

National Information Technology Authority – Uganda

National Information Security Framework (NISF)

NATIONAL INFORMATION SECURITY POLICY (NISF)



National Information Technology Authority – Uganda

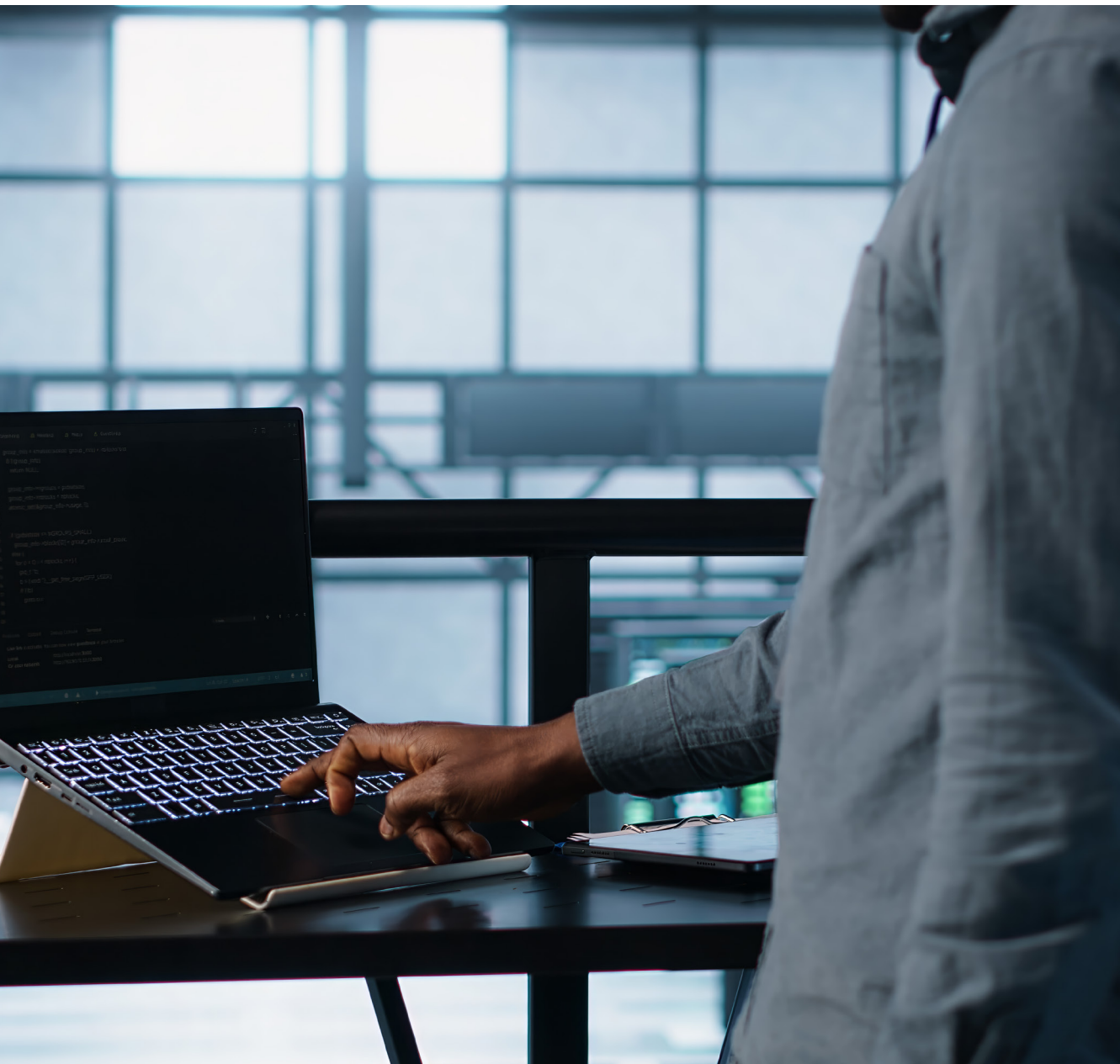
National Information Security Framework (NISF)

NATIONAL INFORMATION SECURITY POLICY (NISP)

2026

Version History

No.	Date	Section	Amendment
0.1	08//01/2014	Draft	Initial draft for NITA-U consideration.
1.0	11/02/2014	Final Draft	Updated after NITA-U Review.
2.0	08/09/2025	Draft	Enhanced draft for NITA-U consideration.



Preface

The digitalization of national services, economic sectors, and critical infrastructures has brought tremendous opportunities for the advancement of Uganda. It has expanded access to e-government services, strengthened financial inclusion, and positioned Uganda to benefit from the global digital economy. However, it has also introduced increasingly complex and evolving threats to the confidentiality, integrity, and availability of information assets that are essential to our national interests and citizen trust.

Recognizing these challenges, the Government of Uganda, through the **National Information Technology Authority – Uganda (NITA-U)**, has updated this **National Information Security Policy (NISP)** to provide a unified, risk-based framework for protecting the nation's information resources.

This Policy establishes the **mandatory minimum-security requirements** for all **Ministries, Departments, Agencies (MDAs), Local Governments (LGs), and Critical Information Infrastructure (CII) Operators**, as well as other public and private sector entities that process national information. It introduces a structured approach built on four **policy pillars** — Security Governance, Personnel Security, Physical Security, and Information Security — which are further operationalised through the **National Information Security Framework (NISF)** and its supporting toolkits.

The NISP aligns with **global best practices and standards**, including **ISO/IEC 27001/27002, ISO/IEC 27035, NIST Cybersecurity Framework, CIS Controls, COBIT, and OWASP**, while remaining firmly rooted in Uganda's **legal, regulatory, and operational environment** such as the **Data Protection and Privacy Act (DPPA, 2019)**, the **Computer Misuse Act (2011, amended 2022)**, and the **NITA-U Act (2009)**.

The successful implementation of this Policy requires **collective effort, leadership commitment, continuous adaptation, and a culture of proactive security** across all sectors. It calls upon all stakeholders — government, regulators, private sector operators, academia, and civil society — to take ownership of their responsibilities and work collaboratively to ensure Uganda's **digital resilience**.

Together, by adopting this Policy and its accompanying toolkits, Uganda will be better positioned to **mitigate cyber risks, protect critical infrastructure, safeguard citizen data, and enable secure innovation** for a thriving digital future.



Dr. Hatwib Mugasa
EXECUTIVE DIRECTOR

National Information Technology Authority – Uganda (NITA-U)

Table of Contents

Preface	iii
Abbreviations and Acronyms.	vii
1. Introduction.	1
1.1 Overview	1
1.2 Applicability of the National Information Security Policy	2
1.2.1 Critical Infrastructure (CI)	3
1.2.2 Critical Information Infrastructure (CII)	3
1.3 Policy Review Cycle	3
1.4 Structure of the Policy	3
1.5 Adaptation of Security Controls	4
1.6 National Legislation and Regulations.	4
1.7 International Standards and Cybersecurity Frameworks	5
2. Policy Context	6
2.1 Uganda National Cybersecurity Strategy (2022–2026)	6
2.1.1 Purpose of the Strategy	7
2.1.2 Strategic Initiatives under the Strategy	7
2.1.3 Objectives of the Strategy	8
2.1.4 Global, Regional & Uganda-Specific Cybersecurity Trends	8
2.1.5 International Benchmarking	11
2.1.6 NISP Pillars and Linkages (Enhanced)	12
2.1.6.1 NISP Policy Pillars	12
2.1.6.2 Linkage to NISF Standards (SS1–SS7)	13
2.1.6.3 Integration with Toolkits	13
2.1.7 Legal, Strategic & Framework Linkages	14
2.1.7.1 Linkages to National Acts and Regulations	14
2.1.7.2 Linkages to International Standards and Frameworks	15
2.1.7.3 Linkages to Regional & Continental Frameworks	15
2.1.7.4 Linkages to National Strategies & Programmes	15
2.2 Relationship Between the Cybersecurity Strategy and the NISP	16
3. Guiding Principles	17
3.1 Top Leadership Accountability	17
3.2 Collective Responsibility	17
3.3 Personal Accountability	17
3.4 Risk Management and Proportionality	18
3.5 Secure and Assured Sharing	18
3.6 Suitable, Trustworthy, and Reliable Staff	18
3.7 Resilience	18

4.	Uganda-Specific Enhancements	20
4.1	Breach Notification	20
4.2	Expanded Scope of Application	20
4.3	National Cybersecurity Skills Pipeline	21
4.4	Sector-Specific Priorities	21
5.	NISP Policy Pillars	23
5.1	Security Governance	23
5.1.1	Introduction	23
5.1.2	Policy Statement on Information Security	24
5.1.2.1	Issue Policy Statement on Information Security	24
5.1.2.2	Articulate Information Risk Appetite	25
5.1.3	Information Security Organization	25
5.1.3.1	Responsibilities of Boards and Accounting Officers	26
5.1.3.2	Responsibilities of the Information Risk Owner (IRO)	27
5.1.3.3	Responsibilities of Data Protection Officer (DPO)	27
5.1.3.4	Responsibilities of Information Asset Owners	28
5.1.3.5	Responsibilities of the Security Coordination Group	28
5.1.3.6	Responsibilities of the Operational Security Team	28
5.1.4	Responsibilities of Technical and Specialized Roles	28
5.1.5	Responsibilities of Project and Operational Roles	29
5.1.6	Risk Management	30
5.1.7	Awareness, Education, and Training	31
5.1.8	Business Continuity and Disaster Recovery	31
5.1.9	Incident Management	31
5.1.10	Assurance and Compliance	32
5.2	Information Security	32
5.2.1	Introduction	32
5.2.2	Information Security Policy	32
5.2.3	Asset Management	33
5.2.4	Emerging Technology Security	33
5.2.4.1	Cloud Computing	33
5.2.4.2	Application Programming Interfaces (APIs)	34
5.2.4.3	Artificial Intelligence (AI)	34
5.2.4.4	Operational Technology / Industrial Control Systems (OT/ICS)	35
5.2.5	Secure Information Sharing	35
5.2.6	Supply Chain Security	35
5.2.7	Access Management	36
5.2.8	Network Security Controls	36
5.2.9	Malicious Code Protection	37
5.2.10	Portable and Removable Media Security	37

5.2.11	Remote Access Security	37
5.2.12	Protective Monitoring	38
5.2.13	Information Back-Ups	38
5.2.14	Security Accreditation	38
5.3	Personnel Security	39
5.3.1	Introduction	39
5.3.2	Security Roles and Responsibilities	40
5.3.3	Baseline Security Clearance	40
5.3.4	National Security Vetting	40
5.3.5	Ongoing Personnel Security Management	41
5.3.6	Exit Management.	41
5.3.7	Security Awareness and Culture.	42
5.4	Physical Security	42
5.4.1	Introduction	42
5.4.2	Physical Security Perimeter	42
5.4.3	Entry Controls	43
5.4.4	Internal Data Centre Physical Access Controls	43
5.4.5	Equipment Protection	44
5.4.6	Secure Equipment Disposal and Re-Use	44
5.4.7	Physical Security Monitoring & Response.	44
5.4.8	Physical Security Policy Reviews	45
	Appendix A – Accompanying Documents	46
	Appendix B - Definitions of Terms.	48
	Appendix C - RACI Matrix – Specialized Roles for Emerging Technology Security	52

Abbreviations and Acronyms.

Acronym	Meaning
AI	Artificial Intelligence
API	Application Programming Interface
BCP	Business Continuity Plan.
BS	Baseline Security.
BSI IT-Grund Schutz	German Federal Office for Information Security's IT Baseline Protection (IT-Grund Schutz)
BYOD	Bring Your Own Device.
CA	Certificate Authority
CCTV	Closed-Circuit Television.
CI	Critical Infrastructure.
CII	Critical Information Infrastructure.
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CSA	Cloud Security Alliance
DIS	Directorate of Information Security.
DPO	Data Protection Officer
DPPA	Data Protection and Privacy Act
DRP	Disaster Recovery Plan.
GoU	Government of Uganda.
ICT	Information and Communication Technology
IDS/IPS	Intrusion Detection System/Intrusion Prevention System.
IRO	Information Risk Officer.
ISMS	Information Security Management System.
ISO/ IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information Technology.
MFA	Multi-Factor Authentication.
NISAG	National Information Security Advisory Group.
NISF	National Information Security Framework.
NISP	National Information Security Policy.
NITA-U	National Information Technology Authority-Uganda.
OT	Operational Technology
PDCA	Plan-Do-Check-Act.

