# 11.1 ICT Policy, 2072 (2015)

## A. Background and Purpose

- **Full Name:** National Information and Communication Technology Policy, 2072 (2015)
- **Issued by:** Ministry of Communications and Information Technology (MoCIT)
- **Purpose:** To guide Nepal's digital transformation by establishing a framework for ICT infrastructure development, e-governance, cybersecurity, and legal reforms .

## B. Key Objectives of ICT Policy 2072

| Objective | Description |
|---|---|
| **Infrastructure Development** | Expand ICT access across Nepal, including rural areas |
| **E-Governance** | Transition government services to digital platforms (e-administration and e-economy) |
| **Cybersecurity** | Enhance security and build citizen confidence in using ICT |
| **Legal Reform** | Improve existing cybercrime and cybersecurity legislation |
| **Institutional Capacity** | Establish new units within government to enforce cyber laws |

## C. Major Institutional Outcomes of the Policy

The policy led to the creation of several key institutions :

| Institution | Purpose |
|---|---|
| **Computer Crimes Investigation Unit** | Part of Nepal Police; investigates cybercrimes |
| **National Electronic Communication Security Centre** | Focuses on securing electronic communications |
| **Information Security Response Team Nepal (NPCERT)** | Later renamed/evolved into ITERT; handles cybersecurity incidents |

## D. Current Status (Important for Exam)

- The ICT Policy 2072 is currently **under review** for revision and integration with other policies (Telecommunications Policy 2060, Broadband Policy 2071) .
- It has been supplemented by newer policies:
  - **National Cyber Security Policy, 2080 (2023)** – Nepal's first dedicated cybersecurity policy
  - **Digital Nepal Framework, 2076 (2019)** – Focuses on sectoral digital transformation

**Key Point for Exam:** While ICT Policy 2072 remains the foundational ICT policy, newer policies (especially National Cyber Security Policy 2080) have updated and expanded its provisions.

---

# 11.2 Electronic Transaction Act, 2063 (2008)

## A. Overview

- **Full Name:** Electronic Transaction Act, 2063 (2008)
- **Also known as:** ETA 2063
- **Effective from:** Bhadra 24, 2063 (September 2, 2006)
- **Extends to:** All of Nepal and applies to Nepali citizens anywhere who commit offences under this Act

## B. Purpose of the Act

ETA 2063 is Nepal's primary law governing:

- **Legal recognition of electronic records** (documents in digital form have legal validity)
- **Digital signatures** (legally binding authentication)
- **Cybercrime offences** (unauthorized access, data damage, etc.)
- **Electronic transactions** (security, authenticity, and integrity of online transactions)

## C. Key Provisions (Exam Focus)

### 1. Legal Recognition of Electronic Records (Section 4)

- Information, documents, or records maintained in **electronic form** have the same legal validity as written or printed documents .
- This enables e-governance and paperless transactions.

**2. Definitions Provided by the Act**

| Term | Definition |
|---|---|
| **Computer System** | Hardware and software components |
| **Computer Network** | Interconnected computers |
| **Computer Database** | Organized collection of data |
| **Electronic Record** | Data, record, image, or sound transmitted, received, or stored electronically |
| **Electronic Form** | Information generated through magnetic, optical, computer memory, or similar devices |

**3. Cybercrime Offences Under ETA 2063**

| Section | Offence | Description |
|---|---|---|
| **Section 45** | Unauthorized Access | Accessing a computer or network without permission |
| **Section 46** | Damage to Computer Systems | Intentionally damaging computer systems, information, or data |

**4. Jurisdiction of the Act**

The Act applies to offences committed :

- Within Nepali territory (territoriality principle)
- By Nepali citizens outside Nepal (active nationality principle)
- Against Nepali citizens outside Nepal (passive nationality principle)
- That produce substantial effects within Nepal (effects doctrine)

**5. Digital Signatures**

- ETA 2063 provides the legal framework for **digital signatures** using asymmetric cryptography (public/private keys).
- Certifying Authorities (CAs) licensed by the government issue digital signatures.
- The **Controller of Certifying Authorities (CCA)** under MoCIT regulates them.

