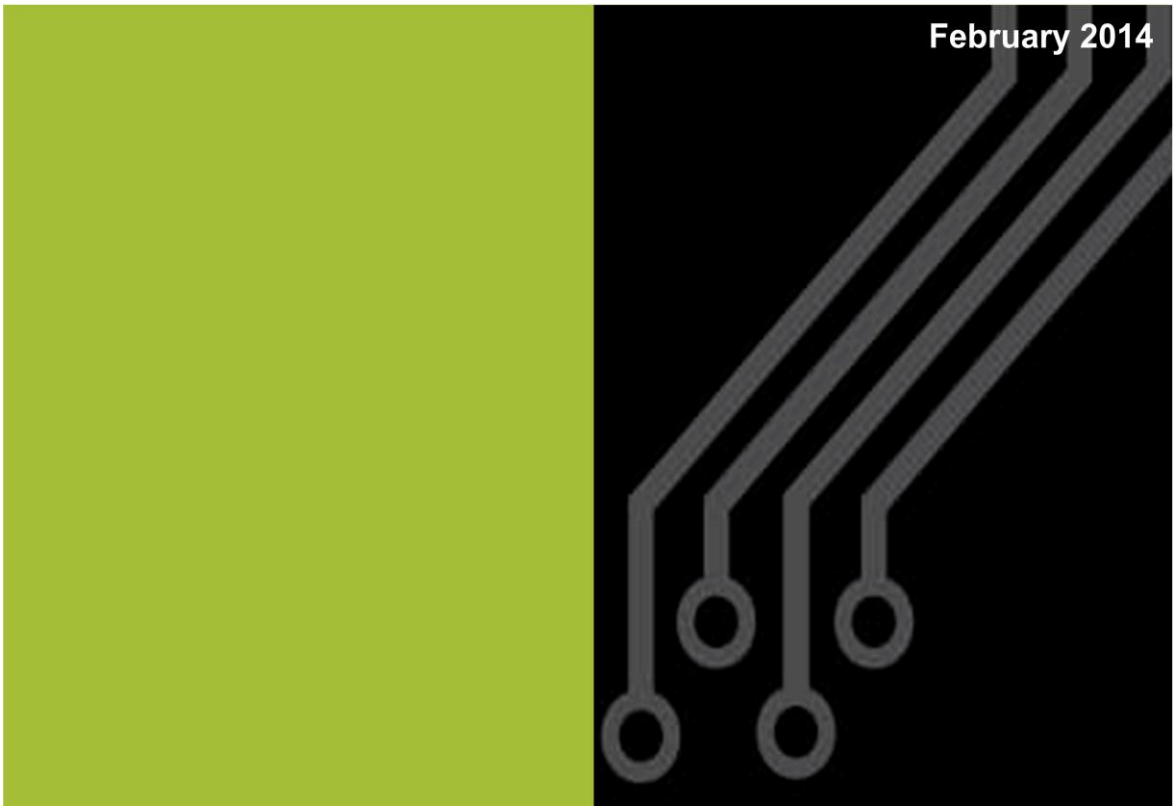
NITA UGANDA
- Driving the IT Revolution -

NATIONAL INFORMATION SECURITY FRAMEWORK (NISF) PUBLICATION

National Information Security Policy



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

Table of Contents

Introduction

1 Introduction

1.1 Overview

This document is the National Information Security Policy. The policy outlines the mandatory minimum security controls that all public and private sector organisations that use, own and/or operate protected computers, handle official communications and personal data must apply to reduce their vulnerability to cyber threats. The use of the security measures mandated by this policy would increase the capacity of organisations to endure and recover from cyber attacks.

1.2 Applicability of National Information Security Policy

As noted above, this policy is mandatory for all public and private sector organisations that use, own and/or operate protected computers, handle official communications and personal data. In accordance with the Computer Misuse Act 2011, the term “protected computers” refers to computers used directly in connection with or necessary for Uganda’s security, defence, diplomacy; law enforcement; communications infrastructure, banking and financial services, public utilities; public key infrastructure and public safety. In this policy, “official communications” encompass information that Ministries, Departments, Agencies and Local Governments (MDALs) create and process during their day-to-day business activities. Official communications have lower security sensitivity than data handled by protected computers. However, the loss, theft and unauthorised disclosure of “official communications” could have negative consequences on the MDALs. Lastly, “personal data” covers data that relates to an individual.

1.2.1 Critical Infrastructure (CI)

In this policy, “critical infrastructure” is the collective term for all systems used directly in connection with or necessary for protected computer activities, the handling of official communications and personal data. This policy adopts the International Telecommunication Union (ITU)’s definition of critical infrastructure (CI). Hence, in this policy, CI comprises of “key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these.” According to the ITU, CI encompasses physical elements such as facilities, buildings and equipment and virtual elements such as systems and data. The ITU further observes that the physical and virtual elements of the infrastructure include human aspects such as the protection of personnel and the mitigation of the insider threat. This policy addresses all aspects of the ITU definition of CI because it covers governance, information, personnel and physical security.