PDI	Personal Data Inventory
PKI	Public Key Infrastructure
RoPA	Records of Processing Activities
RTP	Risk Treatment Plan
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SOC	Security Operations Center
TLP	Traffic Light Protocol
UPS	Uninterruptible Power Supplies.
USB	Universal Serial Bus.
VPN	Virtual Private Network
WAF	Web Application Firewall
ZTA	Zero Trust Architecture



1. Introduction.

1.1 Overview

The **National Information Security Policy (NISP)** establishes the overarching vision and principles for securing Uganda's digital ecosystem. It provides the national anchor from which the **National Information Security Framework (NISF)**, sectoral standards, and supporting toolkits derive.

Since the initial issuance of the NISP in 2014, Uganda's digital transformation has accelerated rapidly, with expanding **e-Government services, Critical Information Infrastructure (CII)**, and cross-border data flows. This transformation is increasingly underpinned by the adoption of **cloud-hosted platforms, Application Programming Interfaces (APIs), Artificial Intelligence (AI), and Operational Technology/ Industrial Control Systems (OT/ICS)**. While these technologies create new opportunities for efficiency and growth, they also expose MDAs, Local Governments (LGs), and CII Operators to increasingly **sophisticated cyber threats**.

To remain relevant in this dynamic environment, the Enhanced NISP builds on the original policy pillars of:

1. Security Governance
2. Personnel Security
3. Physical Security
4. Information Security

and strengthens them through integration with the **seven NISF Security Standards (SS1–SS7)**:

- SS1: Technical Risk Assessment
- SS2: Risk Management & Accreditation
- SS3: Security Classification

- SS4: Personnel Security
- SS5: Physical Security
- SS6: Incident Management
- SS7: Data Privacy & Protection

The policy is further operationalized through **supporting toolkits and mechanisms** including:

- MDA & LG Compliance Checklist
- Corrective Action Plan (CAP) Register and Dashboard
- Compliance & Maturity Dashboards
- Insider Threat Register & Dashboard
- Incident Register & KPI Dashboard
- Statement of Applicability (SoA) Template
- Integrated Implementation Guidance Notes

These toolkits provide measurable, auditable evidence of implementation, enabling MDAs, LGs, and CII operators to demonstrate compliance, track residual risks, and support national oversight by NITA-U and sector regulators.

The Enhanced NISP also embeds **Uganda-specific regulatory requirements**, including:

- The **72-hour data breach notification rule** under the Data Protection and Privacy Act (2019) and Regulations (2021).
- Integration of **Local Governments (LGs)** into compliance and oversight obligations, alongside MDAs and CII operators.
- Stronger focus on **national capacity-building**, including skills development, awareness campaigns, and sector-specific cybersecurity readiness.

Finally, the Enhanced NISP aligns with **international standards and best practices**, notably ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, NIST Cybersecurity Framework, CIS Controls, and GDPR, while taking lessons from advanced digital nations such as Estonia and Singapore. This ensures that Uganda's policy is both **globally benchmarked** and **locally contextualized**, positioning the country to achieve secure, resilient, and trusted digital transformation.

1.2 Applicability of the National Information Security Policy

This policy is mandatory for all public and private sector organizations that use, own, and/or operate:

- Protected computers,
- Critical Information Infrastructure,

- Official communications systems, and
- Personal data processing environments.

In accordance with the most recent amendments (2022) to Uganda's Computer Misuse Act, protected computers are now defined as those integral to, or utilized in, the operation of:

- National security,
- Defense, diplomacy, and law enforcement,
- Communications infrastructure,
- Banking and financial services,
- Public utilities,
- Public key infrastructure, and
- Public safety.

These provisions reflect the Act's expanded scope, emphasizing the critical importance of these systems in safeguarding national interests and ensuring the integrity of essential services.

Official communications encompass information that Ministries, Departments, Agencies, and Local Governments (MDALs) create and process in daily business activities. While generally less sensitive than data processed by protected computers, their loss, theft, or unauthorized disclosure can still cause reputational, operational, and legal harm.

Personal data refers to any information relating to an identifiable individual, subject to the protections under the Data Protection and Privacy Act (2019).

1.2.1 Critical Infrastructure (CI)

The policy adopts the **International Telecommunication Union (ITU)** definition of **Critical Infrastructure** — systems whose disruption would have a debilitating impact on public health, safety, commerce, national security, or any combination thereof.

Examples include:

- Power generation and distribution systems,
- National transport networks,
- Water treatment and distribution,
- Financial market infrastructures.

1.2.2 Critical Information Infrastructure (CII)

Critical Information Infrastructure refers to information and communication technologies (ICTs) that operate or control CI sectors such as health, water, transport, government, finance, energy, and emergency services.

It also includes cloud-hosted systems, industrial control systems (ICS), SCADA environments, and specialized operational networks that, if disrupted, could impair essential services.

1.3 Policy Review Cycle

The National Information Technology Authority – Uganda (NITA-U) shall review this policy at least annually or as required to address:

- Emerging cyber threats and global threat intelligence,
- Advances in technology (including AI, cloud, and OT security),
- Evolving business and regulatory requirements, and
- Lessons learned from significant incidents and audits.

Reviews will be informed by national security priorities, the National Cybersecurity Strategy (2022–2026), and stakeholder feedback.

1.4 Structure of the Policy

The National Information Security Framework (NISF) is structured into multiple tiers, each serving a distinct purpose in strengthening national information security. This policy sits at Tier Three, which focuses on defining mandatory minimum-security requirements. These requirements are organized into four thematic areas:

1. Security Governance
2. Information Security
3. Personnel Security
4. Physical Security

While the NISF tiers represent the overall hierarchy of policies, standards, and guidelines, the thematic areas define the specific domains in which these requirements must be applied.

1.5 Adaptation of Security Controls

The mandatory requirements in this policy establish baseline security controls. Organizations are required to customize and strengthen these controls to address their specific:

- Risk environment,
- Critical assets,
- Sector-specific threats, and
- Regulatory obligations.

All governing boards and senior management must:

- Identify additional controls to address unique cyber threats,
- Align measures with their risk appetite and asset sensitivity,
- Continuously review and update controls as threats, technologies, and operations evolve.

This approach ensures that controls remain effective, proportionate, and forward-looking, in support of Uganda's goal to safeguard national interests and maintain public trust.

1.6 National Legislation and Regulations.

The National Information Security Policy is underpinned by the following key legislative instruments that define the legal and regulatory landscape for cybersecurity, data protection, digital transactions, and information system governance in Uganda:

Legislative Instrument	Year	Notes
The National Information Technology Authority, Uganda (Amendment) Act	2024	Introduces new mandates for NITA-U
The Computer Misuse (Amendment) Act	2022	Addresses social media abuse, child data protection, hate speech, etc.
The Data Protection and Privacy Regulations	2021	Clarifies compliance, breach reporting, and registration procedures
The Data Protection and Privacy Act	2019	Foundation for data subject rights, lawful processing
Information Technology Certification Regulations (Amendment)	2018	Updates provider accreditation mechanisms
The Computer Misuse Act	2011	Addresses cybercrime and unauthorized access
The Electronic Signatures Act	2011	Legal recognition of electronic signatures
The Electronic Transactions Act	2011	Legitimizes e-commerce and digital contracts
The Regulation of Interception of Communications Act	2010	Covers lawful interception of digital communications
The National Information Technology Authority, Uganda Act	2009	Mandate for NITA-U

Legislative Instrument	Year	Notes
The Uganda Citizenship and Immigration Control (Amendments) Act	2009	Digital identity and national registries context
The National Security Council Act	2009	National security governance framework
The Employment Act	2006	Personnel and labour policy for digital workplaces
The Police (Amendment) Act	2006	Law enforcement in digital crime matters
The Access to Information Act	2005	Transparency and information access rights
The Uganda People's Defence Forces Act	2005	Military involvement in national cybersecurity
The Security Organizations Act	1987	Establishes national intelligence and cyber response mandates
The Official Secrets Act	1964	Protects classified information from unauthorized disclosure

1.7 International Standards and Cybersecurity Frameworks

The implementation of this policy is informed and supported by internationally recognized information security standards, risk management principles, and technical control frameworks, including but not limited to:

Standard / Framework	Year	Issuing Body	Relevance
ISO/IEC 27001:2022	2022	ISO	Core standard for ISMS implementation
ISO/IEC 27002:2022	2022	ISO	Implementation of guidance on controls.
ISO/IEC 27005:2022	2022	ISO	Risk management techniques for ISMS
ISO/IEC 31010:2019	2019	ISO	Risk assessment techniques
ISO 31000:2018	2018	ISO	Enterprise risk management framework
NIST SP 800-53 Rev. 5	2020	NIST	Security and privacy control catalogue
NIST SP 800-61 Rev. 3	2024	NIST	Incident response and coordination guide
NIST Cybersecurity Framework (CSF) 2.0	2024	NIST	Comprehensive cybersecurity framework
NIST SP 800-88 Rev. 1	2014	NIST	Media sanitization best practices
CIS Controls v8	2021	CIS	Practical security control sets
ISA/IEC 62443 Series	2020	ISA/IEC	Security for Industrial Control Systems (ICS/OT)
OWASP API Security Top 10	2023	OWASP	Application and API vulnerability guide

2. Policy Context

The Government of Uganda (GoU) regards information security as a foundational enabler for the efficient, safe, and secure delivery of public services. It also serves as a critical pillar of national security, ensuring the protection of Critical Information Infrastructure (CII) and Critical Infrastructure (CI) that sustain the nation's economy and public welfare.

With the growing complexity of the cyber threat landscape — including ransomware-as-a-service, AI-enabled attacks, supply-chain compromises, and insider threats — the protection of national information assets has become a matter of urgent priority. Safeguarding these assets is no longer an IT function alone, but a **national imperative** that underpins public trust, economic stability, and operational continuity.

Uganda's approach to information security is anchored in:

- The **Data Protection and Privacy Act (DPPA), 2019**, establishing obligations for lawful data processing, breach notification, and data-subject rights.
- The **Uganda National Cybersecurity Strategy (2022–2026)**, which provides a forward-looking roadmap for coordinated governance, resilience, and awareness.
- The **National Information Security Policy (NISP)**, which defines minimum security requirements and national policy pillars.
- The **National Information Security Framework (NISF)**, which operationalises NISP through seven Security Standards (SS1–SS7) and integrated toolkits.

Together, these instruments form a **comprehensive cybersecurity governance model**, ensuring that Ministries, Departments, Agencies (MDAs), Local Governments (LGs), and CI Operators implement evidence-based security controls that are auditable, enforceable, and aligned with global best practices.

2.1 Uganda National Cybersecurity Strategy (2022–2026)

The Government of Uganda recognizes that cybersecurity is a cornerstone of national security, economic resilience, and citizen trust in digital services. The Uganda National Cybersecurity Strategy (2022–2026) builds on earlier initiatives but introduces a **comprehensive, risk-based, and forward-looking approach** aligned with international best practices and regional commitments.

The Strategy emphasizes:

- **Safeguarding critical information assets** — protecting the confidentiality, integrity, and availability (CIA) of national information systems.
- **Ensuring business and service continuity** — maintaining resilience for government services and critical private sector functions.

- **Protecting citizens' personal data** — in compliance with the Data Protection and Privacy Act (2019) and international privacy principles.
- **Securing Critical Information Infrastructure (CII)** — including energy, telecommunications, water, finance, health, and transport sectors.
- **Strengthening national resilience against evolving threats** — such as ransomware-as-a-service (RaaS), AI-enabled attacks, supply-chain compromises, and insider threats.
- **Promoting coordinated governance** — through NITA-U, sector regulators, and the National Cybersecurity Coordination Centre (NCCC).
- **Building capacity and public awareness** — scaling technical skills, cyber awareness campaigns, and partnerships with academia, civil society, and the private sector.

2.1.1 Purpose of the Strategy

The Uganda National Cybersecurity Strategy (2022–2026) was developed by the Government of Uganda, through the Ministry of ICT and National Guidance, to provide a comprehensive national response to evolving cyber threats.

Its purpose is to:

- Build a **safe, resilient, and trusted digital ecosystem** that underpins Uganda's social and economic development.

