5
TOTAL	30	Actions: 25-30=Process invoice normally. 18-24=Note improvement areas. Below 18=Issue written PIP within 5 business days. Two consecutive quarters below 18=Consider Step-in Rights (Clause 9, M5-T13).	/30
Action taken:	[ ] Invoice processed [ ] SLA penalties deducted: NPR ___ [ ] PIP issued — date: ___ [ ] Step-in Rights under consideration		
Completed by: _____ Designation: _____ Date: _____			

M5-T15 | SLA Performance Report — Vendor submits monthly with invoice. IT Official reviews before payment.					
KPI	SLA Target (per contract)	Actual This Month	Breaches	Penalty (NPR)	Evidence
System uptime (business hours)	[e.g., 99.5%]	[Actual %]	[Yes/No]	NPR [Amount]	[Screenshot/log]
P1 incident response time	[e.g., 4 hrs on-site]	[Average actual]	[No. of breaches]	NPR [Amount]	[Incident log]
P1 incident resolution time	[e.g., 24 hrs]	[Average actual]	[No. of breaches]	NPR [Amount]	[Incident log]
Monthly maintenance completed	[Scheduled tasks]	[Completed Y/N]	[No. missed]	NPR [Amount]	[Maintenance record]
TOTAL SLA PENALTIES THIS MONTH:				NPR [Total]	

M5-T15 | SLA Performance Report — Vendor submits monthly with invoice. IT Official reviews before payment.					
Invoice Amount Claimed:	NPR [Amount]	Net Amount after Penalty:	NPR [Claim minus penalties]		
IT Official Verification:	[ ] SLA Report verified [ ] Penalty deductions confirmed [ ] Invoice APPROVED for payment [ ] Invoice WITHHELD — reasons: ___				

5.10 Procurement Scenario Navigator / खरिद परिदृष्य मार्गदर्शक

Quick-reference guide for the most common ICT procurement situations in Gandaki Province LG offices. Verify current threshold values at ppmo.gov.np before applying any method.

Scenario	Typical Value — Gandaki Province LG	Method	Critical Protections	Most Common Mistake
A: Laptops/Desktop Computers Standard hardware refresh	NPR 2,00,000–6,00,000 (rural, 5-10 units) NPR 6,00,000–20,00,000 (urban, bulk)	Below NPR 10L: Sealed QuotationAbove NPR 10L: Open IFQ or NCB[Verify Table 5.2]	Market Survey M5-T25 (3 quotes) · Brand-neutral specs with PassMark scores · 3-year warranty · Local service center · COA verification at acceptance · PAMS registration within 7 days	Writing 'HP laptop' or 'Dell computer' in specs · Not requiring local service center · Not verifying COA stickers · Not registering in PAMS
B: Server Procurement For local data hosting	NPR 3,00,000–8,00,000 (entry-level)NPR 8,00,000–20,00,000 (production with RAID)	Below NCB threshold: SQ or Open IFQAbove NPR 20L: NCB 1S1E[Verify Table 5.2]	Evaluate GIDC hosting first (document decision) · Brand-neutral specs with RAID level specified · 3-year warranty · UPS with 30-min backup · PAMS registration	Not evaluating GIDC first · No RAID specified (single point of failure) · No UPS provision

Scenario	Typical Value — Gandaki Province LG	Method	Critical Protections	Most Common Mistake
C: Custom Software Development Citizen portal, revenue system	NPR 5,00,000–20,00,000 (small system) NPR 20,00,000–50,00,000 (integrated system)	NPR 5L–20L: RFP, QCBS 80:20Above NPR 20L: EOI+RFP (NCB)IT Norms 2082 mandatory	Source code ownership Clause 2 (M5-T13) · NCSC VAPT before go-live · All 9 GEA 2.0 artifacts as payment milestones · UAT with actual end-users · Data residency within Nepal · Step-in Rights Clause 9	Releasing final payment before VAPT clearance · No source code ownership clause · UAT done by developer only (not actual users)
D: ICT Consulting/ Advisory Feasibility, strategy, audit, assessment	NPR 2,00,000–8,00,000 (small advisory)NPR 8,00,000–20,00,000 (comprehensive)	Below NPR 5L: SQ from standing listNPR 5L–20L: RFP, QCBS 80:20IT Norms 2082 mandatory	IT Norms 2082 rates mandatory · Technical and financial envelopes separate · 70/100 technical threshold · NDA signed before any government data shared	Setting Team Leader above NPR 200,000/ month without justification · Opening financial envelopes before technical evaluation complete
E: AMC Renewal Hardware AMC or software support	NPR 50,000–2,00,000/year (hardware)NPR 1,00,000–5,00,000/ year (software)	Apply consulting thresholds (Table 5.2)For renewals: check competitive procurement requirement(Do not automatically renew)	Response time SLA (P1: 4hrs on-site) · 3-year warranty for hardware confirmed · Local service center in Gandaki Province · NDA with each AMC vendor · Quarterly scorecard M5-T22	Automatically renewing without competitive check · No SLA penalty clauses · AMC vendor given unsupervised server room access

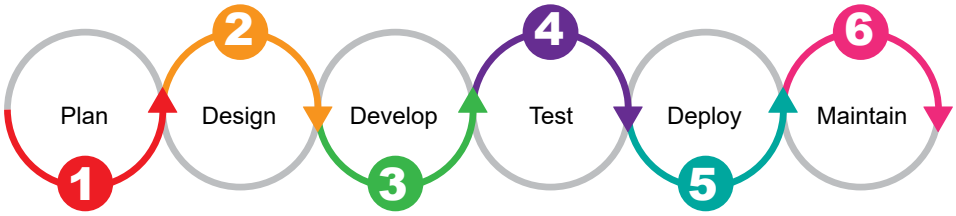
MODULE 6

SYSTEM DEVELOPMENT AND MAINTENANCE

Plan/Design	Develop/Test	Deploy	Maintain

Module 6 provides with comprehensive, practical guidance for the complete software system development lifecycle — from initial requirements through design, secure development, testing, deployment, source code management, API governance, ongoing maintenance, and disaster recovery. Every procedure in this module is aligned with Nepal's Government Enterprise Architecture 2.0 (GEA 2.0) mandatory artifact requirements, COBIT 2019 BAI03 (Build, Acquire, and Implement), and internationally recognized secure development standards.

The Government Software Development Lifecycle



6.1 System Development Life Cycle (SDLC) / प्रणाली विकास जीवनचक्र — *SDLC*

The System Development Life Cycle (SDLC) defines how government ICT systems are planned, built, tested, deployed, and maintained. IT Officials do not write code — they commission, govern, review, and accept software from vendors. Understanding SDLC is essential for writing effective ToRs, managing vendor delivery, protecting public investment, and ensuring GEA 2.0 compliance throughout the project.

6.1.1 Waterfall — Sequential, Gate-Controlled Delivery
वाटरफल — क्रमिक, नियन्त्रित वितरण

In Waterfall, each phase must be completed and government-approved before the next begins. Ideal for systems with stable legal requirements (civil registration, revenue, SUTRA/FRS integration).

Phase / चरण	Government Action (IT Official)	Deliverable / Payment Gate
1. Planning योजना	Prepare TCN (M5-T03). Set budget using IT Norms 2082. designated authority approval before procurement.	Approved TCN + Annual ICT Plan (M5-T01)
2. Requirements आवश्यकता	Review and sign SRS and FRS. Any gap = return to vendor. No signed SRS/FRS = no development commences.	Signed SRS + FRS → Release 20%
3. Design डिजाइन	Review System Architecture Document for GEA 2.0 compliance: REST/JSON APIs, GIDC hosting, NID integration, WCAG accessibility.	Signed Architecture Doc → Release 20%
4. Development विकास	Monitor milestones. Review interim builds. Withhold payment for non-compliant deliverables.	Milestone reports → Release 20%
5. Testing परीक्षण	Conduct government UAT with actual users (Section 6.3). Review Test Results. Log defects.	Signed UAT → Release 20%
6. Go-Live तैनाती	NCSC VAPT clearance (Section 6.8). Designated authority signs Go-Live Checklist (F 6.10). Source code handover verified.	VAPT Clearance + F 6.10 → Release 20%

6.1.2 Agile/Scrum — Iterative, Sprint-Based Delivery
एजाइल/स्क्रम — पुनरावृत्तिमा आधारित वितरण

Agile delivers the system in 2–4 week Sprints. Suitable for citizen portals and e-service integrations where requirements evolve through user feedback. The IT Officcial serves as Product Owner — an active role every Sprint, not just at milestones.

Scrum Term	What Government Must Know / सरकारले जान्नुपर्ने कुरा
Product Owner **उत्पाद स्वामी**	The IT Official (or designated officer) who prioritizes features in the Product Backlog. Participates in every Sprint. This is a minimum 20% time commitment per Sprint — not a passive role.
Product Backlog **कार्य सूची**	Government's complete prioritized feature list. Defines what the system must do. The IT Officcial maintains and updates throughout the project.
Sprint Review **स्प्रिन्ट समीक्षा**	End-of-Sprint meeting where the vendor demonstrates completed features. The IT Official formally accepts or rejects each feature. Sprint Review sign-off gates progress payment.
Definition of Done **पूर्णताको परिभाषा**	Government-agreed criteria that a feature must meet before acceptance: GEA 2.0 compliant, unit-tested, security-reviewed, documented.
Government absence risk	If the IT Official is unavailable during a Sprint, development stalls. Delays cost the same as extended Waterfall timelines without Waterfall's predictability. Assign a backup Product Owner.

6.1.3 Which Methodology to Choose — Decision Guide
कुन विधि रोज्ने — निर्णय मार्गदर्शन

Factor	→ Waterfall	→ Agile/Scrum
Requirements	Stable, legally defined	Evolving, citizen feedback needed
Budget	Fixed-price contract	Time-and-material with cap
System type	Core transaction (civil registration, revenue, tax, financial)	Citizen portal, Nagarik App integration, e-service improvement
Government capacity	IT Official available at milestones only	IT Official can commit 20%+ time per Sprint
Audit trail	Clear sequential milestones — preferred by CIAA	Sprint-by-Sprint documentation needed
Recommended for Gandaki Province LGs	**Default for most LG core systems**	Consider only with dedicated Product Owner

6.1.4 Government Sign-Off Gates — Apply to Both Methodologies
सरकारी स्विकृती प्रक्रियाहरु — दुवैमा अनिवार्य

Regardless of SDLC methodology, the government offices must apply six sign-off gates. No gate can be skipped. Payment is released only after the IT Official writes a sign-off.

Gate	Sign-Off Action	Links payment?
Gate 1: ToR / TCN Approved	Designated authority approves TCN (M5-T03) before procurement commences. Budget confirmed per IT Norms 2082.	Precondition
Gate 2: Requirements Signed	IT Official signs SRS + FRS (Section 6.2, F 6.1 compliance). No development without signatures.	Releases 20%
Gate 3: Architecture Approved	IT Official confirms GEA 2.0 compliance in Architecture Document (REST/JSON, GIDC, NID, WCAG).	Releases 20%
Gate 4: UAT Passed	Government UAT with actual users. All Critical defects resolved. IT Official signs F 6.1 (Test Plan + Test Results Document).	Releases 20%
Gate 5: VAPT Cleared	NCSC VAPT Clearance Letter received. All Critical/High findings remediated (Section 6.8).	Releases 20%
Gate 6: Go-Live Authorized	Designated authority and IT Official sign F 6.10 Go-Live Checklist. All 9 GEA artifacts confirmed. Source code handed over.	Releases final 20%

Note (📌):
ToR specification: Waterfall — 'Each phase requires written IT Official sign-off before next commences.' | Agile — 'Sprint Review sign-off gates each progress payment. Sprint value: NPR [amount]. Maximum [N] Sprints.' | Hybrid — 'Waterfall phase gates apply overall; iterative delivery within Development phase permitted.'

6.2 GEA 2.0 Mandatory Artifacts and Templates
GEA 2.0 अनिवार्य कागजातहरू र टेम्प्लेटहरू

GEA 2.0 mandates 9 specific documentary artifacts for every government software project. The IT Official uses F 6.1 to verify each artifact at the relevant gate before releasing payment. All 9 must be completed before go-live — no exceptions regardless of SDLC methodology.