## D. Limitations of ETA 2063

- The Act focuses primarily on **electronic transactions and financial security**, not comprehensive cybercrime criminal law .
- Does not fully address all cybercrimes (e.g., cyberstalking, online harassment, child exploitation) – some are covered by other laws (Children's Act 2048, National Penal Code 2017) .
- A new **Information and Technology Bill** is being drafted to address these gaps .

## E. Related Rules and Acts

| Name | Relationship |
|---|---|
| **Electronic Transactions Rules, 2064 (2007)** | Rules framed under ETA 2063 to implement its provisions |
| **Banking Offence and Punishment Act 2064 (2008)** | Covers unauthorized electronic withdrawals, fraud, and forgery in banking |
| **Privacy Act 2075 (2018)** | Protects privacy of electronic communications and personal data |
| **National Penal Code 2074 (2017)** | Contains general cyber-related offences (Section 276: forgery, Section 298: breach of privacy via electronic means, Section 300: causing annoyance, Section 307: libel) |

---

# 11.3 Information Technology Emergency Response Team (ITERT) Operation and Management Directive, 2075 (2018)

## A. Background

- **ITERT (Information Technology Emergency Response Team)** is Nepal's national **CERT (Computer Emergency Response Team)** .
- Originally established as **NPCERT (Nepal CERT)** in 2016 following the ICT Policy 2072 .
- The **ITERT Operation and Management Directive, 2075** formalized its structure, functions, and operations.

## B. Purpose of ITERT

ITERT serves as Nepal's **national coordination center** for:

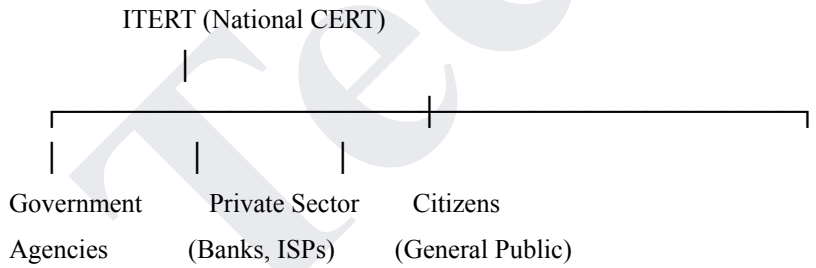
- Responding to **cybersecurity incidents** (hacking, phishing, malware outbreaks, DDoS attacks)
- Issuing **early warnings** and alerts about emerging threats
- Coordinating with **domestic and international CSIRTs/CERTs** for information sharing

## C. Key Functions of ITERT (Exam Focus)

| Function | Description |
|---|---|
| **Incident Response** | Receive, analyze, and respond to cybersecurity incidents affecting Nepal |
| **Threat Alerts** | Issue public and private alerts about new vulnerabilities and attacks |
| **Coordination** | Work with ISPs, financial institutions, government agencies, and law enforcement (Cyber Bureau) |
| **Capacity Building** | Train organizations and individuals on cybersecurity best practices |
| **International Cooperation** | Collaborate with international CERTs (e.g., APCERT, OIC-CERT) |

## D. Role in Nepal's Cybersecurity Ecosystem

text




## E. Related Institution: National Cyber Security Centre

- Established under the **National Cyber Security Policy, 2080**
- Works alongside ITERT to implement national cybersecurity strategies

# 11.4 Government Website Development and Management Directive, 2078 (2021)

## A. Overview

- **Issued by:** Ministry of Communications and Information Technology (MoCIT)
- **Replaced:** Previous Website Development and Management Directive, 2068 BS
- **Purpose:** To standardize, secure, and streamline all government websites in Nepal

## B. Key Provisions of the Directive (Exam Focus)

### 1. Standardization (Uniformity)

| Requirement | Details |
|---|---|
| **Model Template** | All government websites must be based on a model prepared by the Department of Information Technology (DoIT) |
| **Integrated Website Management System (IWMS)** | Launched in 2023; allows government agencies to create and manage websites using standardized templates |
| **Web Monitoring System** | Continuously monitors government websites for hacking, defacement, downtime, and security issues |

### 2. Content Requirements

Government websites must include :