- Protect **critical national infrastructure** and digital services from disruption, compromise, or exploitation.
- Safeguard **citizens' rights and personal data**, ensuring compliance with the Data Protection and Privacy Act (2019).
- Enhance Uganda's **cyber resilience and preparedness** against national, regional, and global threats.
- Promote a **whole-of-society approach**, engaging government, private sector, academia, and civil society.

2.1.2 Strategic Initiatives under the Strategy

To achieve its purpose, the Strategy sets out key initiatives, including:

- **Establishing a National Cybersecurity Coordination Centre (NCCC)** under NITA-U for national-level oversight and coordination.
- **Strengthening incident response capacity** through sectoral CSIRTs and enhancement of CERT-UG.
- **Rolling out Public Key Infrastructure (PKI) and secure digital identity systems** to support trusted e-government and e-commerce services.
- **Supporting Micro, Small, and Medium Enterprises (MSMEs)** with tailored cybersecurity guidelines, awareness, and training.

- **Conducting regular risk assessments, incident drills, and threat intelligence sharing** across MDAs, LGs, and CII Operators.
- **Implementing a national cybersecurity skills pipeline**, including professional training, academic integration, and capacity building for law enforcement and judiciary.
- **Launching national awareness campaigns** to promote public trust and safe use of digital services.
- **Formalising public-private partnerships (PPPs)** to enhance collaboration, information sharing, and resilience of critical supply chains.
- **Updating legislation and regulatory frameworks** to address emerging technologies, such as Artificial Intelligence (AI), Cloud Computing, APIs, and OT/ICS environments.

2.1.3 Objectives of the Strategy

The Strategy is designed to achieve the following objectives:

- 1. **Strengthen national cybersecurity preparedness and response capabilities** by building institutional frameworks, CSIRTs, and incident management processes.
- 2. **Protect critical information infrastructure (CII)** across essential sectors such as telecoms, energy, water, finance, health, and transport.
- 3. **Enhance cyber resilience and trust** in Uganda's digital economy and e-government services.

- 4. **Promote a cyber-skilled workforce and digital literacy**, ensuring cybersecurity is mainstreamed into education, professional training, and capacity-building initiatives.
- 5. **Foster international, regional, and multilateral partnerships** to support intelligence sharing, capacity building, and harmonisation of standards.
- 6. **Provide an enabling governance and legal framework** that keeps pace with evolving cyber threats and emerging technologies.

2.1.4 Global, Regional & Uganda-Specific Cybersecurity Trends

The global cybersecurity landscape is evolving at unprecedented speed, driven by technological, geopolitical, and economic forces. For Uganda and Africa, these shifts present both opportunities and significant risks, especially for **Critical Information Infrastructure (CII)** in energy, finance, health, and transport.

1. Sophistication of Cyber Threats

- **Ransomware-as-a-Service (RaaS):** Criminal syndicates now offer ransomware kits as a service, lowering barriers to entry.
 - ~ *Uganda/Africa:* Recent ransomware cases have targeted hospitals, education institutions, and government agencies across East Africa, highlighting systemic risk to service delivery.

- **AI-enabled phishing and disinformation:** Attackers use AI to craft convincing spear-phishing emails and disinformation campaigns.

- ~ *Uganda:* Government ministries and agencies have already suffered targeted phishing campaigns, resulting in credential theft and service outages.

- **Advanced Persistent Threats (APTs):** State-sponsored and organized cyber groups focus on espionage, data theft, and sabotage.

- ~ *CII in Uganda:* Energy and telecom operators are key targets due to geopolitical and economic positioning.

- **Insider threats:** Staff misuse of access, whether malicious or accidental, remains a leading cause of breaches.

- ~ *Uganda:* Weak vetting and absence of continuous monitoring in MDAs and LGs increase exposure.

- **Supply chain attacks:** Threat actors increasingly compromise third-party vendors, ICT suppliers, or service providers to gain indirect access to government and critical sector systems.

- ~ *Uganda:* Recent incidents in East Africa have highlighted risks in outsourced IT services, core banking software, and government procurement systems, requiring stronger due diligence and supply chain security.

2. Technological Disruption

- **Quantum computing:** Although still emerging, it threatens existing encryption, demanding crypto-agility and forward planning.

- **Cloud services & SaaS ecosystems:** Accelerated migration of government workloads to cloud platforms introduces new supply-chain dependencies.

- ~ *Uganda:* Many MDAs and LGs now host services on regional and global cloud providers with insufficient security-by-contract safeguards.

- **API-driven e-Government services:** APIs are now the backbone of digital transformation but expose data to injection and leakage attacks.

- ~ *Uganda:* Several national platforms (tax, health, education) rely on APIs, requiring stronger governance.

- **OT/ICS and IT convergence:** Industrial Control Systems (ICS) in utilities and transport are increasingly networked, exposing CII to cyber-physical attacks.

- ~ *Africa:* Power grid and oil/gas operators have already reported ICS malware incidents.

3. Governance & Trust Models

➤ **Zero Trust Architecture:** Global shift from perimeter-based models to continuous verification of users, devices, and systems.

~ *Uganda:* Few MDAs have adopted Zero Trust, leaving networks vulnerable to lateral movement after a breach.

➤ **Secure-by-Design and Secure-by-Default:** International supply-chain frameworks mandate security embedded from the outset.

~ *Africa:* Procurement processes still treat cybersecurity as an add-on, not a baseline requirement.

➤ **Privacy-by-Design:** Driven by GDPR and equivalent laws, ensuring that privacy is integral to systems and processes.

~ *Uganda:* The **Data Protection and Privacy Act (2019)** establishes this requirement, but implementation remains inconsistent across sectors.

4. Regional & Continental Developments

➤ **African Union:** The Malabo Convention provides a baseline for data protection and cybersecurity, but implementation is uneven.

➤ **East African Community (EAC):** Regional harmonization is underway, creating opportunities for cross-border cooperation and threat intelligence sharing.

➤ **Uganda:** CERT-UG continues to strengthen but needs deeper integration with sectoral CERTs (finance, telecom, energy). The **Smart Uganda** and **e-Government 2025 strategies** expand digital opportunities but simultaneously enlarge the attack surface.

5. Implications for Uganda

➤ Uganda must:

- ~ Prioritize **CII protection** (utilities, energy, telecoms, finance, health, transport).
- ~ Strengthen **incident reporting and escalation** mechanisms, including the **72-hour breach notification rule** under the Data Protection and Privacy Act.
- ~ Scale up **cybersecurity skills development** and awareness campaigns across MDAs, LGs, and CII operators.
- ~ Institutionalize **continuous monitoring** via NISF toolkits (compliance dashboards, CAPs, insider threat registers, incident KPI dashboards).

➤ This ensures Uganda remains **locally grounded, regionally aligned, and globally benchmarked** in its cybersecurity posture.

2.1.5 International Benchmarking

Uganda's Enhanced NISP recognizes that while the national context is unique, valuable lessons can be drawn from **leading global and regional cybersecurity frameworks**. These benchmarks ensure that Uganda's policy remains **globally credible, regionally relevant, and nationally implementable**.

1. Estonia – Secure e-Government and National Resilience

➤ **Key Lesson:** Estonia is a global leader in secure e-Government through its **X-Road digital backbone**, which enforces end-to-end encryption, secure data exchange, and distributed trust.

➤ Relevance to Uganda:

- ~ As Uganda expands its e-Government services (Smart Uganda, eGov 2025), the Estonian model underscores the need for **secure-by-design data exchange frameworks**.
- ~ Estonia's commitment to **cyber exercises (e.g., Locked Shields through NATO CCDCOE)** demonstrates the importance of national cyber readiness drills — a model Uganda can emulate for **CII operators**.

2. Singapore – Critical Information Infrastructure (CII) Protection

➤ **Key Lesson:** Singapore's **Cybersecurity Act (2018)** designates CII sectors (energy, water, healthcare, transport, government, telecoms, finance) and imposes strict obligations on operators, including incident reporting, audits, and licensing.

➤ Relevance to Uganda:

- ~ Uganda's NISP must emphasize **CII designation, protection, and regulation** across sectors such as energy, finance, telecoms, transport, and health.
- ~ Singapore also demonstrates effective **public-private partnerships**, ensuring industry shares responsibility with government. Uganda can adopt similar models to improve **MDAs-LGs-private sector collaboration**.

3. EU NIS2 Directive – Harmonization and Accountability

➤ **Key Lesson:** The **EU's NIS2 Directive (2023)** expands security obligations across essential and digital service providers, introduces strict supervisory measures, and enforces breach reporting.

➤ **Relevance to Uganda:**

- ~ Provides a model for **regional harmonization** within the East African Community (EAC).
- ~ Reinforces Uganda's adoption of **mandatory breach notification** under the Data Protection and Privacy Act (2019).
- ~ Emphasizes the role of regulators in **supervision, penalties, and enforcement** — a gap Uganda must address to strengthen accountability.

4. **African Continental Lessons**

- **Key Lesson:** The **AU Malabo Convention (2014)** sets a continental baseline for data protection and cybersecurity, although adoption remains patchy.

➤ **Relevance to Uganda:**

- ~ Uganda can position itself as a **regional leader** by fully operationalizing NISP/NISF in line with Malabo, creating an example for other AU member states.
- ~ Regional harmonization (EAC, COMESA) offers opportunities for **cross-border CERT collaboration and cyber capacity-building**.

5. **Implications for Uganda**

- Uganda's Enhanced NISP is strengthened by benchmarking against Estonia, Singapore, the EU, and AU frameworks.

➤ Key policy directions include:

- ~ **Secure-by-Design e-Gov services** (Estonia).
- ~ **Mandatory CII designation and protection** (Singapore).
- ~ **Regional harmonization and strong supervisory enforcement** (EU NIS2).
- ~ **Continental alignment with Malabo Convention** (AU).

- These benchmarks ensure that Uganda's policy is both **globally informed** and **locally actionable**, positioning the country to lead in East Africa's cybersecurity maturity.

2.1.6 **NISP Pillars and Linkages (Enhanced)**

The **National Information Security Policy (NISP)** is founded on four core pillars that articulate Uganda's high-level security objectives. These pillars remain constant, but their operationalisation is achieved through the **National Information Security Framework (NISF)** and its supporting toolkits.

2.1.6.1 **NISP Policy Pillars**

1. **Security Governance** – Establishing leadership, accountability, and structured risk management for information security across MDAs, LGs, and CII operators.
2. **Personnel Security** – Ensuring trusted, vetted, trained, and continuously monitored staff across the employment lifecycle (recruitment, retention, and exit).

3. **Physical Security** – Safeguarding people, premises, and physical assets against unauthorised access, tampering, and disruption.
4. **Information Security** – Protecting the confidentiality, integrity, and availability (CIA) of data, systems, and services through technical and procedural controls.

2.1.6.2 Linkage to NISF Standards (SS1–SS7)

To operationalise these policy pillars, NITA-U developed the **NISF Security Standards (SS1–SS7)**, which translate high-level objectives into detailed control requirements:

- **SS1 – Technical Risk Assessment**
→ Governance + Physical + Information Security
- **SS2 – Risk Management & Accreditation** → Governance + Information Security
- **SS3 – Security Classification** → Governance + Information Security
- **SS4 – Personnel Security** → Personnel + Governance
- **SS5 – Physical Security** → Physical + Governance
- **SS6 – Incident Management** → Governance + Information Security
- **SS7 – Data Privacy & Protection** → Governance + Information Security + Personnel

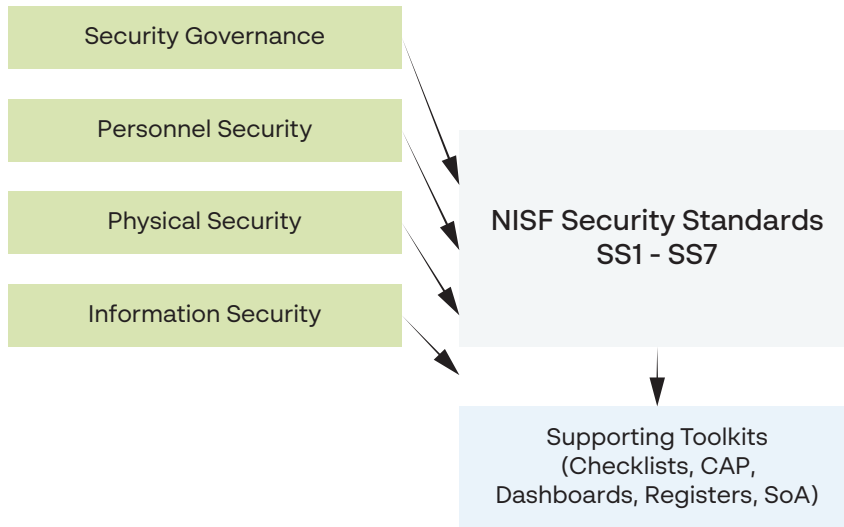
Each standard contains **baseline controls, implementation guidance, and evidence requirements**, all of which link back to one or more of the four NISP pillars.