#	GEA 2.0 Artifact / Template	IT Official Verification Responsibility	Gate
1	**Software Requirements Specification (SRS)** — what the system must do; all functional requirements; user roles; data flows	Review completeness against ToR. Every stated government requirement must be traceable to an SRS section.	Gate 2
2	**Functional Requirements Specification (FRS)** — how each function works; business rules; validation logic	Verify FRS matches the approved SRS. No new requirements added without change control.	Gate 2
3	**System Architecture Design Document** — technical blueprint; server topology; API design; GIDC/IDMC hosting decision; NID integration; WCAG accessibility	Verify GEA 2.0 compliance: REST/JSON APIs, Nepal data residency, GIDC-first hosting, NID integration plan, WCAG 2.1 AA.	Gate 3
4	**Database Design Document** — entity relationship diagram; table structures; data dictionary; privacy classification of each data field	Verify citizen PII fields are identified and classified. No unnecessary PII collection. Encryption plan for sensitive fields.	Gate 3
5	**API Specification** (OpenAPI/Swagger format) — all inter-system APIs with endpoints, parameters, authentication, and data payloads	Verify all APIs use REST/JSON. Swagger/OpenAPI document present. Authentication method specified (OAuth 2.0 / API key).	Gate 3
6	**Test Plan + Test Results Document** — test strategy; test cases; expected vs actual results; defect log; regression test results	Government reviews test coverage: all SRS requirements tested; Critical/ High defects resolved before UAT commences.	Gate 4 pre-UAT
7	**User Manual** (in Nepali) — step-by-step guide for all system functions; screenshots; troubleshooting; common error messages	Verify manual is in plain Nepali. Every citizen-facing function explained.	Gate 5 pre-go-live
8	**Training Material** — presentations, exercises, and job aids for IT Official and front-desk staff training	Verify material covers all user roles. Training delivery plan included. The government retains training materials.	Gate 5 pre-go-live
9	**NCSC VAPT Clearance Letter** — issued by NCSC after all Critical and High findings are remediated	Confirmed receipt of Clearance Letter from NCSC. Not a vendor certificate — must be from NCSC directly.	Gate 5 (VAPT)

6.2.1 Additional Templates — Code Review and Test Case Reporting
थप टेम्प्लेटहरू — कोड समीक्षा र परीक्षण रिपोर्ट

F 6.2 | Code Review Checklist — IT Official or designated technical reviewer completes before UAT gate	
Check Item	**Status**
Does the source code structure match the approved Architecture Document (Section 6.3)?	[ ] Yes [ ] No [ ] Partial
Are all API endpoints implemented as specified in the API Specification (Artifact 5)?	[ ] Yes [ ] No [ ] Partial

Are hardcoded credentials, API keys, or passwords present in the codebase? (Must be ZERO — any found = reject)	[ ] Yes [ ] No [ ] Partial
Is sensitive citizen PII data encrypted in the database as per the Database Design Document (Artifact 4)?	[ ] Yes [ ] No [ ] Partial
Are SQL injection, XSS, CSRF, and other OWASP Top 10 vulnerabilities mitigated in the code?	[ ] Yes [ ] No [ ] Partial
Are all third-party open-source libraries listed with their versions and license types? Any GPL-incompatible licenses?	[ ] Yes [ ] No [ ] Partial
Does the code include inline comments and documentation sufficient for a new developer to maintain the system?	[ ] Yes [ ] No [ ] Partial
Is the build process documented (README, Makefile, Docker config, etc.) so the system can be rebuilt from source?	[ ] Yes [ ] No [ ] Partial
Are there automated unit tests covering at least 60% of business logic functions?	[ ] Yes [ ] No [ ] Partial
Is the code stored in the government-controlled repository with commit history intact (Section 6.3)?	[ ] Yes [ ] No [ ] Partial
Reviewed by IT Official(Designation): _____ Date: _____	

F 6.3 | Test Case Report — Vendor submits; IT Official reviews before UAT gate					
Item/ विवरण	Details / विवरण	Status / स्थिति	Reference		
Module / Feature	Test Case Description	Expected Result	Actual Result	Status (Pass/Fail)	Defect Ref
[System module]	[Describe what was tested and how]	[What should happen]	[What actually happened]	[ ] Pass [ ] Fail	[Ref if failed]
[Module]	[Test case 2]				
[Module]	[Test case 3]				
Authorized IT Official: _____ Date: _____ Designated Authority (Designation) (if required): _____					

6.3 Secure Source Code Management / सुरक्षित स्रोत कोड व्यवस्थापन

GEA 2.0 requires the government to own 100% of all source code developed under government contracts. Source code is the most critical deliverable — it determines whether the government can maintain, modify, or move the system after the vendor relationship ends. Poor source code management is the single most common cause of vendor lock-in in government ICT.

- **The government owns the code, not the vendor** — the vendor is paid to build it, not to retain it. Include source code ownership clauses in ALL ICT contracts (Module 5 M5-T13 Mandatory Contract Clauses).
- **The government must receive code incrementally** — do not wait until project completion. Require source code repository access from Day 1 of the contract. Withhold payment for milestones where code is not committed to the repository.
- **Code must be buildable by the government** — receiving files that cannot be compiled into working software is not compliance with GEA 2.0. Verify build instructions work independently

of the vendor.

- **When the vendor leaves, the government must continue** — the AMC vendor or a replacement vendor must be able to take over from the source code alone, without the original developer's knowledge.

6.3.1 Source Code Repository — IT Official Responsibilities
स्रोत कोड भण्डार — IT अधिकृतको जिम्मेवारी

Action	How / When	Risk if not done
Establish a government repository	A government-controlled repository (GitHub, GitLab, Gitea, or even a secured server with Git) must be set up BEFORE contract starts. Vendor commits to government repo — never the reverse.	Government has no code access if vendor withdraws
Grant vendor access — not ownership	Vendor gets write access to a government-owned repository. The government always has admin access. Record credentials in F 4.25 (Credentials Register).	Vendor can delete or restrict government's own code
Require regular commits	Specify in the ToR: 'Vendor shall commit to the government repository at minimum weekly. Each milestone delivery requires a tagged version commit.'	Government cannot verify development progress
Verify build independence	At each gate and at project completion, have a technical reviewer (IT Official or hired third-party) build the system from the source code without vendor assistance.	System cannot be maintained after vendor exits
Revoke vendor access at contract end	On final payment, formally revoke vendor's repository access. Document in F 4.24 (Technical Handover Checklist).	Former vendor can modify or access government code

F 6.4 | Secure Source Code Handover Checklist — IT Official completes at Gate 6 (Go-Live)	
Check Item	**Status**
Source code ownership clause included in contract (M5-T13) and NDA signed (M5-T16)?	[ ] Yes [ ] No [ ] Partial
Government repository established and IT Official has admin access before development commenced?	[ ] Yes [ ] No [ ] Partial
All source code committed to a government repository with complete commit history?	[ ] Yes [ ] No [ ] Partial
README / build instructions present — can the system be built from source without vendor assistance?	[ ] Yes [ ] No [ ] Partial
All third-party libraries and their versions listed (dependency manifest: package.json, requirements.txt, pom.xml, or equivalent)?	[ ] Yes [ ] No [ ] Partial
Open-source license inventory provided — no GPL-incompatible licenses in a closed system?	[ ] Yes [ ] No [ ] Partial

Database migration scripts included (if any) for setting up the database from scratch?	[ ] Yes [ ] No [ ] Partial
Environment configuration template (.env.example or equivalent) provided without actual secrets/passwords?	[ ] Yes [ ] No [ ] Partial
API keys and credentials removed from source code — stored separately in government secrets management?	[ ] Yes [ ] No [ ] Partial
Vendor repository access formally revoked on final payment? (IT Official confirms in F 4.24)	[ ] Yes [ ] No [ ] Partial
Reviewed by IT Official: _____ Date: _____	

6.4 Data Management Essentials / तथ्याङ्क व्यवस्थापनका आवश्यकताहरू

The government is a data custodian — citizens own their personal data; the government holds it in trust. The IT Official must ensure every ICT system collects only necessary data, stores it securely within Nepal, and handles it per the Individual Privacy Act 2075 and GEA 2.0. Poor data management is a legal liability and a citizen rights violation.

6.4.1 Data Classification — Government Standard / तथ्याङ्क वर्गीकरण — सरकारी मानक

Classification वर्ग	Description विवरण	Examples उदाहरण	Access पहुँच	Storage भण्डारण
PUBLIC **सार्वजनिक**	Can be shared with anyone. No harm from disclosure.	Website content, public notices, approved budget summaries, service fees, office hours	Anyone	Any medium — standard security
INTERNAL **आन्तरिक**	For government staff only. Not for public disclosure.	Operational reports, internal circulars, staff schedules, incomplete decisions	Government staff only — ID verification	Encrypted at rest; access-controlled systems
CONFIDENTIAL **गोपनीय**	Sensitive — limited access. Includes citizen PII.	Citizen names, citizenship numbers, tax records, land ownership, health information, financial transactions	Named officers on need-to-know basis only — 2FA required	Encrypted at rest and in transit; strict access logs; Nepal servers only
RESTRICTED **प्रतिबन्धित**	Highest sensitivity. Unauthorized disclosure causes serious harm.	Encryption keys, API secrets, system passwords, court orders, security vulnerability details	System administrators only — hardware security module / sealed vault	Maximum encryption; air-gapped or HSM; no cloud storage; physical access controls

6.4.2 Data Management Obligations for IT Officials / IT अधिकृतका तथ्याङ्क व्यवस्थापन दायित्वहरू

- **Data minimization:** Specify in every ToR that the system shall collect ONLY the data fields necessary for the stated service. Every data field requires a justification. 'Collect now, use later' is a Privacy Act 2075 violation.
- **Nepal data residency:** All government citizen data must be hosted within Nepal — GIDC/ IDMC (preferred) or DoIT-enlisted Nepal data center. Cross-border data transfer without legal

basis is prohibited (Data Center Directives 2081).

- **Retention and disposal:** Define data retention periods in every system ToR (e.g., civil registration: 100 years; tax records: 7 years; CCTV: 30 days). Data must be securely deleted — not simply 'made inactive' — after a retention period.
- **Breach notification:** If citizen data is accessed without authorization, notify affected citizens and report to NCSC within 72 hours (National Cybersecurity Policy 2080). Log in F 4.17 (Security Incident Report).
- **Vendor data access:** Vendors must sign NDA (M5-T16) before ANY data access. Data shared with vendors is limited to what is necessary for the contracted service. Vendors cannot use citizen data for any other purpose.

System Data Classification Register — Maintain for every government system			
Item / विवरण	Details / विवरण	Status / स्थिति	Reference
System Name	[Name of the government ICT system]	Classification Level	[Highest classification level of data held — Public / Internal / Confidential / Restricted]
Data Fields Held	[List all citizen PII fields: name, citizenship no., address, etc.]	Legal Basis for Collection	[Law/regulation authorizing collection of each PII field — Privacy Act 2075, LGOA 2074, etc.]
Storage Location	[GIDC / IDMC VM / DoIT-enlisted provider — specify Nepal data center name]	Encryption Standard	[AES-256 at rest / TLS 1.2+ in transit — verify implementation in Architecture Document]
Retention Period	[Define retention period per data type — civil registration 100 years, CCTV 30 days, etc.]	Disposal Method	[Secure deletion standard: DoD 5220.22-M or physical destruction for hardware]
Data Custodian Officer	[Name and designation of officer responsible for this system's data]	Last Privacy Review	[Date of last Privacy Act 2075 compliance review — required annually]
Authorized IT Official: _____ Date: _____ Designated Authority (Designation) (if required): _____			

6.5 DevOps, Security, Quality Assurance, and Testing Checklists / DevOps, सुरक्षा, गुणस्तर र परीक्षण जाँचसूचीहरू

DevOps is the practice of integrating development, security, and operations throughout the project — not leaving security and quality to the end. From the government's perspective, DevOps means: specifying security and QA requirements in the ToR, verifying compliance at each gate, and requiring the vendor to demonstrate automated testing and security scanning before any code goes to production.

- **Government specifies, vendor implements** — include all security and QA requirements in the procurement ToR (Module 5, Section 5.4). These are not optional — they are government acceptance criteria.
- **Security is not an add-on** — it requires the vendor to integrate security checks at every stage: secure coding standards, automated vulnerability scanning, dependency checks, and static analysis.
- **Testing coverage is a contract requirement** — specify minimum unit test coverage (60%+) and integration test coverage in the ToR. Vendor submits Test Results Document (F 6.3) before UAT commences.

- **VAPT is the government's independent security verification** — vendor testing is internal; NCSC VAPT is external and independent. Both are required.

F 6.6 | Security Integration Checklist — IT Official verifies before approving Gate 4 (UAT)	
Check Item	**Status**
Are secure coding guidelines (e.g., OWASP Top 10) specified in the contract and confirmed followed by the vendor?	[ ] Yes [ ] No [ ] Partial
Has the vendor conducted Static Application Security Testing (SAST) — scanning source code for vulnerabilities?	[ ] Yes [ ] No [ ] Partial
Has the vendor conducted Dynamic Application Security Testing (DAST) — testing the running application?	[ ] Yes [ ] No [ ] Partial
Are all third-party libraries/dependencies scanned for known vulnerabilities (CVE database)?	[ ] Yes [ ] No [ ] Partial
Are API endpoints protected with authentication (OAuth 2.0 / API key) and authorization (role-based access)?	[ ] Yes [ ] No [ ] Partial
Is SQL injection protection implemented on all database-facing code?	[ ] Yes [ ] No [ ] Partial
Is Cross-Site Scripting (XSS) protection implemented on all web-facing code?	[ ] Yes [ ] No [ ] Partial
Are security headers configured on all web applications (HSTS, Content-Security-Policy, X-Frame-Options)?	[ ] Yes [ ] No [ ] Partial
Is HTTPS enforced on all web and API endpoints (TLS 1.2 minimum — TLS 1.3 preferred)?	[ ] Yes [ ] No [ ] Partial
Has the vendor provided security test evidence (SAST and DAST reports) for IT Official review?	[ ] Yes [ ] No [ ] Partial
Reviewed by IT Official (Designation): _____ Date: _____	

F 6.7 | QA and Testing Standards Checklist — IT Official verifies before UAT gate	
Check Item	**Status**
Has the vendor submitted unit test results with minimum 60% code coverage across business logic functions?	[ ] Yes [ ] No [ ] Partial
Have integration tests confirmed all API interfaces between system modules work as specified?	[ ] Yes [ ] No [ ] Partial
Has regression testing been completed after each bug fix cycle — ensuring fixes do not break existing functions?	[ ] Yes [ ] No [ ] Partial
Have performance tests been conducted: can the system handle expected peak citizen load with acceptable response times?	[ ] Yes [ ] No [ ] Partial

F 6.7 | QA and Testing Standards Checklist — IT Official verifies before UAT gate	
Check Item	**Status**
Have accessibility tests been conducted against WCAG 2.1 Level AA for all citizen-facing interfaces?	[ ] Yes [ ] No [ ] Partial
Has the vendor provided a defect log showing all known defects, their severity, and resolution status?	[ ] Yes [ ] No [ ] Partial
Are all Critical defects (system crashes, data loss, security holes) resolved before UAT commences?	[ ] Yes [ ] No [ ] Partial
Has the vendor demonstrated the system works correctly in Nepali language for all citizen-facing functions?	[ ] Yes [ ] No [ ] Partial
Has browser and device compatibility been tested for citizen-facing portals (mobile-first per DNF 2.0)?	[ ] Yes [ ] No [ ] Partial
Reviewed by IT Official (Designation): _____ Date: _____	

6.6 API Governance, Data Custodian MoU, and Token & Throttling / API सुशासन, डेटा संरक्षक MoU र टोकन/थ्रोटलिङ

Every data exchange between government systems must use GEA 2.0-compliant REST/JSON APIs. **The IT Official approves all API integrations** — no system may exchange citizen data without a signed Data Custodian MoU and documented API governance controls. API tokens and throttling prevent unauthorized access and system abuse.