- Office name and contact information
- Services offered by the office
- Employee details
- Citizen charter
- Downloadable forms
- Frequently Asked Questions (FAQs)
- Complaints management system
- Automated assistant (chatbot)

### 3. Technical Standards

| Standard | Requirement |
|---|---|
| **Hosting** | All government websites must be hosted on the **Government Integrated Data Center (GIDC)** |
| **Accessibility** | Must be "disabled-friendly" (accessible to persons with disabilities) |
| **Bandwidth** | Must be operable even on low internet bandwidth |
| **Formats** | Content should be in HTML, PDF, and Word formats |
| **Mobile App** | A separate mobile app is available to view government websites |

### 4. Security and Maintenance

| Requirement | Frequency |
|---|---|
| **Regular security testing** | Ongoing |
| **Annual status examination** | Once per year (by DoIT) |
| **Updates when office bearers change** | Within 24 hours |
| **Continuous monitoring** | Via Web Monitoring System |

TechPSC

**5. Benefits of the Directive**

| Benefit | Description |
|---|---|
| **Cost reduction** | Agencies no longer need to build websites independently |
| **Uniformity** | Consistent look, feel, and information across all government portals |
| **Security** | Centralized monitoring and rapid response to hacking/downtime |
| **Ease of management** | Non-technical staff can update content using templates |
| **Reduced dependency** | No need for qualified IT workforce in every agency |

## C. Implementation Status

- Launched initially with MoCIT and its four subordinate bodies (Department of Information and Broadcasting, Postal Services Department, DoIT, Department of Printing)
- Being expanded to all ministries and government agencies

---

TechPSC

# 11.5 Roles of Related Institutions

## 11.5.1 Ministry of Communication and Information Technology (MoCIT)

**Overview:** The **apex body** responsible for formulating and implementing policies, laws, and standards for Nepal's communication and information technology sectors.

**Key Responsibilities (Exam Focus):**

| Responsibility | Description |
|---|---|
| **Policy Formulation** | Draft and issue ICT policies (ICT Policy 2072, National Cyber Security Policy 2080, etc.) |
| **Legislation** | Prepare and propose bills related to IT, telecommunications, mass media, and social media |
| **Regulation** | Oversee and regulate the IT and telecommunications sectors |
| **Directives Issuance** | Issue binding directives (e.g., Government Website Directive 2078, Social Media Directive 2080) |
| **Frequency Management** | Allocate and manage radio frequency spectrum |
| **International Coordination** | Represent Nepal in international ICT forums |
| **E-Governance Promotion** | Lead digital transformation initiatives across government |

**Recent Major Achievements (for exam context):**

- Issued **National Cyber Security Policy, 2080** (first ever)
- Issued **Directive on Managing Social Networking Sites Use, 2080**
- Launched **Integrated Website Management System (IWMS)**
- Established **National Cyber Security Centre**

**Minister (Current for exam reference):** Jagdish Kharel (as of Dec 2025)

## 11.5.2 Department of Information Technology (DoIT)

**Overview:** The **technical arm** of MoCIT responsible for implementing IT policies, developing standards, and providing technical services to government agencies.

**Key Responsibilities (Exam Focus):**

| Responsibility | Description |
|---|---|
| **Model Website Development** | Creates the standard template for all government websites |
| **Annual Website Audit** | Examines the status of all government websites annually |
| **IWMS and Web Monitoring System** | Developed and operates these systems |
| **System Management** | Provides system managers to government bodies to help manage their websites |
| **Technical Standards** | Sets technical standards for government IT systems |
| **Capacity Building** | Trains government personnel on IT systems |
| **Procurement Support** | Advises on IT procurement for government agencies |

**Key Fact:** DoIT is **not** a policy-making body – it **implements** policies set by MoCIT.

TechPSC

## 11.5.3 National Information Technology Center (NITC) / Government Integrated Data Center (GIDC)

**Overview:** NITC is the central IT service provider for the Government of Nepal. GIDC is its core facility for hosting government data and applications.