2.1.6.3 Integration with Toolkits

The NISF is further supported by **practical toolkits** that provide measurable and auditable evidence of implementation:

- **MDA & LG Compliance Checklist**
– Self-assessment tool aligned to all SS controls.
- **Corrective Action Plan (CAP) Register & Dashboard** – Tracks remediation of identified gaps.
- **Compliance & Maturity Dashboards** – Auto-calculated metrics on control implementation and maturity levels.
- **Insider Threat Register & Dashboard** – Tracks insider-related risks and trends (SS4).
- **Incident Register & KPI Dashboard** – Monitors incident metrics (MTTD, MTTC, closure rates) (SS6).
- **Statement of Applicability (SoA) Template** – Documents control applicability and implementation status.
- **Integrated Implementation Guidance Notes** – Provide step-by-step evidence and control verification guidance.

NISP Pillars & Standards Integration Flow



2.1.7 Legal, Strategic & Framework Linkages

While the NISP is implemented through its four pillars, SS1–SS7, and supporting toolkits, it is also **anchored in national legislation, aligned to international standards, and harmonised with regional obligations**. These external linkages ensure that Uganda’s cybersecurity policy is both **locally enforceable and globally credible**.

2.1.7.1 Linkages to National Acts and Regulations

The NISP derives legal authority and enforceability from Uganda’s core statutes, including:

- **Data Protection and Privacy Act (DPPA), 2019 and Regulations (2021):** Establish lawful processing, data-subject rights, and the 72-hour breach notification rule.

- **NITA-U Act (2009) & e-Government Regulations:** Define NITA-U’s oversight mandate for ICT standards and interoperability.
- **Computer Misuse Act (2011, amended 2022):** Criminalises unauthorised access, data interference, and cybercrime.
- **Electronic Transactions Act (2011) & Electronic Signatures Act (2011):** Provide legal recognition of digital records and trust services.
- **Public Procurement and Disposal of Public Assets (PPDA) Act:** Requires integration of security requirements into procurement and supplier contracts.
- **National Records & Archives Act (2001):** Governs secure classification, retention, and disposal of records.

2.1.7.2 Linkages to International Standards and Frameworks

The NISP is aligned to recognised international good practices, including:

- **ISO/IEC 27001 & 27002:2022** – Information security management and control catalogue.
- **ISO/IEC 27005** – Risk assessment methodology.
- **ISO/IEC 27035** – Incident management lifecycle.
- **ISO/IEC 22301** – Business continuity.
- **ISO/IEC 27701** – Privacy management.
- **NIST Cybersecurity Framework (CSF 2.0)**: Identify, Protect, Detect, Respond, Recover.
- **NIST SP 800-53 & SP 800-61**: Security and incident response controls.
- **CIS Controls v8**: Practical security baselines.
- **OWASP ASVS & API Security Top 10**: Secure application and API integration practices.

2.1.7.3 Linkages to Regional & Continental Frameworks

The NISP also advances Uganda's obligations under regional and continental instruments:

- **African Union Malabo Convention (2014)**: Establishes continental baselines on cybersecurity, cybercrime, and personal data protection.

➤ **East African Community (EAC) Cybersecurity Framework:**

Enables regional harmonisation and cross-border cooperation.

- **COMESA & AfCFTA digital strategies**: Provide obligations for trusted data flows and interoperability across borders.

2.1.7.4 Linkages to National Strategies & Programmes

The NISP is fully integrated with Uganda's national ICT and digital transformation agenda:

- **Smart Uganda Master Plan (2020–2025)**: Prioritises secure digital infrastructure and services.
- **e-Government Strategy (2020–2025)**: Establishes interoperability, trust frameworks, and security-by-design.
- **National IT Project Management Methodology (NITPMM)**: Embeds information security throughout the ICT project lifecycle.
- **National Critical Infrastructure Protection framework (forthcoming)**: Introduces resilience obligations for CII sectors.

2.2 Relationship Between the Cybersecurity Strategy and the NISP

The Uganda National Cybersecurity Strategy (2022–2026) defines the **strategic vision and priorities** for safeguarding Uganda’s digital ecosystem. It sets the direction for national cyber resilience, critical infrastructure protection, skills development, and international cooperation.

The National Information Security Policy (NISP) complements this Strategy by translating its objectives into **mandatory minimum-security requirements** for all Ministries, Departments, Agencies (MDAs), Local Governments (LGs), and Critical Information Infrastructure (CII) Operators.

The National Information Security Framework (NISF) operationalises the NISP through seven Security Standards (SS1–SS7) and supporting toolkits, ensuring that compliance can be **measured, evidenced, and audited**.

Together, the **Strategy, NISP, and NISF** form a **tiered framework**:

- The **Strategy** sets the national vision and strategic objectives.
- The **NISP** defines mandatory policy requirements.
- The **NISF** provides implementation standards, control catalogues, and toolkits for compliance monitoring.



3. Guiding Principles

The following guiding principles provide the foundation for all decisions, actions, and security implementations under the National Information Security Policy (NISP). They are aligned with ISO/IEC 27001:2022, the NIST Cybersecurity Framework (CSF), and regional obligations to ensure that Uganda's approach is risk-driven, resilient, and future-proof.

3.1 Top Leadership Accountability

Ultimate responsibility for the protection of organizational information assets rests with Boards, Chief Executives, Cabinet Ministers, and Accounting Officers.

Leadership must:

- Establish clear accountability and reporting frameworks for information security governance.
- Approve and regularly review information security strategies, risk appetites, and performance indicators.
- Promote a security-by-design culture across all functions and projects.
- Integrate information security considerations into corporate governance, procurement, and strategic planning.
- Ensure that adequate resources (budget, personnel, and technology) are allocated to security programs.

3.2 Collective Responsibility

Information security is a shared responsibility involving every stakeholder, staff, contractors, partners, and suppliers. All must:

- Comply with approved security policies, procedures, and codes of conduct.
- Remain vigilant to identify, report, and help mitigate security threats or incidents.
- Actively participate in regular awareness, simulation, and capacity-building programs

3.3 Personal Accountability

Every individual must safeguard the information, systems, and resources entrusted to them. This includes:

- Following approved security rules, standards, and operational procedures.
- Preventing unauthorized access, disclosure, alteration, or destruction of information.
- Recognizing that non-compliance can result in disciplinary action, contract termination, or criminal prosecution under applicable laws.

3.4 Risk Management and Proportionality

Security measures must be informed by structured risk management processes to ensure they are **proportionate and cost-effective**:

- Conduct formal risk assessments periodically and whenever systems or threats change.
- Tailor controls based on **asset criticality, threat landscape, and business context**.
- Avoid over-engineering (excessive controls) or under-protection (insufficient controls).
- Apply the **defense-in-depth principle** to layer security measures.

3.5 Secure and Assured Sharing

Organizations must ensure the secure and reliable exchange of information internally and externally by:

- Applying suitable controls for all forms of information and transfer methods.
- Using encryption, authentication, and secure channels where appropriate.
- Ensuring that data classification guides the sharing process.
- Validating recipient authorization before sharing sensitive or classified information.

3.6 Suitable, Trustworthy, and Reliable Staff

Organizations must only grant access to critical IT assets to staff who are trustworthy and competent. This includes:

- Conducting background checks and vetting before hiring.
- Providing continuous training to maintain skills and awareness.
- Reviewing staff access privileges regularly and adjusting based on role changes.
- Removing access promptly upon termination or transfer.

3.7 Resilience

Organizations must embed resilience into all critical operations to withstand and recover from cyber-attacks, disasters, or disruptions. This includes:

- Developing and maintaining Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs).
- Testing these plans through simulations, tabletop exercises, and live drills at least annually.
- Ensuring that recovery objectives (RTOs, RPOs) are clearly defined and achievable.
- Maintaining redundancy for critical infrastructure, including cloud-based failover capabilities, where feasible.



4. Uganda-Specific Enhancements

Uganda's National Information Security Policy (NISP) must reflect local realities, legal frameworks, and sectoral priorities. The following enhancements build upon international best practices while ensuring alignment with Uganda's **Data Protection and Privacy Act (DPPA), 2019**, the e-Government Strategy, and NITA-U's mandate for oversight across Ministries, Departments, Agencies (MDAs), Local Governments (LGs), and Critical Infrastructure (CI) Operators.

4.1 Breach Notification

- All organisations are required to **notify the Personal Data Protection Office (PDPO)** of personal data breaches within **72 hours** of becoming aware of the incident, as mandated by the DPPA.
- MDAs, LGs, and CI Operators must also ensure **timely notification to sector regulators** (e.g., BoU, UCC, ERA, MoH) and, where relevant, affected data subjects.
- Incident reporting must align with the **national CSIRT/CERT-UG** processes to support national-level situational awareness.
- Information Security Breaches (non-personal data) must be reported to the National **CSIRT/CERT-UG** through the established channels.

4.2 Expanded Scope of Application

- The NISP applies to:
 - ~ **MDAs and LGs** – responsible for public service delivery, policy enforcement, and citizen data protection.
 - ~ **Critical Infrastructure Operators (CII)** – sectors such as finance, telecom, energy, water, transport, and healthcare.
 - ~ **Third-Party Providers** – contractors, cloud service providers, and vendors handling government or citizen data.
- This ensures coverage of the entire ecosystem of actors that process or safeguard Uganda's critical information assets.

4.3 National Cybersecurity Skills Pipeline

Uganda recognises that human capacity is as critical as technical controls. To address gaps in skills and awareness:

- Establish a **cybersecurity skills development pipeline** across academia, government, and industry.
- Partner with universities and TVET institutions to integrate **cybersecurity curricula** and professional certifications.
- Expand **awareness and digital hygiene campaigns** for public servants and citizens (e.g., phishing awareness, safe cloud use).
- Promote **specialised training tracks** for incident responders, auditors, and CI operators.
- Encourage public-private partnerships to build a **national pool of cybersecurity professionals** and reduce reliance on external expertise.

4.4 Sector-Specific Priorities

To reflect Uganda's national priorities, the following domains require enhanced controls and oversight:

- **Finance & Banking** – resilience against ransomware, mobile money fraud, and SWIFT-related cyberattacks.

~ Regulatory Reference: Bank of Uganda (BoU) Cybersecurity Guidelines, 2013; BoU Circulars on ICT Risk Management.

- **Energy & Utilities** – protection of SCADA/ICS/OT systems against supply chain and state-sponsored threats.

~ Regulatory Reference: Electricity Regulatory Authority (ERA) – sector safety and reliability directives; alignment with Uganda Energy Policy.

- **Healthcare** – safeguarding patient data, e-health platforms, and medical devices from breaches.

~ *Regulatory Reference:* Ministry of Health (MoH) eHealth Policy (2013) and DPPA, 2019.

- **Telecommunications** – enforcing lawful interception safeguards, SIM registration integrity, and data localisation.

~ *Regulatory Reference:* Uganda Communications Commission (UCC) Act and SIM Registration Regulations, 2012.

- **Government Cloud (GovCloud)**

– ensuring cloud security, vendor accountability, and multi-tenancy risk management.

~ *Regulatory Reference:* NITA-U eGovernment Regulations, 2014; NITA-U Cloud and Shared Services Guidelines.

These enhancements ensure that Uganda's NISP is **grounded in global standards but tailored to national legal, operational, and sectoral realities**.



5. NISP Policy Pillars

The National Information Security Policy (NISP) is founded on four strategic pillars that articulate Uganda's high-level security objectives. These pillars provide the overarching foundation for national resilience and are operationalised through the National Information Security Framework (NISF) and its supporting toolkits.

The four NISP Pillars are:

1. **Security Governance** – Establishing leadership, accountability, and structured risk management for information security across MDAs, LGs, and CII operators.
2. **Personnel Security** – Ensuring trusted, vetted, trained, and continuously monitored staff across the employment lifecycle (recruitment, retention, and exit).
3. **Physical Security** – Safeguarding people, premises, and physical assets against unauthorized access, tampering, and disruption.
4. **Information Security** – Protecting the confidentiality, integrity, and availability (CIA) of data, systems, and services through technical and procedural controls.