- **The government approves every API connection** — API integration is a governance decision, not a technical one left to vendors. Unauthorized API connections are a privacy and security violation.
- **Data Custodian MoU is mandatory before any PII exchange** — sign before any citizen data flows between systems or agencies (F 6.8). Defines what data, for what purpose, with what security.
- **API tokens are government property** — production API tokens (keys, OAuth client secrets) are government credentials. Store in F 4.25 (Credentials Register). Rotate annually or when staff change.
- **Rate limiting protects government systems** — throttling prevents a single caller from overwhelming government APIs with excessive requests (whether accidental or malicious).

F 6.8 | API Governance Checklist — IT Official signs before any API goes into production	
Check Item	**Status**
Is the API documented in OpenAPI/Swagger format (GEA 2.0 Artifact 5, Section 6.2)?	[ ] Yes [ ] No [ ] Partial
Does the API use REST/JSON only — no SOAP, XML-RPC, or proprietary formats?	[ ] Yes [ ] No [ ] Partial

F 6.8 | API Governance Checklist — IT Official signs before any API goes into production	
Check Item	**Status**
Is authentication required for all API endpoints — no unauthenticated public write access?	[ ] Yes [ ] No [ ] Partial
Is authentication implemented via OAuth 2.0 or API key (not Basic Auth or no auth)?	[ ] Yes [ ] No [ ] Partial
Are API access logs maintained — recording caller identity, timestamp, endpoint, and response code?	[ ] Yes [ ] No [ ] Partial
Is rate limiting (throttling) configured — maximum requests per minute per caller specified and enforced?	[ ] Yes [ ] No [ ] Partial
Is a Data Custodian MoU (F 6.8) signed for every API connection that exchanges citizen PII?	[ ] Yes [ ] No [ ] Partial
Are all API tokens/keys stored in the government Credentials Register (Module 4, F 4.25)?	[ ] Yes [ ] No [ ] Partial
Is there an API versioning strategy — so future updates do not break existing integrations?	[ ] Yes [ ] No [ ] Partial
Has the API been tested through NCSC VAPT scope (F 7.18 Annex I includes all API endpoints)?	[ ] Yes [ ] No [ ] Partial
Reviewed by IT Official (Designation): _____ Date: _____	

6.6.1 Token Management and API Throttling Standards / API टोकन व्यवस्थापन र थ्रोटलिङ मानक

Topic	Government Standard / Requirement
API Token Types	**API Keys** — long-lived credentials for system-to-system integration (e.g., Nagarik App → LG system). Store in F 4.25. **OAuth 2.0 tokens** — short-lived (expires in 1 hour) for user-authenticated sessions. **JWT (JSON Web Tokens)** — signed tokens for stateless authentication. Government systems can use OAuth 2.0 or API keys.
Token Storage	API keys and OAuth client secrets must NEVER be: hardcoded in source code, stored in plain text files, included in mobile apps, or shared via email/messaging. Store in: server environment variables, a secrets manager, or government hardware security module (HSM). Record all production tokens in Module 4 F 4.25 (Credentials Register).
Token Rotation	Government production API tokens must be rotated: (a) annually as a scheduled maintenance task (F 4.22), (b) immediately when any staff member with token access leaves (F 4.24 Handover), (c) immediately if a security incident suggests token compromise (F 4.17 Security Incident Report).

Topic	Government Standard / Requirement
API Throttling	Require all government API vendors to implement throttling. Standard minimums: (a) Per-caller rate limit: max 100 requests/minute for general APIs; max 10/minute for sensitive PII queries. (b) Burst limit: max 200 requests over any 10-second window. (c) Daily quota per integration: specify per system based on expected traffic. Include throttling requirements in the ToR and verify in the API Governance Checklist.
Token Failure Response	API must return HTTP 401 (Unauthorized) for invalid/expired tokens and HTTP 429 (Too Many Requests) for throttling violations — with Retry-After header. Government IT Official monitors API logs monthly for authentication failures and throttling events.

F 6.9 | Data Custodian MoU — Sign before any citizen PII flows via API between agencies or systems

Item / विवरण	Details / विवरण
Parties	Agency A (Data Provider): _____ | Agency B (Data Recipient): _____
Data Scope	Specific citizen data fields to be exchanged: _____
Legal Basis	Legal authority for data sharing (cite specific law/section): _____
Purpose	Stated purpose for which data will be used — data recipient may NOT use for any other purpose
Security	Encryption standard: _____ | Access control: _____ | Audit logging: [ ] Required
Retention	Data retention period at Agency B: _____ | Deletion method on expiry: _____
Audit Rights	Agency A has the right to audit Agency B's data handling at any time with 7 days' notice
Validity	Valid from: _____ to: _____ | Annual renewal required: [ ] Yes | IT Officials sign both sides

Authorized IT Official (Designation)r: _____ Date: _____

Designated Authority (if required): _____

6.7 VAPT Coordination and System Go-Live

VAPT समन्वय र प्रणाली संचालन अनुमति

VAPT is the government's independent security verification of any internet-facing system before citizens are allowed to use it. It is conducted by NCSC — free for government bodies — and is mandatory under GEA 2.0 and the National Cybersecurity Policy 2080. **The IT Official coordinates VAPT; the vendor facilitates**.

- **Contact NCSC at +977-1-4200144** to schedule VAPT. Submit F 7.18 Annex I Scoping Document in person at NCSC, Singhadurbar.
- **Whitelist NCSC IP 202.45.145.183** on all firewalls, WAFs, and rate-limiting systems before VAPT begins — or VAPT cannot proceed. Yo
- **Vendor facilitates, government coordinates** — vendor provides test credentials and whitelists NCSC IP; IT Official submits the request and tracks remediation.
- **Critical findings must be fixed before go-live** — NCSC issues Critical findings within 7 days; High within 30 days. Request re-VAPT if Critical findings were found. NCSC Clearance Letter required before Go-Live sign-off.

F 6.10 | System Go-Live Checklist — IT Official AND Designated Authority both sign. No go-live without this.	
Check Item	**Status**
All 9 GEA 2.0 mandatory artifacts delivered, reviewed, and IT Official-approved? (F 6.1 Compliance Checklist)	[ ] Yes [ ] No [ ] Partial
Government UAT completed with actual front-desk users? All critical defects resolved? F 6.1 Test Results Document confirmed and UAT sign-off recorded?	[ ] Yes [ ] No [ ] Partial
NCSC VAPT completed? NCSC Clearance Letter received? All Critical/High findings remediated?	[ ] Yes [ ] No [ ] Partial
Source code delivered to a government repository? Build verified independently? F 6.4 Source Code Handover signed?	[ ] Yes [ ] No [ ] Partial
Data Classification Register (F 6.5) completed? Privacy Act 2075 compliance verified?	[ ] Yes [ ] No [ ] Partial
API Governance Checklist (F 6.7) signed? Data Custodian MoU (F 6.8) executed for all PII-sharing APIs?	[ ] Yes [ ] No [ ] Partial
RTO/RPO targets defined in F 4.21? DR Plan documented? IDMC backup configured (Module 7, IDMC I4)?	[ ] Yes [ ] No [ ] Partial
Staff training completed? User Manual (Nepali) delivered? Training materials in government custody?	[ ] Yes [ ] No [ ] Partial
System Maintenance Schedule (F 6.11) established? AMC contract in place before go-live?	[ ] Yes [ ] No [ ] Partial
Rollback plan documented — can the system be taken offline and previous state restored within 4 hours if go-live fails?	[ ] Yes [ ] No [ ] Partial
Reviewed by IT Official (Designation): _____ Date: _____	

6.8 System Maintenance and Lifecycle Management

प्रणाली मर्मतसम्भार तथा जीवनचक्र व्यवस्थापन

System maintenance is a planned government obligation, not reactive firefighting. The IT Official should maintain the System Maintenance Schedule and verify vendor AMC performance monthly. **Vendors execute maintenance; the government verifies and approves invoices only after verification**.

F 6.11 | System Maintenance Schedule — Maintain for ALL production systems. Review monthly.		
Item / विवरण	**Details / विवरण**	**Status / स्थिति**
Security patches (Critical/High)	Within 7 days of release. The IT Official verifies patches applied in staging before production.	Monthly
Security patches (Medium/Low)	Within 30 days of release.	Monthly

F 6.11 | System Maintenance Schedule — Maintain for ALL production systems. Review monthly.		
Item / विवरण	**Details / विवरण**	**Status / स्थिति**
Backup verification	Check the backup software console — all jobs show SUCCESS. Daily by IT Official (Module 4 F 4.9).	Daily
Backup restoration test	Restore one file/record from yesterday's backup. Log in Module 4 F 4.20.	Weekly
SSL certificate renewal	Renew 60 days before expiry. Automate where possible.	Annual (check 60 days ahead)
API key/token rotation	Rotate all production API keys. Update Credentials Register (F 4.25).	Annual / on staff change
Annual VAPT	Schedule with NCSC at the annual system go-live anniversary date.	Annual
Bi-annual DR test	Test RTO/RPO achievement. Document in F 6.11 DR Test Report.	Bi-annual
Dependency updates	Update third-party libraries. Check for deprecated or unsupported components.	Quarterly
Performance review	Review system response times, error rates, and capacity against growth projections.	Quarterly
Authorized IT Official: _____ Date: _____ designated authority (if required): _____		

See Also (📌):

Vendor SLA monitoring: Module 5 M5-T22 (Vendor Scorecard) + M5-T15 (Monthly SLA Report)
Backup procedures: Module 4 Section 4.9 · Emergency contacts: Module 4 F 4.24

6.9 System Decommissioning / प्रणाली विसर्जन

Decommissioning a government system requires designated authority approval and formal process — not simply switching off a server. Citizen data must be transferred or securely destroyed per the Privacy Act 2075. Source code, licenses, hardware, and asset registers must all be properly handled.

F 6.12 | System Decommissioning Checklist — designated authority approval required before proceeding	
Check Item	**Status**
designated authority approval for decommissioning obtained and documented? Legal obligation to retain any data reviewed?	[ ] Yes [ ] No [ ] Partial
Citizen data migration completed — all records required by retention schedule migrated to the replacement system?	[ ] Yes [ ] No [ ] Partial
Residual citizen data securely deleted per DoD 5220.22-M standard or physical media destruction?	[ ] Yes [ ] No [ ] Partial

F 6.12 | System Decommissioning Checklist — designated authority approval required before proceeding	
Check Item	**Status**
Data Classification Register (F 6.5) updated — data disposal date and method documented?	[ ] Yes [ ] No [ ] Partial
Source code archived in a government repository — complete and buildable? Build verified post-archive?	[ ] Yes [ ] No [ ] Partial
API connections to the decommissioned system removed? API Governance Checklist (F 6.8) references updated?	[ ] Yes [ ] No [ ] Partial
Data Custodian MoUs referencing this system formally terminated? Partner agencies notified?	[ ] Yes [ ] No [ ] Partial
Vendor access revoked — API keys, server credentials, repository access? F 4.25 Credentials Register updated?	[ ] Yes [ ] No [ ] Partial
System removed from ICT Asset Register (Module 4 F 4.14) and PAMS (within 7 days)?	[ ] Yes [ ] No [ ] Partial
System removed from Service Catalogue (Module 7 M7-T07) and GIWMS website?	[ ] Yes [ ] No [ ] Partial
Hardware wiped (DoD 5220.22-M) or destroyed? E-waste disposed per IT Policy 2015 requirements?	[ ] Yes [ ] No [ ] Partial
System removed from Application RTO/RPO Register (F 4.21) and Maintenance Schedule (F 6.11)?	[ ] Yes [ ] No [ ] Partial
Reviewed by IT Official (Designationr: _____ Date: _____	

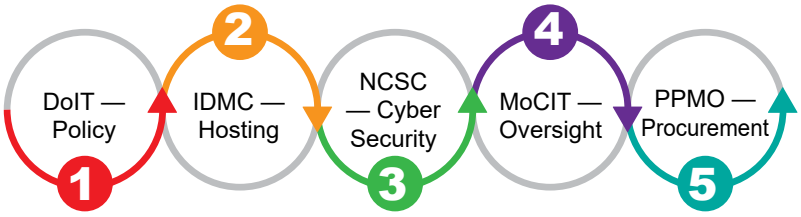
MODULE 7

SERVICE COORDINATION AND SYSTEM MANAGEMENT

DoIT	IDMC/GIDC	NCSC	MoCIT	PPMO

To achieve the 'connected government' vision of the Digital Nepal Framework 2.0 and the Nepal Government Enterprise Architecture (GEA 2.0), provincial ministries and local governments must actively coordinate with federal ICT service agencies. This module provides a comprehensive operational guide to all centralized ICT services available — including the exact SOPs, official request letters, forms, and checklists required to access each service. Every document in this module is ready for immediate use.

Who the Local IT Official Coordinates With



7.1 Government ICT Agencies — At a Glance / सरकारी ICT निकायहरू — संक्षिप्त परिचय

All government ICT service requests in Nepal flow through four national agencies. This section provides the reference overview. Subsequent sections cover each agency's services in the Organization → Services → How to obtain format requested.