**Contact Information (for reference):**

- **Location:** Singhdarbar, Kathmandu
- **Phone:** +977-1-5970646 (Technical Support), 4211917
- **Email:** info@nitc.gov.np

**Key Responsibilities of NITC (Exam Focus):**

| Responsibility | Description |
|---|---|
| **Government Hosting** | Hosts all government websites and applications (mandated by Website Directive 2078) |
| **GIDC Operation** | Manages the Government Integrated Data Center – the central data repository for government data |
| **Infrastructure** | Provides server, storage, and network infrastructure to government agencies |
| **Technical Support** | Offers technical support to government offices for IT systems |
| **Security Monitoring** | Works with Security Operation/Monitoring Center to secure government IT assets |

**Why GIDC is Important:**

- **Centralization:** Instead of each ministry having its own servers, all are hosted centrally
- **Security:** Better security controls, monitoring, and backup
- **Cost Savings:** Reduced hardware and maintenance costs
- **Disaster Recovery:** Centralized backup and recovery planning

**Important for Exam:** The **Government Website Development and Management Directive, 2078** mandates that **all government websites must be hosted on GIDC** .

## 11.5.4 Security Operation / Monitoring Center

**Overview:** A dedicated facility (or function) responsible for **continuous monitoring, detection, and response** to security threats targeting government IT infrastructure.

**Key Functions (Exam Focus):**

| Function | Description |
|---|---|
| **24/7 Monitoring** | Continuously monitors government networks, servers, and applications for security incidents |
| **Threat Detection** | Identifies potential intrusions, malware, DDoS attacks, and unauthorized access |
| **Incident Response** | Coordinates with ITERT and other agencies to contain and mitigate security breaches |
| **Web Monitoring** | Specifically monitors government websites for defacement, downtime, and hacking attempts |
| **Alerting** | Sends real-time alerts to administrators when threats are detected |
| **Forensics** | Assists in investigating security incidents (preserving digital evidence) |

**Relationship with Other Institutions:**

| Institution | Relationship |
|---|---|
| **ITERT** | Coordinates on incident response; ITERT handles national-level coordination, SOC handles monitoring |
| **NITC/GIDC** | SOC monitors the infrastructure hosted at GIDC |
| **DoIT** | Works with DoIT on web monitoring (Web Monitoring System) |
| **Cyber Bureau (Nepal Police)** | SOC may escalate criminal incidents for investigation |

**Key Point for Exam:** The **Web Monitoring System** launched by DoIT in 2023 is a key tool used by the Security Operation/Monitoring Center to monitor government websites .

# Quick Revision Table (Section 11 - Legislations and Institutions)

| Legislation / Institution | Year (BS) | Key Purpose |
|---|---|---|
| **ICT Policy** | 2072 | Foundational ICT policy; led to creation of NPCERT/ITERT, Cyber Bureau |
| **Electronic Transaction Act (ETA)** | 2063 | Legal recognition of e-records, digital signatures, cybercrime offences |
| **ITERT Directive** | 2075 | National CERT operations; incident response coordination |
| **Government Website Directive** | 2078 | Standardizes, secures, and centralizes government websites on GIDC |
| **National Cyber Security Policy** | 2080 | Nepal's first dedicated cybersecurity policy (newer than ICT Policy 2072) |
| **MoCIT** | - | Policy-making; issues directives; leads digital transformation |
| **DoIT** | - | Technical implementation; develops website templates; audits |
| **NITC / GIDC** | - | Hosts all government websites and data |
| **Security Operation/Monitoring Center** | - | 24/7 monitoring; detects and responds to threats |

TechPSC

# Important Exam Tips for Section 11

1. **Know the difference:**
   - **ICT Policy 2072** = Broad ICT framework
   - **ETA 2063** = Cybercrime and e-transactions law
   - **National Cyber Security Policy 2080** = Dedicated cybersecurity (newer)
2. **Remember the mandate:** Government websites **must** be hosted on **GIDC** (per Website Directive 2078).
3. **Linking institutions:**
   - MoCIT → Makes policy
   - DoIT → Implements policy (technical)
   - NITC/GIDC → Hosts infrastructure
   - Security Center → Monitors
   - ITERT → Responds to incidents
4. **Recent updates (for current affairs context):**
   - National Cyber Security Policy 2080 issued
   - IWMS and Web Monitoring System launched (2023)
   - Social Media Directive 2080 issued

TechPSC