These pillars are further translated into actionable requirements through the **NISF Security Standards (SS1-SS7)**, which define baseline controls, implementation guidance, and evidence requirements. Supporting toolkits — such as the MDA Compliance Checklist, CAP Dashboard, Insider Threat Register, and Incident KPI Dashboard — ensure that the pillars can be measured, monitored, and continuously improved.

5.1 Security Governance

5.1.1 Introduction

Security governance refers to the leadership, organizational structures, policies, procedures, and accountability mechanisms required to direct, manage, and monitor information security effectively across the organization.

Security governance ensures that:

- Information security supports strategic business objectives.
- Risks are identified, assessed, treated, and reported consistently.
- Accountability is established at all organizational levels

This policy adopts the Plan–Do–Check–Act (PDCA) continuous improvement model, aligned with ISO/IEC 27001:2022 and the NIST Cybersecurity Framework (CSF), to ensure governance processes remain relevant to evolving threats.



Figure 1 – The PDCA Model for Information Security Governance.

5.1.2 Policy Statement on Information Security

Boards are supreme governing bodies that provide GoU and private sector organizations guidance on overall policy direction and strategies. Boards also facilitate, supervise and support management in the implementation of their mandate and strategies. Given that Boards must consider all the major risks affecting their organizations, it is crucial that they issue a policy statement on information security. The purpose of the Board statement is to underline the importance of information risk management to effective and secure operations.

Boards and Executive Leadership must:

- Recognize information as a strategic and critical business asset.
- Define and approve an Information Risk Appetite Statement.
- Assign clear roles and responsibilities for information security governance.
- Review the Information Security Policy at least annually or after major incidents.
- Embed security-by-design into strategies, operations, and projects.

To achieve the security outcomes mandated above, organizations must:

5.1.2.1 Issue Policy Statement on Information Security

Issuing a formal policy statement is essential: it clearly demonstrates leadership commitment, sets expectations, and embeds security into the organization's culture. Organizations must:

- Declare the organization's commitment to safeguarding information assets.
- Identify the Accounting Officer (or equivalent) as accountable for security governance.
- Require organization-wide awareness of policy provisions.
- Mandate regular training, compliance monitoring, and continuous improvement.



5.1.2.2 Articulate Information Risk Appetite

A statement of information Risk Appetite states the level and type of information risks that a given organization is willing to accept, tolerate or survive in the pursuit of its strategic goals.

The Information Risk Appetite Statement must guide:

- Risk acceptance, transfer, mitigation, and avoidance decisions.
- Prioritization of security investments.
- Governance oversight and tolerance for residual risk.
- Alignment with sector-specific regulations and threat environments

5.1.3 Information Security Organization

Organizations must have an effective organization to manage its information security activities. The Accounting Officer must establish such an organization with a view of achieving the mandatory minimum-security outcomes.

Organizations must implement an Information Security Management System (ISMS) with defined governance layers:

- Strategic – Boards & Accounting Officers.
- Tactical – Risk Owners, Data Protection Officers, Security Coordination Groups.
- Operational – Security Teams, IT Operations, and Control Owners.

The chart below visualizes the Information Security Management System (ISMS) structure, showing roles from The Board to operational teams to ensure accountability and effective coordination.

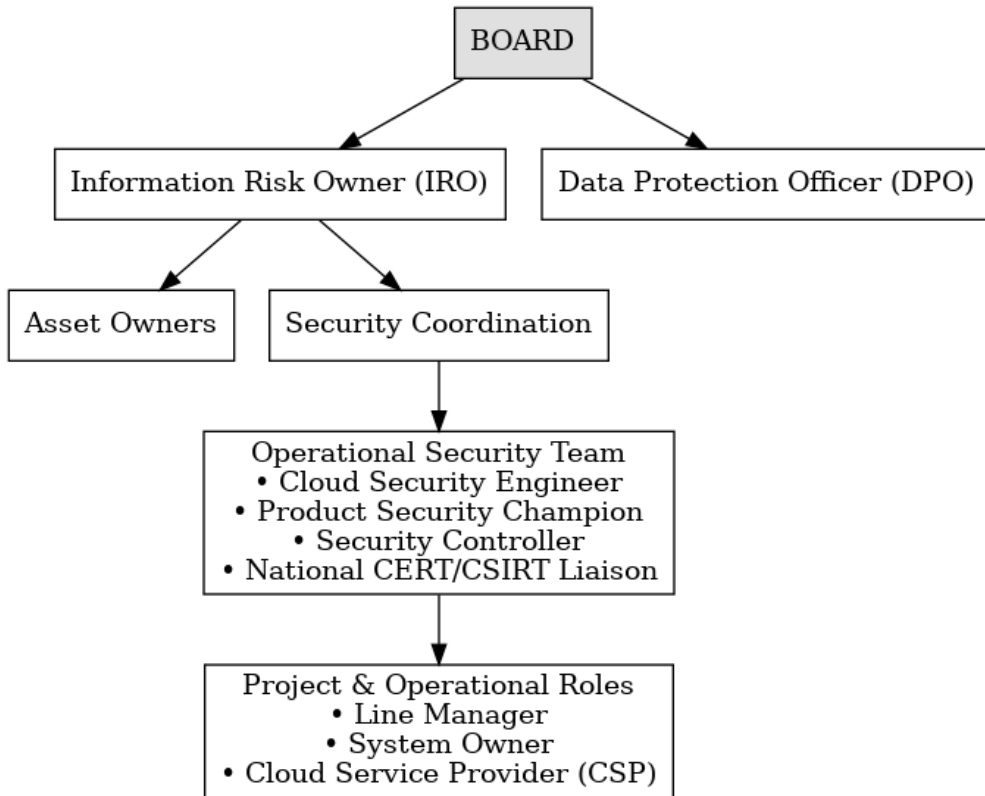


Figure 2 – The ISMS Structure.

5.1.3.1 Responsibilities of Boards and Accounting Officers

At the strategic level, the Board and Accounting Officers are responsible for ensuring strong governance of information security. Their key duties include:

- Recognizing information risk as a corporate risk and ensuring it is integrated into the organization's enterprise risk management and planning processes.
- Reviewing information security performance quarterly, including risk treatment updates, incident trends, and control effectiveness metrics, to inform continuous improvement.
- Including information security governance in annual reports and Statements on Internal Control, demonstrating commitment to legal compliance, risk management, and data protection.

5.1.3.2 Responsibilities of the Information Risk Owner (IRO)

The security organization shall appoint a Board-level official to the role of Information Risk Owner (IRO) with responsibilities to delegate. The Information Risk Owner must:

- Oversee risk identification, evaluation, and treatment across all assigned information assets.
- Validate risk categorization and control decisions in the Risk Treatment Plan (RTP).
- Ensure alignment of risk treatment with modern technologies such as cloud, APIs, AI, and operational technology (OT).
- Coordinate with the DPO to ensure that personnel security and privacy risks comply with the DPPA.
- Assess the physical and logical security of third-party and cloud service providers, including review of certifications and audit reports.
- Support tailoring of baseline controls based on asset criticality and impact levels.
- Foster a risk-aware culture in collaboration with the CISO, DPO, and asset owners.

5.1.3.3 Responsibilities of Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the data protection strategy and ensuring full compliance with the Data Protection and Privacy Act (DPPA), 2019 and its Regulations.

Key Responsibilities:

- Ensure organizational compliance with the DPPA and related regulations.
- Maintain the Personal Data Inventory (PDI) and Records of Processing Activities (RoPA).
- Advise on lawful basis for processing, consent models, and cross-border data transfers.
- Conduct and review Data Protection Impact Assessments (DPIAs), especially for systems processing sensitive or high-risk data.
- Work closely with the Information Security Incident Response Team (ISIRT) during security incidents involving personal data to assess breach severity, notify the Personal Data Protection Office (PDPO), and guide communication with affected individuals.
- Review personnel security vetting processes to ensure lawfulness and proportionality of personal data handling.
- Be consulted during the Authorization to Operate (ATO) process to provide data protection risk input for high-risk systems.
- Report to the Board independently of IT, ensuring impartial oversight of data protection activities.

5.1.3.4 Responsibilities of Information Asset Owners

Information asset owners must be heads of division or department and perform the following functions:

- Responsible for the classification, handling, and security of assigned information assets.
- Determine protection needs based on business criticality and CIA requirements.
- Collaborate with IRO in control selection and risk assessments.
- Approve access levels, data sharing mechanisms, and change control.
- Ensure compliance with protection and classification schemes.

5.1.3.5 Responsibilities of the Security Coordination Group

Led by Board-level Information Risk Owner, the information security coordinators must perform the following functions:

- Coordinates between IT, HR, Legal, DPO, and business units for ISMS activities.
- Manage security awareness training, incident response coordination, and escalation protocols.
- Tracks ISMS milestones, policy updates, control reviews, and internal audit follow-ups.
- Supports maintenance of the ISMS documentation library.

5.1.3.6 Responsibilities of the Operational Security Team

Led by chief information security officer or similar role, the operational security team must perform the following functions:

- Implements technical, physical, and administrative controls.
- Operates security infrastructure (e.g., SIEM, firewalls, encryption systems).
- Monitors security events, conducts log reviews, and remediates incidents.
- Enforces access controls and performs routine system hardening and patching.
- Participates in vulnerability assessments and penetration testing

5.1.3.7 Responsibilities of Technical and Specialized Roles

Cloud Security Engineer

Responsible for the secure configuration, monitoring, and continuous improvement of cloud environments to ensure compliance with the organization's ISMS and contractual obligations. Key duties:

- Implement and maintain cloud security architecture and hardening guidelines.
- Configure and monitor cloud workloads to detect threats, vulnerabilities, and misconfigurations.
- Collaborate with Cloud Service Providers (CSPs) to validate compliance with contractual and regulatory requirements.

- Automate cloud security controls and integrate them into CI/CD pipelines.
- Provide security guidance for cloud migration and modernization projects.

Product Security Champion

An engineer embedded within a development team to integrate security into DevSecOps practices. Key duties:

- Advocate for secure software development lifecycle (SSDLC) principles within their team.
- Conduct code reviews, threat modeling, and security testing.
- Liaise between development teams and security leadership to address security findings.
- Promote security automation and tooling within development workflows.
- Maintain awareness of emerging application security threats and mitigations.

Security Controller

Supports line managers in managing physical and remote work security. Key duties:

- Receive and escalate immediate reports of lost or stolen equipment.
- Support enforcement of physical and logical security requirements for remote staff.
- Ensure compliance with organization-approved secure workspace practices.
- Coordinate with facilities, IT, and HR to address physical security concerns.

- Maintain records of security incidents affecting physical assets.

National CERT/CSIRT

The primary national coordination center for cybersecurity incident management, operating under the Ministry of ICT and National Guidance. Key responsibilities:

- Serve as the authoritative source for national threat intelligence.
- Disseminate advisories and vulnerability alerts to MDAs and critical infrastructure operators.
- Support coordinated response to large-scale or cross-sector incidents.
- Provide incident analysis, forensic assistance, and post-incident reporting.
- Maintain secure information-sharing channels between public and private sector stakeholders.

5.1.3.8 Responsibilities of Project and Operational Roles

Line Manager

Responsible for managing the day-to-day implementation of security policies within their teams and ensuring compliance with organizational and legal requirements.

Key responsibilities:

- Identify and manage observable, work-related behaviors of security concern while respecting employee privacy under the Data Protection and Privacy Act (DPPA).
- Ensure team adherence to physical and information security requirements in both on-site and remote work environments.

- Facilitate timely reporting of security incidents and coordinate initial response actions.
- Support awareness and training programs by reinforcing security expectations within teams.
- Maintain oversight of asset allocation, usage, and retrieval.

System Owner

Accountable for the security and lifecycle management of assigned systems.

Key responsibilities:

- Ensure systems are designed, implemented, and operated in compliance with the ISMS and applicable regulations.
- Maintain up-to-date risk assessments and security documentation for assigned systems.
- Coordinate with technical teams to implement and maintain appropriate controls.
- Approve changes, upgrades, or decommissioning activities after security review.
- Ensure security controls remain effective throughout the system's operational life.

Cloud Service Provider (CSP)

Recognized as a critical external partner in the shared responsibility model for cloud security.