Agency निकाय	Full Name पूरा नाम	Services for ICT Officers	Portal / Contact
OPMCM	Office of Prime Minister and Council of Ministers	• Parent ministry- National ICT/ AI Policy • oversees DoIT, IDMC NCSC, OCC	**Web:** opmcm.gov.np Singhadurbar, Kathmandu, Nepal info@opmcm.gov.np 01-5971000 Toll free no 1110

Agency निकाय	Full Name पूरा नाम	Services for ICT Officers	Portal / Contact
DoIT सूचना प्रविधि विभाग	Department of Information Technology (DoIT)	• GIOMS • E-Attendance • Nagarik App integration • GIWMS website • SMS Gateway • GEA compliance	**Portal:** onlinesystem.doit.gov.np/ All DoIT requests via this portal ONLY Babarmahal, Kathmandu info@doit.gov.np; mailsupport@doit.gov.np (For e-mail issues) 1-4112334, 1-4117940
IDMC / GIDC एकीकृत डेटा केन्द्र	Integrated Data Management Center Government Integrated Data Center	• Domain registration (.gov.np) Server colocation • VM/VPS government cloud (G-Cloud) • Offsite backup and data replication	**Web:** idmc.gov.np Submit in person or email to IDMC, Singhadurbar, Kathmandu info@idmc.gov.np; support@idmc.gov.np 01-4211527; 4211917; 4211710; 01-5970646
NCSC: साइबर सुरक्षा केन्द्र	National Cyber Security Centre	• Free VAPT for all government bodies • Cybersecurity advisories • 24/7 cyber incident response hotline	**Hotline:** +977-1-4200144 (24/7) **VAPT IP to whitelist:** 202.45.145.183 **web:** ncsc.gov.np
OCC प्रमाणीकरण कार्यालय	Office of the Controller of Certifications	• Oversight of Certifying Authorities for Digital Signature Certificates under ETA 2063	**web:** occ.gov.np Verify current authorized CAs before applying
PPMO सार्वजनिक खरिद कार्यालय	Public Procurement Monitoring Office	• e-GP portal (bolpoatra.gov.np) • Standard Bidding Documents • Blacklist registry • Procurement guidance	**e-GP:** bolpoatra.gov.np **Web:** ppmo.gov.np
EGB	E-Governance Board	• National e-Governance policy coordination • GEA 2.0 / DNF 2.0 oversight • Inter-agency digital coordination	**Web:** egc.gov.np/ Singhadarbar, Kathmandu administration@egc.gov.np 9851356057

7.2 DoIT Services — Department of Information Technology

सूचना प्रविधि विभाग (DoIT) सेवाहरू

DoIT | Department of Information Technology (सूचना प्रविधि विभाग)

Role: e-governance platform for all government offices — GIOMS, Nagarik App , GIWMS, e-Attendance, SMS Gateway, GEA verification, website monitoring, and IT training.

Portal: http://onlinesystem.doit.gov.np/ | Contact: See doit.gov.np for current contact details

IMPORTANT (⚠):
MANDATORY: ALL DoIT service requests must be submitted through the DoIT online portal: http://onlinesystem.doit.gov.np/ — do NOT submit only by post or email. Standard request letter template (signed by designated authority with office seal) is available on the portal for each service.

7.2.1 DoIT Services Summary / *DoIT* सेवाहरूको सारसंग्रह

All 10 DoIT services are available via the mandatory online portal. Each requires an official request letter signed by the designated authority with an office seal. The table below shows all services, their core requirement, and how to submit. Services with complex or unique requirements are detailed in the callout boxes that follow.

Service / सेवा	What it provides प्रदान गर्ने सेवा	Key requirement before applying	Submit via
S1: GIOMS Government Integrated Office Management System	Digitizes daily office operations, including electronic file management, correspondence (Darta–Chalani), Tok Aadesh, and Tippani, enabling paperless government processes.	GIOMS Readiness Checklist (available on portal). Designate GIOMS focal person. Minimum computer with internet for each users	DoIT portal: onlinesystem.doit.gov.np
S2: E-Attendance Centralized biometric attendance	Biometric staff attendance	Employee count; biometric device installed (or request DoIT device). Stable internet at device location.	DoIT portal
S3: Nagarik App Integration Citizen service mobile platform	Citizens access government services via smartphone — notifications, service status, application submission	GEA 2.0 REST/JSON API developed (F 3.1) + NCSC VAPT clearance + UAT plan + Privacy Act compliance. See detail box below.	DoIT portal + joint API testing with DoIT team
S4: GIWMS + .gov.np Domain Government website + domain	Standardized .gov.np website + RTI-compliant CMS. Domain (e.g., doit.gov.np) registered via IDMC.	Content inventory ready (Citizen Charter, budget, notices, RTI items). Domain name preferences. For domain only: static IP. Coordinate with IDMC Section 7.3.	DoIT portal (GIWMS) + IDMC (domain)
S5: SMS Gateway Centralized government SMS	Official mass SMS to citizens via NTC and Ncell — service notifications, reminders, alerts	Approved Sender ID + tri-party contracts (NTC + Ncell, forms from DoIT portal) + use case policy statement. See detail box below.	DoIT portal + tri-party contract forms
S6: GEA 2.0 Compliance Verification Technical audit certificate	DoIT reviews system for GEA 2.0 compliance. Certificate required before IDMC VM provisioning.	Self-assessment (F 3.1) + SRS + System Architecture Document + API documentation (OpenAPI/ Swagger format).	DoIT portal — upload all documents

7.2.2 Services with Unique Requirements — Additional Detail
विशेष आवश्यकता भएका सेवाहरू — थप विवरण

S3 | Nagarik App Integration — Additional Requirements

- **GEA 2.0 REST/JSON API** must be developed and documented before submitting integration request
- **NCSC VAPT Clearance Letter** on the integration module — mandatory before DoIT joint testing
- **UAT Plan** prepared for joint testing with DoIT Nagarik App technical team
- **Privacy Act 2075 compliance** documented — which citizen data is exchanged and legal basis
- **Service definition document** — each service to be integrated must have data exchange specs
- **After approval:** DoIT Nagarik App team conducts joint API integration and security testing

Action: Start with Module 6 Section 6.2 (GEA 2.0 artifacts) → Module 4 Section 4.8 (VAPT) → User Acceptance Test) → then submit S3 request.

S5 | SMS Gateway — Additional Requirements

- **Tri-party contracts** — separate forms for NTC AND Ncell networks (from DoIT portal)
- **Corporate Subscription Form** — Ncell-specific form (from DoIT portal)
- **Approved Sender ID** — government Sender ID (e.g., 'WALINGMUN') must be DoIT-approved
- **Use case policy statement** — describe message types; DoIT must approve intended use
- **NEVER use for:** promotional, political, personal, or commercial messages
- **Content Guidelines** on DoIT portal must be followed for every message sent

Action: Only for official service notifications: tax reminders, permit renewals, service status, emergency alerts. Gateway usage is monitored by DoIT.

7.3 IDMC Services — Government Integrated Data Center

एकीकृत तथ्याङ्क व्यवस्थापन केन्द्र (IDMC/GIDC) सेवाहरू

IDMC | Integrated Data Management Center

एकीकृत तथ्याङ्क व्यवस्थापन केन्द्र

Role: Manages the Government Integrated Data Center (GIDC) at Singhadurbar. Provides .gov.np domains, VM/VPS government cloud, server colocation, and offsite backup. GIDC hosting must be evaluated FIRST for every new government system.

Portal: idmc.gov.np | Contact: Submit in person or by email to IDMC, Singhadurbar, Kathmandu. Verify current email at idmc.gov.np.

Note (📌): IDMC/GIDC requests are submitted DIRECTLY to IDMC — not via the DoIT online portal. All requests require a designated authority-signed official letter with an office seal. Forms are available at idmc.gov.np.

Prerequisite sequence: GEA 2.0 Certificate (from DoIT S6) → NCSC VAPT → then IDMC VM/colocation provisioning.

Service / सेवा	What it provides	Key requirement	Submit to
I1: Domain Registration .gov.np डोमेन दर्ता	Register official government .gov.np domain (e.g., walingmun.gov.np) Option A: IDMC hosting. Option B: domain only (external government own server IP).	IDMC Domain Registration Form (F 7.13D) from idmc.gov.np. Domain name preferences (3 options). For Option B: provide static IP address. Coordinate with DoIT GIWMS (S4).	IDMC, Singhadurbar — in person or email. Form: F 7.13D (idmc.gov.np)
I2: Server Colocation GIDC सर्भर होस्टिङ	Physical hosting of government-owned server hardware at GIDC — power redundancy, security, cooling, network.	Server colocation form (F 7.14) + DoIT GEA Certificate (S6) + NCSC VAPT Clearance. Device list with serial numbers (Annexure A). Bring your own Ethernet/Fiber cables.	IDMC in person. F 7.14 from idmc.gov.np.

Service / सेवा	What it provides	Key requirement	Submit to
I3: VM / VPS भर्चुअल मेसिन क्लाउड	Virtual server on government cloud — recommended for most new web applications. Scalable, cost-effective, no hardware purchase.	VM/VPS Request Form (F 7.15) + DoIT GEA Certificate (S6) + NCSC VAPT Clearance + Application Architecture Document. Written Nepal data residency confirmation.	IDMC in person or email. F 7.15 from idmc.gov.np.
I4: Offsite Backup अफसाइट ब्याकअप	Backup replication storage at GIDC for critical government systems — geographic redundancy for DR.	Backup configuration form (idmc.gov.np) + data volume estimate (GB/TB) + RTO/RPO targets (Module 4 F 4.19 or Module 6 F 4.23) + IT Official contact for tunnel configuration.	IDMC in person or email. Backup configuration form from idmc.gov.np.

7.4 NCSC — Vulnerability Assessment and Penetration Testing

राष्ट्रिय साइबर सुरक्षा केन्द्र — *VAPT* सेवा

Established: 24 January 2024 (2080 BS) by Cabinet decision, under MoCIT; headquartered in the former Home Ministry building, Singha Durbar. It also serves as Nepal's Digital Forensic Research Centre.

NCSC | National Cyber Security Centre (राष्ट्रिय साइबर सुरक्षा केन्द्र)

Role: Provides free VAPT for all government bodies. Issues cybersecurity advisories. Operates 24/7 incident response hotline. VAPT mandatory for all internet-facing government systems before go-live (GEA 2.0; National Cybersecurity Policy 2080).

Portal: ncsc.gov.np | Contact: Hotline: +977-1-4200144 (24/7) · VAPT IP: 202.45.145.183 (must be whitelisted) · Address: NCSC, Singhadurbar, Kathmandu

How to obtain VAPT:

Step 1: **Schedule Window** – Contact the NCSC to pre-schedule the testing window.

Step 2: **Submit Request** – Deliver the official request letter (signed by the designated authority) and a completed *F 7.18 Annex I Scoping Document* in person to the NCSC.

Step 3: **Assessment Execution** – Facilitate the VAPT audit, which takes 1–5 days depending on the scope.

Step 4: **Remediation Phase** – Remediate all **Critical** findings within 7 days and **High** findings within 30 days.

Step 5: **Obtain Clearance** – Request final validation to receive the official *NCSC Clearance Letter*.

F 7.18 | NCSC VAPT Scoping Document (Annex I) — required with every VAPT request

Complete ALL sections and submit in person to NCSC with the request letter. NCSC will not accept incomplete forms. This is a bilingual form — answer in English or Nepali.

Section (English) / खण्ड (नेपाली)	Required Information / आवश्यक जानकारी
1. Organization Name संस्थाको नाम	Full official name of the requesting government office
2. System / Application Name प्रणाली / एप्लिकेसनको नाम	Full name of the system to be tested
3. URL(s) to be Tested परीक्षण गर्ने URL हरू	List ALL URLs: web portals, admin panels, APIs, mobile app endpoints

4. IP Address(es) IP ठेगाना	Static IP address(es) of the system/server
5. Hosting Environment होस्टिङ वातावरण	[ ] IDMC/GIDC [ ] Other (specify): Note: Must be .gov.np or IDMC-hosted
6. Web Server वेब सर्भर	Name and version — e.g., Apache 2.4, Nginx 1.18, IIS 10
7. Application Server एप्लिकेसन सर्भर	Name and version — e.g., Node.js 18, PHP 8.1, Java 11 / Tomcat 9
8. Database डेटाबेस	Name and version — e.g., PostgreSQL 14, MySQL 8, Oracle 19c
9. Programming Language / Framework प्रोग्रामिङ भाषा	e.g., Laravel (PHP), React+Node, Django (Python), .NET Core
10. Third-Party APIs / Integrations तेस्रो पक्षको API	List all: API URL / Host / Version / Auth type / Testing permission (Yes/No)
11. Backup taken before VAPT? VAPT अघि ब्याकअप	[ ] Yes — Backup date: _____ Backup location: _____
12. NCSC IP Whitelisted? NCCS IP Whitelist गरिएको?	[ ] Yes — NCSC IP 202.45.145.183 is whitelisted on all firewalls, WAFs, and rate-limiting systems
13. Test Accounts परीक्षण खाता	Username / temp password for authenticated testing — or 'Public facing only'
14. VAPT Scope Confirmation VAPT दायरा पुष्टि	I/We agree to allow NCSC to conduct VAPT on the above system and confirm all details are accurate. Authorized Officer: _____ Designation: _____ Date: _____ Seal: _____

7.5 Digital Signature Certificate (DSC) / डिजिटल हस्ताक्षर प्रमाणपत्र (DSC)

Digital Signature Certificates give electronic documents and transactions the same legal validity as physical signatures under ETA 2063 (Module 3, Section 3.3.2). The Authorities and other senior officials who sign official government documents should obtain a DSC from an OCC-registered Certifying Authority.

Step	Action / कार्य	Required Document / आवश्यक कागजात	Where
1	Verify current OCC-authorized Certifying Authorities	Check occ.gov.np for currently authorized CAs. Currently: Radiant InfoTech Nepal Pvt. Ltd. (verify before applying — CAs change).	occ.gov.np
2	Prepare official request letter	Designated authority-signed letter on office letterhead listing all applicants and their designations	Office letterhead + seal
3	Complete applicant detail list	One row per applicant: full name, citizenship type, citizenship number, official email, designation	Available from Certifying Authority or occ.gov.np
4	Complete Schedule-5 Application Form	One form per individual applicant	Available from Certifying Authority (Radiant InfoTech Nepal)
5	Collect supporting documents per applicant	Citizenship certificate copy · Recent passport photo · Appointment letter or official ID copy	Applicant collects

Step	Action / कार्य	Required Document / आवश्यक कागजात	Where
6	Submit to Certifying Authority	Submit package (letter + applicant list + Schedule-5 forms + supporting documents) to the Certifying Authority	Radiant InfoTech Nepal or current OCC-authorized CA — verify at occ.gov.np

Note (📌):

DSC validity: typically 1–2 years. Renewal requires a fresh application through the same process. Verify at occ.gov.np before applying — the list of authorized CAs is updated by OCC. DSCs should be renewed before expiry to avoid disruption to electronic document signing.

7.6 E-Government Systems Directory — Names, URLs, and Contacts
विद्युतीय सुशासन प्रणालीहरूको निर्देशिका — नाम, लिंक र सम्पर्क

The following e-government systems are operational for Gandaki Province provincial and local government offices. This directory was expanded in response to government feedback that system names, URLs, managing agencies, and contact details were missing from the earlier version.

System	Full Name पूरा नाम	URL / Portal	Managing Agency	LG Action Required	Contact for Issues
GIOMS	Government Integrated Office Management System	Access via GIOMS credentials provided by DoIT after onboarding (S1)	DoIT	Onboard via S1. Train ALL staff. Maintain a primary document channel. doit.gov.np	DoIT helpdesk: doit.gov.np
SUTRA	Sub-Treasury Regulatory Application	https://sutra.fcgo.gov.np/	FCGO	Ensure daily financial entries are current. Coordinate with the District Treasury Office for access issues.	District Treasury Office / FCGO
e-GP Portal	Electronic Government Procurement Portal	bolpoatra.gov.np	PPMO	Publish all qualifying ICT procurement on e-GP (Module 5 Section 5.2). Register office account.	PPMO: ppmo.gov.np | Helpline: see ppmo.gov.np
Nagarik App	National Citizen Service Mobile Platform	Citizen-facing app (App Store / Google Play) LG integration: via DoIT S3	DoIT	Integrate priority services (Module 7 Section 7.2 S3). Maintain API uptime.	DoIT helpdesk: doit.gov.np
GIWMS	Government Integrated Website Management System	Your office .gov.np domain (e.g., doit.gov.np) GIWMS platform: via DoIT S4	DoIT (platform) + IDMC (domain)	Register .gov.np domain with IDMC (I1). Onboard GIWMS via DoIT S4. Update RTI content quarterly.	DoIT for GIWMS · IDMC for domain: idmc.gov.np
E-Attendance	Government E-Attendance System	Accessed via GIOMS / separate biometric device	DoIT	Onboard via DoIT S2. Enroll all permanent staff. Report device failures to DoIT immediately.	DoIT helpdesk: doit.gov.np

System	Full Name पूरा नाम	URL / Portal	Managing Agency	LG Action Required	Contact for Issues
PAMS	Public Asset Management System	https://newpams.fcgo.gov.np/	FCGO	Register ALL accepted ICT assets within 7 days of acceptance (Module 4 F 4.14).	FCGO District Office
NID System	National Identity Management System	https://enrollment.donidcr.gov.np/PreEnrollment/	DONIDCR Department of National ID and Civil Registration	Include NID authentication in all new citizen-facing system ToRs (Module 5, Module 6). Mandatory per GEA 2.0 + DNF 2.0.	DONIDCR
DoIT SMS Gateway	Centralized Government SMS Gateway	Via DoIT portal after gateway approval (S5)	DoIT	Apply for gateway via S5. Only official government service notifications permitted.	DoIT helpdesk (after onboarding)

7.7 Annual ICT Coordination Calendar / वार्षिक ICT समन्वय कार्य तालिका

Mandatory ICT coordination activities by month for IT Officials. Cross-reference with Annual ICT Procurement Plan (Module 5 M5-T01) and Monthly Operations Checklist (Module 4 F 4.9).

Month / महिना	Mandatory ICT Coordination Activities
श्रावण (Jul–Aug)	Annual ICT Procurement Plan (M5-T01) — finalized for new fiscal year; Designated authority approval · Physical ICT asset audit (F 4.14) · ICT budget request for new fiscal year · IT Governance Self-Assessment (F 4.2) · PPSU annual ICT review submission
भाद्र (Aug–Sep)	Annual ISMS review (Module 2 F 2.1) · Schedule NCSC VAPT for all internet-facing systems not tested in last 12 months · Review expiring software licenses (F 4.15)
आश्विन (Sep–Oct)	Initiate Q1 procurement per Annual Plan — TCN (M5-T03) preparation · First quarter KPI report to authority · SLA vendor scorecard Q1 review (M5-T22)
कार्तिक (Oct–Nov)	PPMO e-GP portal registration renewal check · DoIT monitoring registration review — verify all portals monitored (S7) · CMMI self-assessment (Module 2 F 2.5)
मंसिर (Nov–Dec)	Bi-annual DR test — P1/P2 systems (Module 4 F 4.21) · Review BCP Emergency Contact List (F 4.24) · Security awareness training for all staff · Digital Signature Certificate renewal check (Section 7.5)
पुष (Dec–Jan)	Mid-year ICT budget review · GIOMS and E-Attendance health check with DoIT · Verify IDMC backup replication current (I4)
माघ (Jan–Feb)	Q2 KPI report · SLA vendor scorecard Q2 review · Domain renewal check for .gov.np domains with IDMC (I1) · IT Official training nominations for upcoming DoIT programs (S9)
फाल्गुण (Feb–Mar)	Privacy Act compliance review (F 3.2 Module 3) · GEA 2.0 compliance check for any systems under development — DoIT verification (S6)
चैत्र (Mar–Apr)	Bi-annual DR test — second test (Module 4 F 4.21) · RTI proactive disclosure annual compliance check (Module 3 F 3.3) · Social media account security review (F 4.22)
बैशाख (Apr–May)	Annual ICT budget preparation for next fiscal year — IT Norms 2082 cost estimates (Module 5 SOP 5.6) · Procurement pipeline list preparation

Month / महिना	Mandatory ICT Coordination Activities
जेठ (May–Jun)	Q3 KPI report · Vendor performance annual review · End-of-year ISMS and COBIT review preparation · Identify ICT staff for next fiscal year training nominations
असार (Jun–Jul)	Annual ICT report to PPSU/designated authority · Contract and AMC expiry review — renew before fiscal year end · IT handover preparation if staff transfers known

7.8 Government ICT Agency Contact Directory / सरकारी ICT निकाय सम्पर्क निर्देशिका

Verify current contact details at official websites before submitting any request — details are subject to change. All requests to national agencies must be on official letterhead signed by the designated authority with an office seal.

Agency	Full Name	Primary Contact	Services (see Section)
DoIT	Department of Information Technology	**PORTAL:** http://onlinesystem.doit.gov.np/ All service requests via portal only **Web:** doit.gov.np	Sections 7.2 (S1-S10)
IDMC	Integrated Data Management Center	Submit in person or by email to: IDMC, Singhadurbar, Kathmandu **Web:** idmc.gov.np (current email on site)	Sections 7.3 (I1-I4)
NCSC	National Cyber Security Centre	**24/7 Hotline:** +977-1-4200144 **VAPT IP:** 202.45.145.183 (whitelist before VAPT) NCsc, Singhadurbar, Kathmandu **Web:** ncsc.gov.np	Section 7.4 (VAPT)
OCC	Office of the Controller of Certifications	OCC, Singhadurbar, Kathmandu **Web:** occ.gov.np Verify authorized CAs at occ.gov.np before applying	Section 7.5 (DSC)
PPMO	Public Procurement Monitoring Office	**e-GP portal:** bolpoatra.gov.np **Blacklist check:** ppmo.gov.np **Web:** ppmo.gov.np	Module 5 (Procurement)
MoC	Ministry of Communication	IT Norms 2082 rates: mocit.gov.np GEA 2.0: mocit.gov.np AI Policy, IT Policy: mocit.gov.np **Web:** mocit.gov.np	Module 3 (Legal framework)
OPMCM	Office of the Prime Minister and Council of Ministers / प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय	OPMCM, Singhadurbar, Kathmandu Web: opmcm.gov.np	E-Governance Board, National Steering Committee (Module 7, Section 7.1)
MoLMCFAGA	Ministry of Land Management, Co-operatives,Federal Affairs & General Administration/ भूमि व्यवस्था, सहकारी, सङ्घीय मामिला तथा सामान्य प्रशासन मन्त्रालय	Singhadurbar, Kathmandu Web: mofaga.gov.np	PLGSP coordination, Local governance IT support, SUTRA / PAMS coordination (Section 7.6)

Agency	Full Name	Primary Contact	Services (see Section)
Nepal Police Cyber Bureau	Cyber Crime Investigation Bureau	**24/7:** +977-1-4412523 For cyber crime reporting (ransomware, hacking, data breaches)	Module 4 Section 4.8 (Security incidents)

7.9 LG ICT Service Catalogue Template / स्थानीय सरकार ICT सेवा सूची टेम्प्लेट

Every LG office should maintain a Service Catalogue — a published list of all ICT services delivered to citizens and staff. Maintain on the GIWMS website and update whenever services change. Reference: Module 2 Section 2.3 (ISO 20000 Service Catalogue requirement).

M7-T07 | LG ICT Service Catalogue / ICT सेवा सूची *Maintain on GIWMS website. Update when services change. Review quarterly.*						
Service Name सेवाको नाम	Service Type सेवाको प्रकार	Description	Channel माध्यम	Hours समय	SLA / Turnaround समयसीमा	Contact सम्पर्क
Civil Registration जन्म दर्ता	Citizen-facing	civil registration certificates (birth, marriage, death)	Counter + VERSPMIS + Nagarik App (if integrated)	Sun–Fri 10:00–17:00	Same day (records found) / 3 days (research)	Municipal Admin counter
Property Tax एकिकृत सम्पत्ती कर	Citizen-facing	Accept and receipt municipal land/property tax payments	Counter + digital payment (if enabled)	Sun–Fri 10:00–16:30	Same-day receipt	Finance Section counter
Building Permit भवन निर्माण इजाजत	Citizen-facing	Issue building permit for residential and commercial construction	Application counter + document review	Sun–Fri 10:00–17:00	15 working days (standard)	Town Planning Section
IT Service Desk IT सेवा डेस्क	Internal staff	Log and resolve ICT incidents and requests from staff	Phone / In-person	Sun–Fri 9:00–17:00	P1: 4 hrs P2: 8 hrs P3: 2 days	IT Official — phone and GIOMS
GIOMS Training GIOMS तालिम	Internal staff	Train staff on GIOMS digital document management	Scheduled sessions / DoIT portal	By arrangement	Per training schedule	IT Official

Publish the Service Catalogue under 'IT Services' or 'Citizen Services' on the GIWMS website. Review and update quarterly or whenever a service is added, modified, or discontinued. Cross-reference: Citizen Charter (Good Governance Act 2064) must list all services including digital channels.

MODULE 8 ANNEXES AND REFERENCE MATERIALS

Tools Reference	Quick Cards	Glossary	Version Control

Contents: Annex 8.1 Master Tools Cross-Reference | Annex 8.2 Six QRC Laminate-Ready Cards | Annex 8.3 Condensed ICT Glossary | Annex 8.4 Key References | Annex 8.5 Version Control | Annex 8.6 List of Abbreviations (moved from Front Matter)

How to use: DAILY OPERATIONS: Use QRC-1 (server room) and QRC-2 (incident triage) at IT Official workstation. PROCUREMENT: Use QRC-3. SECURITY: Use QRC-4. ALL tools reference their home module — always consult the full module for SOPs and detailed procedures.

Print instructions: QRCs 1-6: Print each on A5 cardstock (or cut from A4), laminate, and post in the locations indicated. The Master Tools Table is a desk reference — print on A3 or keep as digital file on IT Official computer desktop.

Annex 8.1 Master Tools Cross-Reference / सबै उपकरणहरूको एकीकृत सन्दर्भ तालिका

All operational tools in this handbook — forms, checklists, SOPs, and templates — listed in order by module. Use this table to locate any tool quickly. Standalone printable versions of all checklists and forms are in the relevant module section.