Key responsibilities:

- Maintain the physical and environmental security of their data centers.
- Provide system and audit logs, as well as technical support, to the

contracting MDA during security incidents.

- Ensure contractual compliance with security, privacy, and availability requirements.
- Implement security measures in line with industry standards and agreed SLAs.
- Participate in security reviews, audits, and incident post-mortems.

5.1.4 Risk Management

Organizations must operate a continuous, lifecycle-based risk management process covering:

- Design Phase – Secure design reviews & threat modeling.
- Implementation – Risk assessments before system go-live.
- Operations – Continuous monitoring & reassessment.
- Decommissioning – Secure disposal & media sanitization (per NIST SP 800-88).

Each organization must maintain a Risk Register documenting identified risks, owners, treatment decisions, residual risks, and approvals.

Below is the Information Security Risk Management Lifecycle showing the critical stages every system must go through:



Figure 3 - Information Security Risk Management Lifecycle.

5.1.5 Awareness, Education, and Training

The purpose of awareness, education and training is to foster an organizational culture that values, protects and handles information assets safely and thereby achieves the mandatory minimum-security outcomes. Organizations must:

- Provide induction training before system access is granted.
- Maintain role-specific awareness programs for all staff.
- Conduct annual refreshers and simulate attacks (e.g., phishing tests).
- Measure training effectiveness through assessments and metrics.

5.1.6 Business Continuity and Disaster Recovery

Business continuity activities aim to show that the organization has the capacity to withstand interruptions to critical business activities and thereby achieve the mandatory minimum-security outcomes. Organizations must integrate information security into Business Continuity Management (BCM) and Disaster Recovery (DR) planning.

As a minimum requirement, organizations must:

- Maintain BCP & DRP covering all critical functions.
- Test plans at least annually and after significant changes.
- Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Integrate cyber resilience measures (redundancy, failover, backups).

5.1.7 Incident Management

Incident management aims to demonstrate that the organization is reducing the likelihood and impact of security incidents and ensuring the quick resumption of business activities in line with the mandatory minimum-security outcomes.

Organizations must implement formal Incident Response Frameworks to:

- Implement a formal Incident Response Framework with defined playbooks.

- Report serious incidents to national authorities (CERT-UG, PDPO).
- Conduct post-incident reviews and update controls accordingly

5.1.8 Assurance and Compliance

Assurance and compliance reporting aims to demonstrate that the organization is achieving the mandatory minimum-security outcomes. Organizations must demonstrate reasonable assurance that security policies are implemented effectively through:

- Perform quarterly risk performance reviews.
- Conduct annual internal and external security audits.
- Track corrective actions and disclose material non-compliance to oversight bodies.

5.2 Information Security

5.2.1 Introduction

Information and the supporting processes, systems and networks that process, store, retrieve, and transmit it, play a vital role in the conduct and success of GoU and private sector operations. Therefore, organizations must protect the information they handle internally and that they share with external partners. Assuring the confidentiality, integrity and availability of information is necessarily a corporate-level concern because security incidents threaten organizational reputations, legal positions and the ability to conduct business operations.

Protecting information from unauthorized access, modification, disclosure, destruction, or disruption is essential to:

- Safeguarding national security and economic stability.
- Preserving public trust and confidence.
- Ensuring business continuity and resilience.
- Maintaining compliance with laws and contractual obligations.

A breach of information security can damage organizational reputation, disrupt operations, and expose sensitive data to unauthorized access or misuse.

5.2.2 Information Security Policy

An information security policy helps improve security if published, enforced, audited and updated to reflect organizational requirements. Organizations must develop a formal Information Security Policy that:

- Is approved by the Board or equivalent authority.
- Clearly defines scope, purpose, objectives, and applicability.
- Specifies baseline and risk-based controls aligned with ISO/IEC 27001:2022.
- Addresses asset management, classification, access control, incident management, and business continuity.
- It is reviewed annually or following significant changes in risk.
- Is communicated to all staff, contractors, and third parties with access to organizational information.

5.2.3 Asset Management

Organizations must achieve and maintain appropriate protection for information assets in compliance with best practices. Effective asset management helps achieve the mandated NISF minimum security outcomes. Organizations must:

- Maintain an up-to-date asset inventory for both information and supporting systems.
- Assign asset ownership and accountability for each asset.
- Classify assets according to sensitivity and business impact
- Apply security controls proportionate to classification.
- Conduct regular asset audits and verification against records.
- Ensure decommissioning processes securely remove or destroy sensitive data.

5.2.4 Emerging Technology Security

In response to evolving digital trends and risks, organizations must adopt proactive security measures for emerging technologies that are increasingly integrated into government and critical sector operations. These include Cloud Computing, Application Programming Interfaces (APIs), Artificial Intelligence (AI), and Operational Technology/Industrial Control Systems (OT/ICS). Controls must ensure these technologies are deployed, managed, and monitored in compliance with applicable legislation, ISO/IEC 27001:2022, and other relevant standards.

5.2.4.1 Cloud Computing

Organizations must:

- Ensure Cloud Service Providers (CSPs) comply with recognized standards (e.g., ISO/IEC 27017, ISO/IEC 27018, CSA Cloud Controls Matrix).
- Define data sovereignty, encryption requirements (in transit and at rest), and the shared responsibility model in all contracts and Service Level Agreements (SLAs).
- Conduct joint risk assessments between the Information Risk Owner (IRO) and Data Protection Officer (DPO) prior to cloud adoption.
- Require cloud providers to implement Multi-Factor Authentication (MFA), robust access controls, and continuous security monitoring.
- Ensure secure data deletion and service decommissioning with verifiable cryptographic erasure.
- Review and approve third-party audit reports (e.g., SOC 2, ISO certifications) annually.

Specialized Role – Cloud Security Engineer (Minimum Requirements):

- Certification: CCSP, ISO/IEC 27017/27018 familiarity.
- Functions: Cloud workload hardening, CSP compliance validation, incident response integration.

- Evidence for Audit: Appointment letter, training certificates, cloud configuration review reports, CSP audit reviews.

5.2.4.2 Application Programming Interfaces (APIs)

Organizations must:

- Secure all APIs with strong authentication (e.g., OAuth 2.0), TLS encryption, and least privilege access controls.
- Maintain a comprehensive inventory of API endpoints and enforce change/version control for all integrations.
- Conduct regular API security testing aligned with the OWASP API Security Top 10.
- Deploy API gateways with anomaly detection, rate limiting, and abuse prevention mechanisms.
- Log and monitor all API traffic, retaining logs securely for forensic purposes.
- Disable and revoke credentials for deprecated or unused APIs immediately.

Specialized Role – Product Security Champion (Minimum Requirements):

- Certification: OWASP/API security training, DevSecOps practices.
- Functions: Secure coding reviews, API threat modelling, enforcement of SSDLC controls.
- Evidence for Audit: Code review logs, security test reports, API inventory register.

5.2.4.3 Artificial Intelligence (AI)

Organizations must:

- Conduct initial and ongoing risk assessments for AI systems, addressing privacy, bias, fairness, and explainability.
- In addition, perform regular assessments or audits of AI systems to detect emerging ethical risks (e.g., bias, discrimination, unfair outcomes) and take corrective action, especially for high-impact or automated decision-making use cases.
- Ensure all AI processing of personal data complies with the Data Protection and Privacy Act, 2019 and conduct Data Protection Impact Assessments (DPIAs) where required.
- Protect AI models and training datasets from poisoning attacks, data leakage, and unauthorized model inference.
- Implement adversarial testing and continuous model performance monitoring.
- Ensure AI decisions, especially those with high impact on individuals or national security, are auditable and transparent.
- Maintain human oversight for AI-driven critical decision-making processes.

Specialized Role – AI Security/Controller (Minimum Requirements):

- Certification: ISO/IEC 23894 (AI RMF), AI ethics/privacy training.
- Functions: Conduct AI risk assessments, implement adversarial testing, ensure explainability and oversight.
- Evidence for Audit: Completed DPIAs, adversarial test logs, AI model governance records.

5.2.4.4 Operational Technology / Industrial Control Systems (OT/ICS)

Organizations must:

- Isolate OT/ICS environments from corporate IT networks using network segmentation or physical air-gapping.
- Apply ISA/IEC 62443 and NIST SP 800-82 guidelines for securing industrial systems.
- Implement continuous monitoring for anomalies, including correlation with SCADA system logs.
- Harden and patch OT systems where possible; where patching is not feasible, apply compensating controls.
- Control and monitor all physical and logical access to OT facilities and systems.
- Include OT-specific scenarios in incident response and disaster recovery plans, prioritizing safety and operational continuity.

Specialized Role – OT/ICS Security Controller (Minimum Requirements):

- Certification: ISA/IEC 62443, NIST SP 800-82 knowledge.
- Functions: OT segmentation, SCADA log monitoring, safety-first incident playbooks.
- Evidence for Audit: SCADA monitoring reports, segmentation diagrams, OT incident drill records.

5.2.5 Secure Information Sharing

Secure information sharing must ensure that partners meet or exceed the mandated NISF minimum security outcomes.

Organizations must:

- Define purpose, format, and security requirements in formal agreements.
- Use encryption and secure transfer protocols.
- Verify partner compliance through periodic reviews.
- Revoke access immediately in case of a breach or contract termination.

5.2.6 Supply Chain Security

All organizations increasingly source ICT systems and software from a global network of suppliers, distributors and business partners. The advantages of a global ICT supply chain include competitive prices, innovative products and flexibility. Regrettably, there is clear evidence that global ICT supply chains have heightened system and software risks. Organizations must:

- Define the purpose, format, and security requirements in formal agreements with suppliers and partners.
- Conduct security due diligence before onboarding suppliers, including background checks and technical security assessments.
- Include security requirements in contracts and SLAs, such as patching timelines, vulnerability disclosure obligations, and breach notification requirements.
- Require suppliers to provide a Software Bill of Materials (SBOM) listing all software components, versions, and dependencies used, to support supply chain transparency, compliance, and risk management, and to enable effective vulnerability management and incident response.
- Specify ownership and escrow arrangements for source code to protect government interests in case of vendor exit or supply chain disruption.
- Require disclosure of programming languages, frameworks, and versions used, ensuring they are supported and free from known critical vulnerabilities.
- Continuously monitor supplier compliance and performance using audits, third-party attestations (e.g., ISO/IEC 27001, SOC 2), and automated risk monitoring tools.

- Enforce contractual consequences for non-compliance, including penalties, contract termination, or mandatory remediation.
- Align procurement processes with NIST SP 800-161r1 supply chain security practices and other recognized international standards.

5.2.7 Access Management

Access management focuses on how to control who gains access to critical infrastructure. At its simplest, access management or control aims to ensure that only business and security requirements determine who accesses information, information processing facilities and business processes. Consequently, access control aims to achieve the minimum-security outcomes. Access must be:

- Grant access on a Need-to-Know and Least Privilege basis
- Apply Multi-Factor Authentication (MFA) for sensitive systems
- Review access rights quarterly or after role changes
- Maintain comprehensive access logs and enable real-time monitoring

5.2.8 Network Security Controls

Proportionate risk-based technical security controls can help achieve the mandated NISF minimum-security outcomes. Therefore, organizations must:

- Segment networks according to business sensitivity
- Deploy firewalls, IDS/IPS, and encryption for data in transit

- Harden network devices and disable unused services
- Continuously monitor network traffic for anomalies
- Establish redundancy and resilience measures

5.2.9 Malicious Code Protection

Malicious code, including viruses, worms, spyware, and Trojans, remains a major threat vector used by attackers to gain unauthorized access or disrupt systems. Threat actors often leverage email attachments, compromised websites, instant messaging, and social media to deliver malicious payloads. These threats exploit vulnerabilities in systems and applications.

Organizations must:

- Use centrally managed anti-malware solutions with real-time protection
- Keep definitions updated automatically
- Restrict unauthorized installations through application whitelisting
- Provide ongoing security awareness training
- Patch and update systems promptly

These controls help reduce the likelihood and impact of malicious code incidents as part of a layered defense strategy.

5.2.10 Portable and Removable Media Security

Portable and removable media devices increase workplace productivity by enabling access to corporate network resources anytime, anywhere. Therefore, the devices are a popular way of gaining access to corporate network resources. Apart from devices that organizations supply, IT departments face pressures to accept the trend of bring your own device (BYOD) where staff seek to use personally owned devices at work.

Portable and removable media like USB drives and CDs can introduce malware or lead to data leakage if lost or misused. Organizations must implement controls to manage and secure their use.