Tool Ref	Title	Type	Module/Section	When to Use
F 1.1	Inclusive ICT Assessment Checklist	Checklist	Module 1, Section 1.3	Before any new digital service is procured or deployed
F 1.2	Data Protection Quick Reference Card	Quick ref — laminate	Module 1, Section 1.4	Monthly data protection review; vendor onboarding
F 1.3	AI/ML Adoption Readiness Checklist	Checklist (designated authority sign-off)	Module 1, Section 1.5	Before any AI or ML system is procured or deployed
F 2.1	ISO 27001 ISMS Self-Assessment	Annual checklist	Module 2, Section 2.2	Annually; present results to IT Steering Committee
F 2.2	ISO 20000 Service Management Checklist	Quarterly checklist	Module 2, Section 2.3	Quarterly SLA and service quality review
F 2.3	COBIT IT Governance Self-Assessment	Annual checklist	Module 2, Section 2.4	Annually; present to IT Steering Committee
F 2.4	ITIL 4 Practice Implementation Checklist	Monthly checklist	Module 2, Section 2.5	Monthly service management review
F 2.5	CMMI Process Maturity Self-Assessment	Annual checklist	Module 2, Section 2.6	Annually; track maturity progression
F 3.1	GEA 2.0 Compliance Checklist	Compliance checklist	Module 3, Section 3.3	Before any software procurement or deployment
F 3.2	Privacy Act 2075 Compliance Checklist	Compliance checklist	Module 3, Section 3.3.2	Annually; before every new system go-live

Tool Ref	Title	Type	Module/Section	When to Use
F 3.3	RTI and Proactive Disclosure Checklist	Quarterly checklist	Module 3, Section 3.3.3	Quarterly portal content compliance review
F 3.4	Data Center Enlistment Checklist	Procurement checklist	Module 3, Section 3.3.7	Before any data center or cloud hosting procurement
F 4.1	ICT Decision Log	Governance log	Module 4, Section 4.1	Record all significant ICT decisions
SOP 4.2.1	Incident Management	SOP	Module 4, Section 4.2	Any unplanned ICT service interruption
SOP 4.2.2	Problem Management	SOP	Module 4, Section 4.2	Any incident recurs more than twice
SOP 4.3.1	Change Enablement — ICT Change Management	SOP	Module 4, Section 4.3	Any system change, however small
SOP 4.3.2	Service Desk Operation — Single Point of Contact	SOP	Module 4, Section 4.3	Every IT contact — single point of entry
SOP 4.5.1	ICT Asset Registration and Tracking	SOP	Module 4, Section 4.5	Every ICT asset procurement
SOP 4.5.2	ICT Asset Disposal and Secure Decommissioning	SOP	Module 4, Section 4.5	Any asset reaching end of life
SOP 4.8.1	Security Incident Response	SOP	Module 4, Section 4.8	Any suspected or actual security incident
SOP 4.8.2	VAPT — Vulnerability Assessment and Penetration Testing	SOP	Module 4, Section 4.8	Before every NCSC VAPT engagement
SOP 4.9.1	Data Backup Procedure	SOP	Module 4, Section 4.9	Ongoing — all critical systems and data
SOP 4.9.2	BCP Development Guide — Five Steps for LG IT Officials	SOP	Module 4, Section 4.9	Building or updating the office BCP
SOP 4.10.1	Social Media Content Approval and Security	SOP	Module 4, Section 4.10	Every official social media post
SOP 4.11.1	ICT Handover for Departing IT Official or ICT-Responsible Staff	SOP	Module 4, Section 4.11	Any IT Official or ICT-responsible staff departure
F 4.2	IT Governance Self-Assessment	Annual checklist	Module 4, Section 4.1	Annually; present to IT Steering Committee
F 4.3	Incident Log	Operational log	Module 4, Section 4.2	Log ALL incidents immediately; review daily
F 4.4	Incident Priority Quick Reference	Quick ref — laminate	Module 4, Section 4.2	Post at IT Official workstation (also QRC-2)
F 4.6	Problem Record	Problem mgmt form	Module 4, Section 4.2	When any incident recurs more than twice
F 4.5	Root Cause Analysis Worksheet (5 Whys)	Analysis form	Module 4, Section 4.2	For every Problem Record

Tool Ref	Title	Type	Module/Section	When to Use
F 4.7	Change Request Form	Change control	Module 4, Section 4.3	BEFORE implementing any system change
F 4.8	Service Desk Daily Log	Service log	Module 4, Section 4.3	Log every IT contact daily
F 4.9	Combined Operations Checklist (Daily/Weekly/ Monthly)	Operations	Module 4, Section 4.4	Daily/Weekly/Monthly operations verification
F 4.10	Physical Security Checklist	Monthly checklist	Module 4, Section 4.6	Monthly; file signed copy for audit
F 4.11	Server Room Entry Log	Access log	Module 4, Section 4.6	Every server room entry and exit
F 4.12	User Account Management Checklist	Monthly checklist	Module 4, Section 4.7	Monthly; disable unauthorised accounts immediately
F 4.13	Patch Management Schedule	Patch tracker	Module 4, Section 4.7	Weekly update; Critical/High patches within 7 days
F 4.14	ICT Asset Register	Asset register	Module 4, Section 4.5	Every procurement; annual audit
F 4.15	Software License Tracker	License mgmt	Module 4, Section 4.5	Every purchase/renewal; flag expiries 90 days ahead
F 4.16	Asset Disposal Checklist	Disposal form (designated authority sign)	Module 4, Section 4.5	Every ICT asset disposal
F 4.17	Security Incident Report	Incident report	Module 4, Section 4.8	Within 48 hours of any security incident
F 4.18	VAPT Preparation Checklist	VAPT checklist	Module 4, Section 4.8	Before every NCSC VAPT
F 4.19	Backup Schedule Template	Backup policy	Module 4, Section 4.9	Define backup for all systems; review annually
F 4.20	Backup Test and Restoration Log	Test log	Module 4, Section 4.9	Every backup test; quarterly full restoration
F 4.21	Application RTO/RPO Register	Recovery register	Module 6, Section 6.6	Updated on new go-lives; reviewed at DR test
F 4.22	BCP/DR Readiness Checklist	IT Official Checklist	Module 6, Section 6.7	Complete annually and after major system changes
F 4.23	DR Test Report	DR test form	Module 6, Section 6.7	After every bi-annual DR test
F 4.24	BCP/DR Emergency Contact List	Emergency ref — print	Module 4, Section 4.9	Update monthly; print copy in server room + with designated authority
F 4.25	Social Media Management Checklist	Combined checklist	Module 4, Section 4.10	Content: each post. Security: quarterly.
F 4.26	Non-Technical Handover Checklist	Handover form	Module 4, Section 4.11	Every departing staff member with ICT responsibilities

Tool Ref	Title	Type	Module/Section	When to Use
F 4.27	Technical Handover Checklist	Technical handover	Module 4, Section 4.11	Every departing IT Official; receiving officer signs
F 4.28	Credentials and Access Handover Register	Confidential security doc	Module 4, Section 4.11	Every departure; store sealed in designated authority's cabinet
SOP 5.1.1	ICT Procurement Process — Lifecycle at a Glance	SOP	Module 5, Section 5.1	Orientation — read before starting any procurement
M5-T01	Annual ICT Procurement Plan	Plan template	Module 5, Section 5.1	Before fiscal year start
M5-T03	Technical Concept Note (TCN)	Business case form	Module 5, Section 5.3	Before ANY procurement — designated authority approval required
M5-T25	Market Price Survey Record	Survey form	Module 5, Section 5.1	Mandatory for all goods procurement (3 quotes min.)
M5-T04	ToR: ICT Goods with Installation	ToR template	Module 5, Section 5.4	Goods procurement requiring installation/configuration
M5-T05	ToR: Software Development	ToR template	Module 5, Section 5.4	Custom software development assignments
M5-T06	ToR: ICT Consulting	ToR template	Module 5, Section 5.4	Advisory/consultancy assignments
M5-T07	Technical Specifications — Desktop/Laptop	Specification template	Module 5, Section 5.4	Any desktop/laptop/computer hardware procurement
M5-T08	Technical Specifications — Software System	Specification template	Module 5, Section 5.4	Any software system procurement
M5-T09	IT Consulting Cost Estimation Worksheet	Costing (IT Norms)	Module 5, Section 5.6	Every consulting TCN — mandatory
M5-T10	Integrity-Based Eligibility Test (Template 1)	Evaluation gateway	Module 5, Section 5.7	Every consulting evaluation before technical scoring
M5-T11	QCBS Mathematical Evaluation Matrix (Template 2)	Evaluation matrix	Module 5, Section 5.7	Every consulting evaluation after Template 1
M5-T24	Pre-Publication Red Flag Checklist (Template 3)	Compliance checklist	Module 5, Section 5.7	Before publishing every bid document
M5-CK01	Consolidated Procurement Compliance Checklist	Process checklist	Module 5, Section 5.5	Throughout every procurement process
M5-CK02	Direct Purchase Bid Evaluation Checklist	Process checklist	Module 5, Section 5.7	For every direct-purchase/ sealed-quotation goods or services evaluation
M5-CK07	ToR Quality Checklist	Quality checklist	Module 5, Section 5.4	Before publishing any consultancy RFP
M5-T13	Mandatory ICT Contract Clauses	Contract reference	Module 5, Section 5.8	ALL ICT contracts regardless of value

Tool Ref	Title	Type	Module/Section	When to Use
M5-T16	Non-Disclosure Agreement (NDA)	Contract template	Module 5, Section 5.8	BEFORE any system access or data sharing
M5-T17	Annual Maintenance Contract (AMC)	Contract template	Module 5, Section 5.8	For hardware/software maintenance procurement
M5-T20	System Acceptance Certificate	Acceptance form	Module 5, Section 5.8	After all tests complete — gates final payment
M5-T21	Vendor Risk Assessment Checklist	Due diligence	Module 5, Section 5.9	Before awarding Critical/High contracts
M5-T22	Vendor Performance Scorecard	Quarterly review	Module 5, Section 5.9	Quarterly for all active AMC/ service vendors
M5-T15	SLA Performance Report	Monthly report	Module 5, Section 5.9	Vendor submits monthly with invoice
M5-T23	Procurement Scenario Navigator	Quick reference	Module 5, Section 5.10	When planning any procurement
F 6.1	GEA 2.0 Compliance Checklist (Milestone)	Milestone checklist	Module 6, Section 6.2	At each project gate before releasing payment
F 6.2	Code Review Checklist	IT Official Checklist	Module 6, Section 6.2	Before UAT gate; verify code security and quality
F 6.3	Test Case Report	Vendor Report	Module 6, Section 6.2	Vendor submits before UAT gate
F 6.4	Secure Source Code Handover Checklist	IT Official Checklist	Module 6, Section 6.3	At Gate 6 (Go-Live)
F 6.5	System Data Classification Register	Compliance Register	Module 6, Section 6.4	Maintain for every system; update annually
F 6.6	Security Integration Checklist	IT Official Checklist	Module 6, Section 6.5	Before approving Gate 4 (UAT)
F 6.7	QA and Testing Standards Checklist	IT Official Checklist	Module 6, Section 6.5	Before UAT gate
F 6.8	API Governance Checklist	Verification checklist	Module 6, Section 6.5	Before approving any API integration
F 6.9	Data Custodian MoU	Inter-agency agreement	Module 6, Section 6.5	Before ANY citizen data flows via API
F 6.10	System Go-Live Checklist	Combined Checklist	Module 6, Section 6.7	IT Official AND designated authority both sign. No go-live without this
F 6.11	System Maintenance Schedule	Maintenance tracker	Module 6, Section 6.8	Maintained monthly; reviewed quarterly
F 6.12	System Decommissioning Checklist	Decommission form	Module 6, Section 6.9	Before any system is permanently switched off
F 7.18	NCSC VAPT Annex I Scoping Document	Bilingual VAPT form	Module 7, Section 7.3	Submit with every VAPT request to NCSC
M7-T07	Service Catalogue Template	Service catalogue	Module 7, Section 7.9	Maintain and publish on official website; update quarterly

Annex 8.2 Six Laminate-Ready Quick Reference Cards

छ वटा ल्यामिनेट-तयार सन्दर्भ कार्डहरू

Print each card on A5 cardstock (148mm × 210mm) or cut from A4. Laminate. Post in the indicated locations. Do not modify content without IT Official and designated authority approval.

QRC-1 | Server Room Daily Operations Checklist

Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation

Daily Check (Every working day)	Status
Servers online — ping or dashboard check. Any anomaly: log in Incident Log (F 4.3).	[ ] ✓ [ ] Issue
Backup jobs from previous night: CONFIRM SUCCESS in backup software. Failed = P2 incident.	[ ] ✓ [ ] Failed
UPS status lights: ALL ON (ONLINE/NORMAL mode). Battery >80% charge.	[ ] ✓ [ ] Issue
Server room temperature within range (18-27°C). Record: ___°C	[ ] ✓ [ ] Issue
Internet connectivity active for all offices.	[ ] ✓ [ ] Issue
No open P1/P2 incidents from previous day unresolved.	[ ] ✓ [ ] Open
NCSC ncsc.gov.np: check for new cybersecurity advisories.	[ ] ✓ [ ] New alert
Weekly Check (Every Sunday before office hours)	**Status**
Restore one test file from yesterday's backup. Log result in F 4.20.	[ ] ✓ [ ] Failed
Review all open incidents in F 4.3. Escalate any P1/P2 unresolved >4 hrs.	[ ] ✓ [ ] Escalated
User accounts — any accounts for departed staff still active? Disable immediately.	[ ] ✓ [ ] Disabled
Critical/High security patches released this week? Apply via Change Request F 4.7.	[ ] ✓ [ ] Patches pending
IT Official (Designation): _____ Date: _____	

QRC-2 | Incident Triage and Response Guide — P1 to P4

Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation

Priority	Definition	First Action	Notify	Response Target
P1 CRITICAL	Core service offline, ransomware, no workaround available (civil registration, revenue, SUTRA, full internet loss)	Isolate affected system NOW. Do NOT switch off — preserve evidence. Phone designated authority IMMEDIATELY.	Designated authority by phone (NOW) + NCSC +977-1-4200144 + Nepal Police Cyber Bureau +977-1-4412523 if cyber	15 min response · 4 hr resolution
P2 HIGH	Major service degraded, key backup failed, multiple users affected — workaround available	Log in F 4.3. Phone designated authority within 30 min. Engage vendor/ IDMC if not resolving within 1 hour.	designated authority by phone within 30 min	1 hr response · 8 hr resolution

QRC-2 | Incident Triage and Response Guide — P1 to P4

Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation

Priority	Definition	First Action	Notify	Response Target
P3 MEDIUM	Single user or single function affected, non-critical, workaround possible	Log in F 4.3. Investigate. Schedule fix within SLA. Include in weekly summary to designated authority.	Weekly designated authority summary	4 hr response · 2 days resolution
P4 LOW	Service request, query, no service disruption	Log in F 4.8 Service Desk Log. Schedule action. No immediate escalation.	Monthly designated authority report	1 day response · 5 days resolution

P1 CYBER INCIDENT — IMMEDIATE STEPS

1. ISOLATE — disconnect network cable/Wi-Fi from affected system
2. PRESERVE — do NOT switch off (preserve forensic evidence)
3. PHONE — Designated authority + NCSC +977-1-4200144 + Police Cyber Bureau +977-1-4412523
4. BACKUP — execute DR Plan from clean backup
5. DOCUMENT — log all actions in F 4.3 and F 4.17

QRC-3 | ICT Procurement Quick Reference

Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation

Method — ICT GOODS	Threshold (NPR) — Verify at ppmo.gov.np	e-GP?	Key Rule
Direct Purchase	Up to 1,00,000	No	Immediate · Market survey not required but best practice
Sealed Quotation (Standing List)	1,00,000 – 10,00,000	No	7 days · 3 quotes from standing list
Open IFQ — Published	10,00,000 – 20,00,000	Recommended	15 days · Publish notice
NCB (1S1E) — Open Bidding	Above 20,00,000 – 2,00,00,000	Mandatory	30 days · PPMO Standard Bidding Document
Method — ICT CONSULTING / SOFTWARE / AMC	**Threshold (NPR)**	**e-GP?**	**IT Norms?**
Direct Selection	Up to 1,00,000	No	Yes — baseline estimate
Sealed Quotation	1,00,000 – 5,00,000	No	Yes — mandatory
RFP — Shortlisted firms	5,00,000 – 20,00,000	No	Yes — QCBS 80:20
EOI + RFP (NCB)	Above 20,00,000	Yes	Yes — QCBS 80:20
MANDATORY BEFORE ANY PROCUREMENT	**MANDATORY IN EVERY CONTRACT**	**ANTI-CORRUPTION SEQUENCE**	

QRC-3 | ICT Procurement Quick Reference *Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation*			
Method — ICT GOODS	**Threshold (NPR) — Verify at ppmo.gov.np**	**e-GP?**	**Key Rule**
✓ Item in Annual ICT Plan (M5-T01) ✓ designated authority TCN (M5-T03) ✓ Market survey / IT Norms estimate ✓ Brand-neutral specifications ✓ PPMO Standard Bidding Document	✓ Data ownership (100% government) ✓ Source code ownership ✓ NDA (M5-T16) before any access ✓ Data residency within Nepal ✓ Step-in Rights Clause 9	1. Template 3 Red Flag (M5-T24) BEFORE publishing 2. Template 1 Eligibility Test (M5-T10) BEFORE scoring 3. Template 2 QCBS Matrix (M5-T11) for scoring	

QRC-4 | Password Policy and 2FA Quick Reference *Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation*	
Password Requirement	**Standard**
Minimum length	12 characters for standard accounts · 16 characters for administrator accounts
Complexity	Upper + lower case + numbers + symbols — all four required
Reuse restriction	Last 12 passwords must not be reused
Expiry	Change required every 90 days · Administrator accounts: 60 days
Shared passwords	PROHIBITED — one account per named individual. No generic 'admin' accounts without 2FA.
Two-Factor Authentication (2FA) — Mandatory For	**Standard**
All administrator accounts	App-based 2FA (Google Authenticator, Microsoft Authenticator) — NOT SMS-only
All remote access / VPN users	App-based 2FA required before any remote session is opened
All accounts with access to citizen PII	App-based 2FA — verify monthly in F 4.12
Official social media accounts	App-based 2FA — verify quarterly in F 4.22
NEVER DO	
Write passwords on paper or post-it notes · Share passwords by phone or messaging app · Use name+birthdate combinations · Use keyboard patterns (qwerty, 123456) · Reuse the same password across multiple systems · Store passwords in unencrypted documents	

QRC-4 | Password Policy and 2FA Quick Reference *Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation*	
If you suspect a password is compromised	
1. Change it IMMEDIATELY · 2. Check audit logs for unauthorized access · 3. Log as P2 incident (F 4.3) · 4. Notify IT Official (if you are not the IT Official, notify the IT Official) · 5. Check for lateral spread to other systems with the same password	

QRC-5 | Backup Verification and DR Quick Reference *Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation*	
Backup Verification — Daily (F 4.9 Daily Checklist)	**Status**
Log into the backup software console. Confirm ALL critical system jobs show SUCCESS status.	[ ] All success [ ] Issue — INC-
If any backup FAILED: raise as P2 incident in F 4.3. Investigate immediately.	[ ] N/A [ ] P2 raised
Backup Restoration Test — Weekly (every Sunday)	**Status**
Pick any file from yesterday's backup. Restore it to a test location. Verify contents are readable.	[ ] Done [ ] Failed — INC-
Log test result in F 4.20 (Backup Test Log): date, system, backup date used, result.	[ ] Logged
Quarterly Full System Restoration Test	**Status**
Restore complete system from backup to non-production environment. Verify all functions.	[ ] Done [ ] Failed — INC-
Record actual RTO achieved vs target RTO in F 4.20. If target missed: update DR Plan.	[ ] RTO met [ ] Missed — update
RTO and RPO Targets (from F 4.21 — update for your office)	
P1 Critical systems (civil registration, financial): RTO 4 hours · RPO 4 hours	Verify quarterly
P2 High systems (email, website): RTO 8 hours · RPO 24 hours	Verify bi-annually
DR Emergency Contacts — Verify monthly in F 4.21	
NCSC (cyber incident + VAPT): +977-1-4200144 (24/7)	Always available
Nepal Police Cyber Bureau: +977-1-4412523 (24/7)	Always available
IDMC/GIDC: Verify current number at idmc.gov.np	Verify monthly
Internet Service Provider NOC: [Fill from F 4.21]	Verify monthly
Primary ICT Vendor/AMC: [Fill from F 4.21]	Verify monthly

QRC-6 | Emergency Contact List — Fill in and post in server room + with designated authority *Print on A5 cardstock · Laminate · Post at: Server room door · IT Official workstation*				
Role / Agency	**Name**	**Phone (Primary)**	**Phone (Backup)**	**24/7?**
Administration Chief (CAO)	[Name]	[Phone]	[Phone]	[ ] Yes [ ] No
IT Official	[Name]	[Phone]	[Phone]	[ ] Yes [ ] No
Deputy IT Official / Backup	[Name]	[Phone]	[Phone]	[ ] Yes [ ] No
ICT Unit, Gandaki	[Name]	[Phone]	[Phone]	[ ] Yes [ ] No
NCSC (Cyber Incident / VAPT)	-	+977-1-4200144	ncsc@nepal.gov.np	[ ] 24/7
Nepal Police Cyber Bureau	-	+977-1-4412523	-	[ ] 24/7
IDMC/GIDC (Data Center)	Duty Officer	Verify at idmc.gov.np		[ ] Yes
Internet Service Provider (ISP)	[Provider]	[NOC Phone]	[Account No.]	[ ] Yes
Primary ICT Vendor / AMC	[Vendor]	[Phone]	[Email]	[ ] Yes [ ] No
Backup Power / Generator	[Technician]	[Phone]	[Phone]	[ ] Yes [ ] No
Last Verified:	**Date:** _____	**IT Official:** _____		

Annex 8.3 Nepali-English ICT Glossary / संक्षिप्त नेपाली-अंग्रेजी ICT शब्दावली

The 40 most important ICT and governance terms for Gandaki Province provincial and local government ICT officers. Terms are given in English with Nepali equivalent and a brief contextual definition.

Term (English)	नेपाली	Definition / Context
2FA (Two-Factor Authentication)	दुई-चरण प्रमाणीकरण	Security method requiring two forms of identity verification — password plus an app-generated code. Mandatory for all admin accounts (Module 4, Section 4.7).
AMC (Annual Maintenance Contract)	वार्षिक मर्मत सम्झौता	Post-warranty service agreement with a vendor covering hardware or software maintenance (Module 5, Section 5.8).
API (Application Programming Interface)	प्रणाली सम्पर्क बिन्दु	Technical interface enabling two systems to exchange data automatically. GEA 2.0 mandates REST/JSON APIs for all government systems (Module 6, Section 6.5).

Term (English)	नेपाली	Definition / Context
BCP (Business Continuity Plan)	व्यापार निरन्तरता योजना	Documented plan ensuring critical citizen services continue during disruption (Module 4, Section 4.9).
Designated Authority (Chief Administrative Officer)	प्रमुख प्रशासकीय अधिकृत	Head of administration in local/provincial government. Responsible for ICT governance decisions and approvals throughout this handbook.
CIAA	अख्तियार दुरुपयोग अनुसन्धान आयोग	Commission for Investigation of Abuse of Authority — Nepal's anti-corruption body. CIAA investigates ICT procurement irregularities and abuse of authority in government.
CMMI (Capability Maturity Model Integration)	प्रक्रिया परिपक्वता मोडेल	Framework for evaluating and improving ICT process maturity from Level 1 (reactive) to Level 5 (optimizing). (Module 2, Section 2.6).
COBIT 2019	IT सुशासन ढाँचा	IT Governance framework distinguishing governance (designated authority/Steering Committee) from management (IT Official). (Module 2, Section 2.4).
DPI (Digital Public Infrastructure)	डिजिटल सार्वजनिक पूर्वाधार	National foundational digital systems: National ID (NID), digital payments, and data exchange. All new citizen portals must integrate with DPI (Module 3, Section 3.4).
DR (Disaster Recovery)	विपद् पुनर्प्राप्ति	Technical procedures for restoring ICT systems after a major failure. DR plan tested bi-annually (Module 6, Section 6.7).
DSC (Digital Signature Certificate)	डिजिटल हस्ताक्षर प्रमाणपत्र	OCC-issued certificate giving electronic signatures the same legal validity as handwritten signatures under ETA 2063 (Module 7, Section 7.4).
e-GP (Electronic Government Procurement)	इलेक्ट्रोनिक सरकारी खरिद	PPMO's mandatory online procurement portal (bolpoatra.gov.np) for publishing procurement notices above specified thresholds (Module 5, Section 5.2).
ETA 2063 (Electronic Transactions Act)	विद्युतीय कारोबार ऐन २०६३	Nepal's law establishing legal validity of electronic records and digital signatures, and defining cyber offences (Module 3, Section 3.3.1).
GEA 2.0 (Government Enterprise Architecture)	गभर्नमेन्ट इन्टरप्राइज आर्किटेक्चर	Mandatory technical blueprint for all government ICT systems: REST/JSON APIs, GIDC hosting evaluation, 9 mandatory artifacts, source code ownership (Module 3, Section 3.3).
GIDC (Government Integrated Data Center)	सरकारी एकीकृत तथ्याङ्क केन्द्र	Nepal government's data center at Singhadurbar, operated by IDMC. First hosting option for all government systems per Data Center Directives 2081.
GIOMS (Government Integrated Office Management System)	सरकारी कार्यालय व्यवस्थापन प्रणाली	DoIT's digital document management and correspondence routing system for government offices (Module 7, Section 7.1 Service 1).

Term (English)	नेपाली	Definition / Context
GIWMS (Government Integrated Website Management System)	सरकारी वेबसाइट व्यवस्थापन प्रणाली	DoIT's standardized government website platform providing .gov.np websites with RTI-compliant content management (Module 7, Section 7.1 Service 4).
IDMC (Integrated Data Management Center)	एकीकृत तथ्याङ्क व्यवस्थापन केन्द्र	Agency managing GIDC; provides domain registration, VM/VPS, server colocation, and backup services to government (Module 7, Section 7.2).
ISMS (Information Security Management System)	सूचना सुरक्षा व्यवस्थापन प्रणाली	Systematic framework of policies, procedures, and controls to protect information assets — per ISO 27001 (Module 2, Section 2.2).
ITIL 4	IT सेवा व्यवस्थापन ढाँचा	Best-practice framework for IT service management. Five core practices: Service Desk, Incident, Problem, Change, Continual Improvement (Module 2, Section 2.5, Module 4).
IT Norms 2082	IT दर मापदण्ड २०८२	MoCIT's mandatory standards for ICT personnel qualifications and monthly rate benchmarks. Mandatory for all ICT consulting cost estimates (Module 3, Section 3.3.6, Module 5).
IT Official	IT अधिकृत	Government official responsible for ICT operations, security, procurement, and compliance in a provincial or local government office.
Least Privilege	न्यूनतम पहुँच सिद्धान्त	Security principle: each user has access only to the data and systems required for their specific role. Monthly review required (Module 4, F 4.12).
LMCFAGA	संघीय मामला तथा सामान्य प्रशासन मन्त्रालय	Ministry of Land Management, Co-operatives,Federal Affairs & General Administration— Liaison ministry for local governance aslo under which PLGSP operates.
MoIC	सञ्चार तथा सूचना प्रविधि मन्त्रालय	Ministry of Information and Communication — issues national ICT policies including GEA 2.0, IT Norms, AI Policy, and IT Policy.
NCSC (National Cyber Security Centre)	राष्ट्रिय साइबर सुरक्षा केन्द्र	Government agency providing free VAPT for government bodies; issues cybersecurity advisories; responds to cyber incidents. Hotline: +977-1-4200144 (24/7).
NDA (Non-Disclosure Agreement)	गोपनीयता सम्झौता	Contract binding vendors to confidentiality of all government and citizen data. Must be signed BEFORE any system access or data sharing (Module 5, Section 5.8).
NID (National Identity Card)	राष्ट्रिय परिचय पत्र	Nepal's biometric digital identity system. All new citizen-facing government systems must integrate with NID for authentication where applicable (GEA 2.0).
OCC	प्रमाणीकरण नियन्त्रक कार्यालय	Office of the Controller of Certifications — oversees Certifying Authorities for Digital Signature Certificates under ETA 2063.