Organizations must:

- Restrict or control use of USB drives, CDs, and external storage
- Encrypt sensitive data on portable devices
- Scan all removable media before use
- Apply BYOD policies with security controls for personal devices

5.2.11 Remote Access Security

Remotely connecting a computer either to another computer or to a network over public networks such as the Internet increases staff flexibility and productivity. Staff with remote access can perform general work activities, access e-mail and transfer files.

However, remote working can increase exposure to cyber threats. To protect systems accessed remotely, organizations must apply layered controls consistent with ISO/IEC 27001:2022.

Remote access increases exposure to threats; organizations must:

- Authorize remote connections based on business need
- Use VPNs with strong encryption
- Enforce MFA for all remote logins
- Log and monitor all remote sessions
- Follow Zero Trust access principles

5.2.12 Protective Monitoring

Protective monitoring helps organizations detect, investigate, and respond to suspicious activities. It supports compliance and provides evidence in case of incidents.

Organizations should take a risk-based approach to selecting the level of protective monitoring undertaken. Thus, the level of protective monitoring should match business requirements, exposure to threats and risks and the business impact of security breaches.

Security monitoring must be continuous and proactive:

- Log all critical system and user activities
- Monitor for anomalies and unauthorized activities
- Protect logs from tampering
- Retain logs per regulatory requirements and use them for investigations

5.2.13 Information Back-Ups

Reliable backups are essential to recover data after incidents such as ransomware or system failures. Controls must reflect data criticality and retention needs.

Therefore, reliable backups must:

- Be scheduled based on data criticality.
- Store encrypted copies onsite and offsite (geographically separate).
- Have restore processes tested regularly.
- Meet legal and business retention requirements.

5.2.14 Security Accreditation

Security accreditation provides formal assurance that systems meet required security standards before use. Organizations demonstrate compliance with security requirements by maintaining documented evidence such as procedures, processes, guidelines and security plans that support the protection of information systems. It ensures systems are tested, documented, and approved based on risk.

Security accreditation is required before systems go live:

- Conduct risk assessments and penetration testing
- Verify control effectiveness through audits
- Document residual risks and obtain management approval
- Re-accredit systems after major changes or annually

5.3 Personnel Security

5.3.1 Introduction

Employees are the most valuable asset in any organization but can also present significant security risks. Insider threats, whether intentional or accidental, result in the disclosure, destruction, manipulation, or loss of sensitive data and critical services.

High-profile incidents globally have shown that insider compromises can cause as much, if not more, damage than external attacks. This underscores the need for proactive, proportional, and continuous personnel security measures to ensure that only suitable, trustworthy, and reliable individuals are granted access to sensitive data, systems, and facilities.

Personnel security is not a one-time vetting activity; it is an ongoing process integrated into the organization's risk management and governance framework. This approach aligns with ISO/IEC 27001:2022 and national legislation by embedding security awareness, vetting, and behavioral monitoring into every stage of employment, from recruitment to post-exit.

Key Objectives:

- Reduce the likelihood of misuse of access to critical infrastructure.
- Ensure personnel suitability before, during, and after employment.
- Detect and respond to indicators of insider threats promptly.



Figure 4 – Security Clearance Levels.

This approach aligns with ISO/IEC 27001:2022 by integrating personnel security into broader risk management, ensuring security measures are appropriate and regularly reviewed.

5.3.2 Security Roles and Responsibilities

National legislation such as the Official Secrets Act (1964), Computer Misuse Act (2011), Data Protection and Privacy Act (DPPA, 2019), and related regulations require that employees, contractors, and third parties understand their security obligations.

Organizations must:

- Define security responsibilities clearly in job descriptions, contracts, and SLAs.
- Require signed confidentiality agreements prior to access.
- Communicate these responsibilities during onboarding and periodic refresher training.
- Apply progressive disciplinary measures for violations, up to and including termination or legal prosecution.
- Ensure managers are trained to identify and escalate personnel security concerns.

5.3.3 Baseline Security Clearance

Baseline Security (BS) clearance provides reasonable assurance that individuals seeking access to critical infrastructure are reliable. Therefore, all candidates seeking employment or contracts in role requiring access to critical infrastructure must undergo and pass BS vetting checks. The level of checks undertaken would depend on business requirements, perceived risks and the value, sensitivity and criticality of the information assets. The bottom line is that BS vetting checks apply to all users of critical infrastructure

Baseline Security Clearance (BS) helps confirm the suitability of staff handling information classified up to RESTRICTED, reducing insider threat risks.

BS Clearance must include:

- Verified identity and right to work checks.
- Employment and education history verification (minimum past 3–5 years).
- Character and professional references.
- Criminal record checks in line with local laws.
- Financial integrity checks for roles with fraud or procurement authority.
- Digital footprint screening where legally permissible, to detect risk indicators.

5.3.4 National Security Vetting

Security clearance is a status granted to individuals that allows them to access certain information. Higher clearance levels ensure that personnel with frequent or high-level access to sensitive or classified information are thoroughly vetted.

The national security vetting process involves tougher checks than BS vetting using two clearance levels as follows:

SECRET Clearance:

- Required for frequent or uncontrolled access to SECRET-classified information.
- Includes BS checks plus enhanced background investigation

TOP SECRET Clearance:

- Required for access to highly sensitive national security information.
- Includes lifestyle interviews, financial audits, social media reviews (where lawful), and in-depth background investigations involving security agencies.

Clearance decisions must be recorded and reviewed periodically in coordination with authorized national security bodies.

5.3.5 Ongoing Personnel Security Management

Personnel security risks can evolve due to changes in personal circumstances, financial hardship, behavioral issues, or ideological shifts. Continuous monitoring is essential to maintain trust and security integrity.

Organizations must:

- Revalidate clearance levels periodically (e.g., every 3–5 years, or earlier for high-risk roles).
- Monitor for insider threat indicators, including unusual system activity, policy violations, or unexplained financial changes.
- Maintain whistleblowing and anonymous reporting mechanisms.
- Require personnel to declare relevant changes in personal or professional circumstances.
- Apply mitigation measures immediately when a risk is identified.

- Ensure rapid access revocation upon termination, resignation, or role reassignment.

5.3.6 Exit Management.

The risk of information leakage or misuse can persist even after an individual leaves an organization. Effective exit management ensures that all access privileges are revoked, assets are recovered, and legal obligations regarding confidentiality are reinforced to prevent post-employment security incidents.

Organizations must:

- Conduct formal exit interviews to reinforce ongoing confidentiality obligations and remind individuals of non-disclosure requirements.
- Retrieve all organization-issued assets, including ID cards, access keys, mobile devices, laptops, and any removable media.
- Terminate all system accounts and physical access privileges immediately upon exit.
- Document and confirm the return of all sensitive documents or storage devices.
- Monitor for any post-exit attempts to access organizational systems or data and escalate incidents if detected.

5.3.7 Security Awareness and Culture.

A strong security culture empowers personnel to act as the first line of defense against insider threats and external attacks. Continuous awareness initiatives and proactive engagement foster an environment where protecting information assets becomes an ingrained habit rather than a compliance requirement.

Organizations must:

- Provide tailored, role-specific security training, including insider threat awareness and prevention strategies.
- Incorporate behavioral security awareness and compliance with security protocols into performance reviews.
- Encourage the reporting of suspicious behavior through clear, confidential, and non-punitive channels.
- Promote regular security drills, campaigns, and communications to keep awareness high.
- Recognize and reward staff who demonstrate exemplary security-conscious behavior.

5.4 Physical Security

5.4.1 Introduction

Physical security is a critical component of the Information Security Management System (ISMS), protecting personnel, information assets, and critical infrastructure against threats such as unauthorized access, theft, espionage, sabotage, terrorism, and environmental hazards.

The key components include as illustrated below;

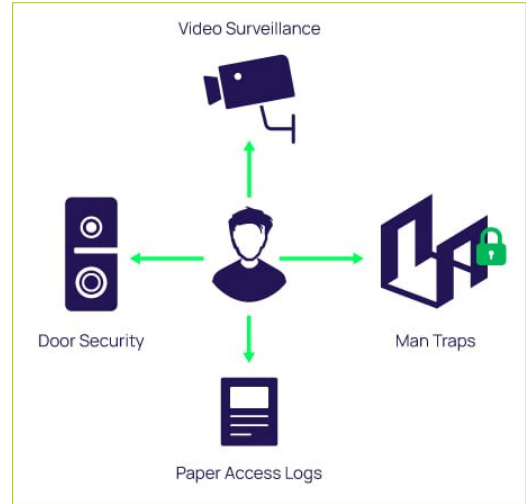


Figure 5 – Key Components of a Security System

Effective physical security follows a layered defense approach where multiple barriers and controls reduce the likelihood and impact of incidents. These measures must be risk-based, integrated with personnel and information security controls, and regularly reviewed under the Plan-Do-Check-Act (PDCA) model for continuous improvement.

5.4.2 Physical Security Perimeter

This policy requires organizations to put in place an adequate physical perimeter around sensitive information processing facilities to stop unauthorized physical access. The physical security perimeter is the first layer of a 'defense-in-depth' approach to security that progressively increases the difficulty of security controls the closer one gets to areas containing sensitive information assets.

Organizations must:

- Define security zones based on asset criticality and documented risk assessments.
- Install robust physical barriers (fences, walls, reinforced doors, shatter-resistant windows).
- Deploy detection and deterrence technologies (motion sensors, CCTV, intrusion alarms).
- Control and monitor all access points with authorized personnel only.
- Include perimeter resilience measures against environmental hazards (floods, fire, earthquakes).
- Maintain clear signage indicating restricted areas.
- Periodically review and update perimeter controls to address evolving threats.

These measures must be supported by documented procedures and periodic reviews to adapt to evolving threats.

5.4.3 Entry Controls

Access to secure areas must be authorized, controlled, and monitored. In line with the risk management/ proportionality principle, the physical entry controls in place must be appropriate with business and security requirements.

Requirements include:

- Use of access control mechanisms (e.g., proximity card readers, biometrics, scanners).
- Visitor management procedures (badges, escorts, sign-in/sign-out procedures).

- Anti-tailgating and anti-piggy backing technologies measures.
- Maintain and review access logs to detect anomalies and support investigations.
- Apply the principle of least privilege for access rights and review them periodically.

5.4.4 Internal Data Centre Physical Access Controls

Internal areas of information processing facilities require additional physical security controls because this is where sensitive information is processed or stored. The internal areas include the data centers, communication and switching centers and end-user areas.

Data centers and server rooms house critical systems and data, requiring enhanced security controls.

Organizations must:

- Segregate sensitive areas and apply stricter access controls
- Use dual-factor or multi-factor authentication for authorized entry.
- Reinforce structures to resist forced entry (e.g., secure walls, reinforced doors).
- Enable 24/7 CCTV surveillance and alarm monitoring.
- Prohibit personal or unauthorized devices in secure zones.
- Control and log the movement of IT equipment and media.
- Conduct regular physical security audits of these areas.

5.4.5 Equipment Protection

Organizations must protect equipment (e.g., electrical supply and cabling infrastructure) and supporting assets from physical threats. The security measures help reduce the risk of unauthorized access to information and loss or damage of equipment.

Organizations must:

- Securely mount and lock critical IT and networking equipment.
- Use tamper-evident seals and secure racks/cabinets
- Conceal and protect network and power cabling against interference or tampering.
- Apply security features (e.g., encryption, device tracking) on portable devices.
- Maintain environmental controls and resilience measures, such as uninterruptible power supplies (UPS), backup generators, and climate monitoring.
- Conduct periodic inspections to ensure ongoing resilience.

5.4.6 Secure Equipment Disposal and Re-Use

Organizations must have in place measures to manage the security risks associated with the disposal and re-use of computer storage media holding sensitive information. The measures must cover the sanitization and disposal of storage assets into secure and less secure environments for repair, exchange and recycling.

When decommissioning IT equipment or storage media organizations must.

- Erase or physically destroy all sensitive data before disposal.
- Document asset disposal in a formal asset management process.
- Use approved disposal vendors with documented security standards.
- Sanitize reassigned equipment before redeployment.
- Align disposal processes with data retention and destruction policies.

5.4.7 Physical Security Monitoring & Response.

Continuous monitoring and a rapid response capability ensure physical security controls remain effective against emerging threats.

Organizations must:

- Implement real-time monitoring of security systems (CCTV, alarms, sensors) from a centralized Security Operations Centre (SOC) or control room.
- Establish on-site or remote guard presence for critical facilities 24/7.
- Integrate physical security alerts with the organization's Incident Response Framework.
- Test alarm and monitoring systems regularly to confirm operational readiness.
- Conduct unannounced penetration testing (red teaming) to evaluate perimeter and entry control effectiveness.

5.4.8 Physical Security Policy Reviews

Regular policy reviews ensure physical security remains aligned with evolving threats, legislation, and organizational needs.

Organizations must:

- Review physical security policies at least annually or following a major security incident.
- Update controls in response to new threat intelligence, risk assessment results, or changes in building layout/operations.
- Involve cross-functional teams (security, IT, HR, facilities, legal) in review processes.
- Document changes and communicate updates to all relevant staff and contractors.
- Benchmark controls against international best practices such as ISO/IEC 27002:2022 and BSI IT-Grund Schutz.



Appendix A – Accompanying Documents

The following documents accompany the National Information Security Policy (NISP) and collectively constitute the **National Information Security Framework (NISF)**.

These supporting documents establish detailed requirements, methodologies, guidance, and assurance mechanisms to enable **consistent implementation, effective operation, continuous monitoring, and continual improvement** of information security governance across Uganda.

All documents have been developed in alignment with international standards (ISO/IEC 27001/27002:2022, NIST CSF, CIS Controls), regional conventions (African Union Malabo Convention, East African Cybersecurity Framework), and Uganda's national legislation (Data Protection and Privacy Act, 2019; e-Government Strategy).

Document Title | Purpose

1. NISF Implementation Manual

Provides step-by-step guidance for MDAs, LGs, and CI Operators on implementing NISF Security Standards (SS1–SS7), sectoral modules (AI, Cloud, API, OT, CII), and Uganda-specific requirements.

2. MDA Compliance Toolkit

- Compliance Checklist (Y/N/NA/P implementation status)
- Corrective Action Plan (CAP) Tracker
- Compliance Dashboard (auto-calculated)
- Maturity Dashboard (Foundational–Advanced scoring)
- Insider Threat Register + Dashboard
- Incident KPI Dashboard
Enables MDAs to self-assess, track, and report compliance to NITA-U.

3. NISF Risk Management Manual

Provides methodologies for risk identification, assessment, and treatment in line with SS1 & SS2. Includes risk appetite statements, templates, and sector-specific guidance.

4. NISF Audit Test Plan Workbook

Practical toolkit for NITA-U assessors and auditors to validate compliance across MDAs/CI Operators. Includes audit test procedures, evidence collection methods, conformity/non-conformity reporting, and stage-based audit templates.

5. Baseline Control Catalogue

Master catalogue of all NISF SS1–SS7 controls. Mapped against ISO/IEC 27002:2022, NIST CSF, CIS, and Uganda's Data Protection and Privacy Act. Forms the authoritative reference for compliance, assessment, and audit.

6. Corrective Action Plan (CAP) Framework

Establishes standard processes for identifying gaps, documenting remediation actions, assigning responsibility, tracking deadlines, and reporting closure.

7. Implementation Guidance Notes

Control-by-control notes explaining implementation expectations, required evidence, and sector examples. Serves as a bridge between the checklist and practical execution.

Important Note

- These supporting documents are **mandatory references** for the implementation of the NISP.
- MDAs, LGs, and CI Operators must consult and apply them in conjunction with the NISP to ensure full compliance with the National Information Security Framework (NISF).
- All documents will be **reviewed and updated periodically** to reflect emerging threats, regulatory changes, international benchmarking, and lessons learned from practical implementation.



Appendix B - Definitions of Terms.

- **Application Programming Interface (API):** A set of rules and protocols that allows different software systems to communicate and share data securely.
- **Artificial Intelligence (AI):** Computer systems designed to perform tasks that normally require human intelligence, such as decision-making, speech recognition, and predictive analytics.
- **AI-Enabled Attack:** Cyberattacks leveraging artificial intelligence to automate phishing, create deepfakes, or evade detection.
- **Business Email Compromise (BEC):** A fraud scheme exploiting email to impersonate executives, vendors, or staff to divert funds or extract sensitive data.
- **Baseline Security (BS):** The minimum set of controls required to ensure the security of systems or individuals before granting access to sensitive information or facilities.
- **CAP (Corrective Action Plan):** A structured record of remediation actions required to address gaps identified in the MDA Compliance Checklist. Tracked via the CAP Register and CAP Dashboard.
- **CERT-UG (Uganda National Computer Emergency Response Team):** Uganda's national CSIRT operated under NITA-U. CERT-UG provides incident coordination, vulnerability advisories, threat intelligence, and national-level response support. It also serves as Uganda's point of contact for regional and international cyber cooperation.
- **Cloud Technologies:** Computing services (including storage, processing, and networking) delivered over the internet, provided in models such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).
- **Compliance Dashboard:** An automated dashboard that calculates overall and standard-specific compliance levels based on the MDA Compliance Checklist.
- **CSIRT (Computer Security Incident Response Team):** An organisational or national team responsible for coordinating incident detection, response, and recovery. In Uganda, CERT-UG functions as the national CSIRT.
- **Critical Information Infrastructure (CII):** ICT systems managing sectors like health, energy, finance, and government, vital to national stability.

➤ **Critical Infrastructure (CI):**

Systems whose disruption would severely impact public health, safety, or national security. Includes physical and virtual assets.

➤ **Data Breach**

A confirmed incident where sensitive, confidential, or protected information has been accessed, disclosed, or destroyed without authorisation.

➤ **DPPA (Data Protection and Privacy Act, 2019):** Uganda's primary legal framework for data protection, mandating lawful processing, breach notification, and data-subject rights.

➤ **Defense-in-Depth:** A layered approach to security that applies multiple protective measures across physical, technical, and procedural controls.

➤ **Incident Register:** A structured log of all incidents, recording ID, category, severity, dates, containment, root cause, and status. Supports dashboard auto-calculation of KPIs.

➤ **Incident Response Playbook:** A structured, pre-approved set of steps and procedures for responding to specific types of security incidents.

➤ **Industrial Control Systems (ICS):** Integrated hardware and software designed to control and monitor industrial processes, often forming part of OT environments. Includes Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS).

➤ **Information Risk Owner (IRO):**

A senior role accountable for the identification, assessment, and treatment of risks related to specific information assets.

➤ **Insider Threat:** A security risk posed by current or former employees, contractors, or partners who misuse their access. May be malicious (espionage, theft) or negligent (weak password practices).

➤ **Insider Threat Register:** An MDA tool for recording, categorising, and tracking insider-related events, linked to the Insider Threat Dashboard.

➤ **KPI (Key Performance Indicator):** Metrics used to assess effectiveness of security functions. In NISP, incident KPIs include Mean Time to Detect (MTTD), Mean Time to Contain (MTTC), and Closure Rates.

➤ **MDA Compliance Checklist:** The self-assessment tool for MDAs, LGs, and CI Operators to record implementation of NISP controls (SS1–SS7), supported by dashboards.

➤ **Maturity Dashboard:** An automated tool that calculates maturity trends across control levels (Foundational, Enhanced, Advanced).

➤ **MTTD (Mean Time to Detect):** The average time between the occurrence of an incident and its detection.

➤ **MTTC (Mean Time to Contain):** The average time between the detection of an incident and its containment.

- **Official Communications:**
Information generated or processed by MDALs during official operations, with lower sensitivity than protected computers but still requiring confidentiality.
- **Operational Technology (OT):**
Hardware and software systems used to monitor, control, and automate industrial processes, such as manufacturing, energy distribution, and critical infrastructure operations.
- **PDCA (Plan-Do-Check-Act):** A continual improvement model used for implementing and managing information security management systems.
- **RaaS (Ransomware-as-a-Service):** Commercialisation of ransomware tools that enable even low-skilled attackers to launch disruptive attacks.
- **Penetration Testing (Pentest):** An authorized, simulated cyberattack on a system to evaluate its security posture and identify exploitable weaknesses.
- **Personal Data:** Data that relates to an identifiable individual, whose unauthorized use can lead to legal or reputational consequences.
- **Residual Risk:** The remaining risk after controls have been implemented, documented in the Compliance Checklist and CAP Register.
- **Risk Appetite:** The amount and type of risk an organisation is willing to pursue or retain in order to achieve its objectives.
- **Risk Tolerance:** The acceptable variation in outcomes related to achieving objectives, often expressed as thresholds or limits.
- **Plan-Do-Check-Act (PDCA) Cycle:** A continuous improvement framework for implementing, monitoring, and refining security measures.
- **Protected Computers:** Computers directly involved in national security, defense, diplomacy, law enforcement, and critical public services.
- **Red Teaming:** Simulated adversarial attacks designed to test the effectiveness of an organization's security defenses and response capabilities.
- **SCADA (Supervisory Control and Data Acquisition):** A type of OT/ICS system used to control industrial processes such as energy generation, water treatment, and transportation.
- **Security Coordination Group (SCG):** A cross-functional team responsible for coordinating information security governance across departments, including IT, HR, legal, and operations.
- **Security Operations Centre (SOC):** A centralized facility for monitoring, detecting, analyzing, and responding to security events in real time.
- **Security Risk Appetite:** The amount and type of information risk an organization is willing to accept in pursuit of its goals.

➤ **Security Risk Appetite:** The level and type of information risk an organization is willing to accept in pursuit of its objectives.

➤ **SoA (Statement of Applicability):** A declaration of applicable NISP controls, their implementation status, and justification for exclusions. Supports audit and verification.

➤ **SOC (Security Operations Centre):** A dedicated facility or function for monitoring, detecting, analysing, and responding to security incidents in real time.

➤ **SS1-SS7 (NISF Security Standards):** The seven security standards under the National Information Security Framework:

- ~ **SS1** – Technical Risk Assessment
- ~ **SS2** – Risk Management & Accreditation
- ~ **SS3** – Security Classification

~ **SS4** – Personnel Security

~ **SS5** – Physical Security

~ **SS6** – Incident Management

~ **SS7** – Data Privacy & Protection

➤ **Supply-Chain Risk**

The risk of compromise introduced by third-party vendors, service providers, or outsourced systems.

➤ **TOP SECRET:** The highest security clearance level required for accessing extremely sensitive national information.

➤ **Vulnerability Assessment:** A systematic process for identifying, quantifying, and prioritizing security weaknesses in systems, networks, and applications.

➤ **Zero Trust Security Model:** A security framework that assumes no implicit trust for any user or device, requiring continuous verification regardless of location or network.



Appendix C - RACI Matrix – Specialized Roles for Emerging Technology Security

Specialized Role	Minimum Baseline Competency	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)	Required Evidence
Cloud Security Engineer	CCSP, ISO/IEC 27017/27018 knowledge, cloud hardening & CSP compliance	Configure & monitor cloud workloads	Information Risk Owner (IRO)	CSP, IT Ops, DPO	Board, Auditors	Appointment letter, CCSP cert, CSP audit reviews, cloud config reports
Product Security Champion (API/ DevSecOps)	Secure coding, OWASP Top 10/API, SSDLC practices	Perform secure code/ API reviews	CIO / Head of IT	Developers, QA teams	IRO, Auditors	Training certificate, code review logs, API inventory, test reports
AI Security/ Controller	AI RMF (ISO/IEC 23894), DPPA compliance, adversarial testing	Conduct AI risk assessments & DPIAs	DPO	IRO, Data Scientists	Board, Auditors	DPIAs, AI governance policy, adversarial test logs
OT/ICS Security Controller	ISA/IEC 62443, NIST 800-82 OT security, SCADA monitoring	Implement OT segmentation & monitoring	Head of Operations / IRO	Facilities, Vendors	Board, Auditors	SCADA log reviews, segmentation diagrams, OT incident drill records
National CERT/ CSIRT Liaison	National/sectoral CSIRT training, incident coordination	Coordinate incident reporting & threat intel sharing	IRO / CISO	CERT-UG, Sector Regulators	Board, PDPO	Incident reports, CERT advisories, drill participation records



Serianu Limited

Kenya Office:
14 Chalbi Drive, Lavington, Nairobi, Kenya



info@serianu.com



@serianultd



Serianu Limited



Africa Cyber Immersion Centre - ACIC



@africacyberimmersioncentre

www.serianu.com

Prepared by **Serianu Limited**



S E R I A N U

NOC
NETWORKS - AUTOMATION - COMMUNICATION