Term (English)	नेपाली	Definition / Context
PAMS (Public Asset Management System)	सम्पत्ति व्यवस्थापन प्रणाली	Government system for registering all property and ICT assets. All accepted ICT assets must be registered in PAMS within 7 working days (Module 4, Section 4.5).
PII (Personally Identifiable Information)	व्यक्तिगत पहिचान गर्न सकिने जानकारी	Any information that can identify a specific individual — name, citizenship number, biometrics, address, financial data. Protected under Privacy Act 2075.
PPA 2063 (Public Procurement Act)	सार्वजनिक खरिद ऐन २०६३	Nepal's law governing all government procurement. Violations create CIAA Investigation findings and personal legal liability (Module 3, Section 3.3.6, Module 5).
PPMO (Public Procurement Monitoring Office)	सार्वजनिक खरिद अनुगमन कार्यालय	PPMO operates the e-GP portal, issues Standard Bidding Documents, and maintains the vendor blacklist. Website: ppmo.gov.np.
PPSU (Provincial Program Support Unit)	प्रदेश नीति तथा योजना सहयोग एकाई	Province technical support unit for local governments operating under PLGSP in each province — provides ICT guidance, capacity building, and policy oversight.
QCBS (Quality and Cost-Based Selection)	गुणस्तर र लागत आधारित छनोट	Procurement evaluation method for consulting: 80% technical quality + 20% price. Mandatory for all ICT consulting procurement (Module 5, Section 5.7).
REST/JSON	खुला API मानक	Technical standards for APIs mandated by GEA 2.0. REST = Representational State Transfer (architecture); JSON = JavaScript Object Notation (data format).
RPO (Recovery Point Objective)	पुनर्प्राप्ति बिन्दु लक्ष्य	Maximum acceptable data loss in case of disaster — defines how old the most recent backup can be. Defined per system in Module 4 F 4.21.
RTO (Recovery Time Objective)	पुनर्प्राप्ति समय लक्ष्य	Maximum acceptable time from disaster to service restoration. P1 critical systems: 4 hours. Defined per system in Module 4 F 4.21.
VAPT (Vulnerability Assessment and Penetration Testing)	सुरक्षा जोखिम परीक्षण	Security testing identifying vulnerabilities before they can be exploited. Free from NCSC (+977-1-4200144). Mandatory before any citizen-facing system goes live.
WCAG 2.1 (Web Content Accessibility Guidelines)	वेब पहुँचयोग्यता मार्गदर्शिका	International accessibility standard for websites. Level AA compliance is mandatory for all government citizen portals (Module 1, Section 1.3, F 1.1).

Annex 8.4 Key References and Official Sources

मुख्य सन्दर्भ तथा आधिकारिक स्रोतहरू

Verify currency of all laws, policies, and thresholds before use — these are subject to amendment. All national laws are freely available at lawcommission.gov.np.

Reference	Access / URL	Notes
Constitution of Nepal 2015	lawcommission.gov.np	Schedules 8 and 9 (LG ICT powers); Articles 27 (RTI) and 28 (Privacy) — Module 3
Individual Privacy Act 2075	lawcommission.gov.np	Citizen data protection obligations — Module 3, Section 3.3.2
Electronic Transactions Act 2063	lawcommission.gov.np	Digital signatures; cyber offences (Sections 44-47) — Module 3, Section 3.3.1
Right to Information Act 2064	lawcommission.gov.np; nic.gov.np	Proactive disclosure; Information Officer obligations — Module 3, Section 3.3.3
Public Procurement Act 2063 + PPR 2064	ppmo.gov.np; lawcommission.gov.np	All ICT procurement thresholds — verify current thresholds before every procurement
GEA 2.0 (Nepal Government Enterprise Architecture)	doit.gov.np	Mandatory for all government system development. Verify latest version.
IT Norms 2082 (MoCIT ICT Rate Standards)	mocit.gov.np	VERIFY CURRENT RATES before every consulting cost estimate — updated annually
National AI Policy 2025 (2082 BS)	mocit.gov.np	Ethical AI adoption requirements — Module 3, Section 3.3.10; Module 1, Section 1.5
Digital Nepal Framework 2.0	mocit.gov.np	National digital transformation strategy — Module 3, Section 3.4
Data Center and Cloud Services Directives 2081	mocit.gov.np or doit.gov.np	GIDC-first hosting; DoIT vendor enlistment — Module 3, Section 3.3.7
National Cybersecurity Policy 2023	ncsc.gov.np	Minimum security standards for government systems — Module 4, Module 2
PPMO Standard Bidding Documents	ppmo.gov.np (free download)	Mandatory for all ICT goods and consulting procurement — Module 5
PPMO e-GP Portal	bolpoatra.gov.np	Mandatory procurement publication portal above threshold
PPMO Vendor Blacklist	ppmo.gov.np	Check before every contract award — Template 1 (M5-T10) requires this
DoIT Official Website	doit.gov.np	DoIT online service portal link, GEA guidance, GIOMS, GIWMS — Module 7

Annex 8.5 List of Abbreviations and Acronyms / संक्षिप्त शब्दहरूको सूची

Abbreviations used throughout this ICT Technical Handbook, listed alphabetically. Moved to Annexes per OCMCM Gandaki Province Government feedback (Point 2: abbreviations should be at the end of the handbook).

Acronym	Full Form / पूरा नाम	Context / Module Reference
1S1E	Single Stage Single Envelop एक-चरण एक खाम बिधी	Bidding — process of bidding applicable for 2 million to 20 million in supply of goods. Module 5
1S2E	Single Stage Double Envelop एक-चरण दुई खाम बिधी	Bidding — process of bidding applicable for above 20 million in supply of goods. Module 5
2FA	Two-Factor Authentication दुई-चरण प्रमाणीकरण	Security — dual verification; mandatory for all admin accounts. Module 4, Section 4.7
AI	Artificial Intelligence कृत्रिम बुद्धिमत्ता	Machine-based intelligence; AI Policy 2025 applies. Module 1 Section 1.6; Module 3 Section 3.3.10
AMC	Annual Maintenance Contract वार्षिक मर्मत सम्झौता	Post-warranty ICT service agreement with vendor. Module 5, Section 5.8
API	Application Programming Interface प्रणाली सम्पर्क बिन्दु	System-to-system data interface; REST/JSON mandated by GEA 2.0. Module 6, Section 6.5
APP	Annual Procurement Plan वार्षिक खरिद योजना	Mandatory annual schedule; all ICT items listed before procurement. Module 5, M5-T01
BCP	Business Continuity Plan व्यापार निरन्तरता योजना	Plan for maintaining services during disruption. Module 4, Section 4.9
CAO	Chief Administrative Officer प्रमुख प्रशासकीय अधिकृत	Head of municipal/provincial administration; signs all major ICT approvals.
CIAA	Commission for Investigation of Abuse of Authority अख्तियार दुरुपयोग अनुसन्धान	Nepal's anti-corruption body; ICT procurement subject to CIAA Investigation.
CMMI	Capability Maturity Model Integration क्षमता परिपक्वता मोडेल	Process maturity model Levels 1–5. Module 2, Section 2.6
COBIT	Control Objectives for Information and Related Technologies	IT governance framework. Module 2, Section 2.4; Module 4, Section 4.1
DNF	Digital Nepal Framework डिजिटल नेपाल ढाँचा	National digital transformation strategy v2.0. Module 3, Section 3.3.9
DoIT	Department of Information Technology / सूचना प्रविधि विभाग	MoCIT agency for e-governance platforms. Module 7, Section 7.2
DRP	Disaster Recovery Plan विपद् पुनर्प्राप्ति योजना	Plan for restoring IT systems after major incident. Module 4, Section 4.9; Module 6, Section 6.7
DSC	Digital Signature Certificate डिजिटल हस्ताक्षर प्रमाणपत्र	OCC-issued certificate for legally valid electronic signatures under ETA 2063. Module 7, Section 7.5
e-GP	Electronic Government Procurement इलेक्ट्रोनिक सरकारी खरिद	Mandatory portal: bolpoatra.gov.np. Module 5, Section 5.2
EOI	Expression of Interest / आशय पत्र	First stage of two-stage consultancy procurement. Module 5, Table 5.2

Acronym	Full Form / पूरा नाम	Context / Module Reference
ETA	Electronic Transactions Act 2063 / विद्युतीय कारोबार ऐन	Digital signatures and cyber offences. Module 3, Section 3.3.2
GEA	Government Enterprise Architecture गभर्नमेन्ट इन्टरप्राइज आर्किटेक्चर	Nepal's mandatory ICT blueprint v2.0. Module 3, Section 3.3.5; Module 6
GIDC	Government Integrated Data Center सरकारी एकीकृत डेटा केन्द्र	GoN data center at Singhadurbar; operated by IDMC. Module 7, Section 7.3
GIOMS	Government Integrated Office Management System	DoIT digital office management system. Module 7, Section 7.2 (S1)
GIWMS	Government Integrated Website Management System	DoIT standard CMS for .gov.np websites. Module 7, Section 7.2 (S4)
ICB	International Competitive Bidding	Bidding Preference for Foreign Bidders also, Module 5
ICT	Information and Communication Technology / सूचना तथा संचार प्रविधि	Computers, internet, and digital communication systems.
IDMC	Integrated Data Management Center / एकीकृत तथ्याङ्क व्यवस्थापन केन्द्र	Operates GIDC; domain, VM, colocation, backup. Module 7, Section 7.3
ISMS	Information Security Management System / सूचना सुरक्षा व्यवस्थापन	ISO 27001 framework for information protection. Module 2, Section 2.2
ITIL	Information Technology Infrastructure Library	IT service management best practices v4. Module 2, Section 2.5; Module 4
LG	Local Government / स्थानीय सरकार	Municipalities and rural municipalities; 85 in Gandaki Province.
MoCIT	Ministry of Communication and Information Technology सञ्चार मन्त्रालय	Federal ministry; publishes GEA 2.0, IT Norms 2082, AI Policy 2025.
MoFAGA	Ministry of Federal Affairs and General Administration संघीय मामला मन्त्रालय	Federal ministry for local governance; PLGSP coordination.
MoU	Memorandum of Understanding समझदारी पत्र	Data Custodian MoU. Module 6, F 6.9
NCB	National Competitive Bidding	Bidding Preference only for Domestic Bidders, Module 5
NCSC	National Cyber Security Centre राष्ट्रिय साइबर सुरक्षा केन्द्र	Free VAPT for government; 24/7 hotline: +977-1-4200144. Module 7, Section 7.4
NDA	Non-Disclosure Agreement गोपनीयता सम्झौता	Binds vendor to confidentiality; sign BEFORE system access. Module 5, M5-T16
NID	National Identity Card / राष्ट्रिय परिचय पत्र	Nepal biometric citizen identity; GEA 2.0 mandates integration in citizen portals.
OAG	Office of the Auditor General / महालेखा परीक्षकको कार्यालय	Constitutional body for annual financial audit of all government bodies.
OCC	Office of the Controller of Certification / प्रमाणीकरण नियन्त्रक	Regulates digital signature CAs under ETA 2063. Module 7, Section 7.5
OCMCM	Office of the Chief Minister and Council of Ministers	Provincial executive office, Gandaki Province; client for this handbook.

Acronym	Full Form / पूरा नाम	Context / Module Reference
PAMS	Property and Asset Management System / सम्पत्ति व्यवस्थापन प्रणाली	FCGO asset register; all ICT assets registered within 7 days. Module 4, F 4.14
PII	Personally Identifiable Information व्यक्तिगत पहिचान जानकारी	Data identifying an individual; protected under Privacy Act 2075. Module 3, Section 3.3.3
PLGSP	Provincial and Local Governance Strengthening Program	GoN program strengthening provincial and local government capacity.
PPA	Public Procurement Act 2063 सार्वजनिक खरिद ऐन	Governs all government procurement; violations create CIAA findings. Module 5
PPMO	Public Procurement Monitoring Office / खरिद अनुगमन कार्यालय	e-GP portal, standard bid documents, threshold verification; ppmo.gov.np
PPR	Public Procurement Regulation 2064 / सार्वजनिक खरिद नियमावली	Governs all government procurement; violations create CIAA findings. Module 5
PPSU	Provincial Programme Support Unit प्रदेश नीति तथा योजना सहयोग	PLGSP provincial coordination unit, Gandaki Province.
QCBS	Quality and Cost-Based Selection गुणस्तर र लागत छनोट	80:20 technical/financial evaluation for ICT consulting. Module 5, Section 5.7
QRC	Quick Reference Card द्रुत सन्दर्भ कार्ड	Laminate-ready A5 card for daily use; six cards in Annex 8.2 of this module.
RTI	Right to Information सूचनाको हक	Citizens' right to access government information; RTI Act 2064. Module 3, Section 3.3.4
RTO / RPO	Recovery Time / Recovery Point Objective	Maximum downtime / data loss targets per system. Module 4, F 4.21
SLA	Service Level Agreement सेवा स्तर सम्झौता	Defined service quality and response times. Module 5, Sections 5.8–5.9
SOP	Standard Operating Procedure मानक सञ्चालन प्रक्रिया	Numbered step-by-step procedure; used throughout Modules 4–7.
TCN	Technical Concept Note प्राविधिक अवधारणा नोट	Mandatory internal business case; designated authority approval required. Module 5, M5-T03
ToR	Terms of Reference कार्य सन्दर्भहरुको सूची	Defines scope of consulting assignment; IT Norms 2082 compliance required. Module 5
TWG	Technical Working Group प्राविधिक कार्यसमूह	Review and sign-off body for this handbook; PPSU/ OCMCM-chaired.
UAT	User Acceptance Testing प्रयोगकर्ता स्वीकृति परीक्षण	Government-conducted testing with actual users before go-live. Module 6, F 6.5
VAPT	Vulnerability Assessment and Penetration Testing सुरक्षा जोखिम परीक्षण	Free NCSC testing before go-live; mandatory per GEA 2.0. Module 7, Section 7.4
VM/VPS	Virtual Machine / Virtual Private Server / भर्चुअल मेसिन	IDMC government cloud hosting option. Module 7, Section 7.3 (I3)
WCAG	Web Content Accessibility Guidelines / वेब पहुँचयोग्यता मार्गदर्शिका	v2.1 Level AA mandatory for all government citizen portals. Module 1, Section 1.3