1.2.2 Critical Information Infrastructure (CII)

The ITU regards Critical Information Infrastructure (CII) as the virtual element of critical infrastructure. The information and communication technologies (ICTs), that form CII, increasingly operate and control critical national sectors such as health, water, transport, communications, government, energy, food, finance and emergency services; their physical assets and the activities of personnel.

1.3 Policy Review Cycle

NITA-U shall review this policy, at least annually, to help ensure that it maintains relevance to business needs, cyber threats and approaches for countering them.

1.4 Structure of National Information Security Policy

The National Information Security Framework (NISF) comprises of five tiers or levels. This policy is at tier three. The policy presents a set of mandatory minimum-security requirements under four headings or parts, which are:

- Security governance;
- Information security;
- Personnel security; and
- Physical security

1.5 Adaptation of Security Controls

It is important to stress that the mandated minimum requirements contained in this policy define baseline security controls only. In reality, organisations would have to do more than merely apply the basic security controls. As a result, organisations must adapt the security controls provided for by this policy to their circumstances. Adaptation is inevitable because critical infrastructures reside in many sectors broadly grouped into health and safety, commerce and national security. Therefore, organisations acting through their Boards, must determine the additional security controls that they must apply to mitigate, to acceptable levels, the cyber threats relevant to their business activities. Boards must reach decisions on the level of security controls appropriate for their organisations by considering their own articulated Risk Appetite, business needs and the value, sensitivity and criticality of the information assets under consideration.

1.6 Applicable Legislation

The following legislation underpins this national information security policy:

i. Uganda (1964), "*The Official Secrets Act, 1964 – Section 4(1)(d),"* The Government of Uganda, Entebbe, Uganda.

ii. Uganda (1987), "*The Security Organisations Act, 2005 – Sections 3",* The Government of Uganda, Entebbe, Uganda.

iii. Uganda (2005a), "*The Access to Information Act, 2005 – Section 5(1)*", in *The Uganda Gazette*, The Government of Uganda, Entebbe, Uganda.

iv. Uganda (2005b), *The Uganda People's Defence Forces Act, 2005,* The Government of Uganda, Entebbe, Uganda.

v. Uganda (2006), *The Police (Amendment) Act, 2006,* The Government of Uganda, Entebbe, Uganda.

vi. Uganda (2009a), "The National Information Technology Authority, Uganda Act, 2009 – *Sections 5(b, (c), (d), (f), (g, (h), (n) and (r)*", in *The Uganda Gazette*, The Government of Uganda, Entebbe, Uganda.

vii. Uganda (2009b), "*The National Security Council Act – Sections 2 and 3",* The Government of Uganda, Entebbe, Uganda.

viii. Uganda (2010), "The Regulation of Interception of Communications Act, 2010", in *The Uganda Gazette*, The Government of Uganda, Entebbe, Uganda.

ix. Uganda (2011a), "The Computer Misuse Act, 2011", in *The Uganda Gazette*, The Government of Uganda, Entebbe, Uganda.

x. Uganda (2011b), "The Electronic Signatures Act, 2011 – *Sections 2 and 21*", in *The Uganda Gazette*, The Government of Uganda, Entebbe, Uganda.

xi. Uganda (2011c), "The Electronic Transactions Act, 2011 – *Section 23 (f)*", in *The Uganda Gazette*, The Government of Uganda, Entebbe, Uganda.

2 Policy Context

The Government of Uganda (GoU) regards information security as an enabler of the efficient, effective, safe and secure delivery of public services. Information security also serves national security goals by protecting CII that operate and control the above-mentioned critical national sectors and their physical assets.

2.1 National Information Security Strategy

The National Information Security Strategy (NISS) described the security risks of technological advance and the risk mitigation measures of such advancement. The NISS recommended the creation of the Directorate of Information Security (DIS) in accordance with the National Information Technology Authority, Uganda (NITA-U) Act, 2009. The DIS, which authored this policy, oversees and promotes information security governance, risk remediation planning and response. The NISS also recommended the creation of a National Information Security Advisory

Group (NISAG) to advise the GoU on information security governance matters. The NISS further mandated the creation of a National Computer Emergency Response Team (CERT) under NITA-U.

3 Guiding Principles

The guiding principles below influence actions and decisions within this policy.

3.1 Top Leadership Accountability

The first principle is that the most senior person in the organisation must assume ultimate accountability for information security. Cabinet Ministers should ensure that MDALs report on their information risk position at least annually.

3.2 Collective Responsibility

The principle requires all individuals to accept a collective duty to contribute to efforts to ensure that critical infrastructure assets and services obtain protection commensurate with their value, sensitive and criticality to their organisations.

3.3 Personal Accountability

Individuals must understand and accept personal accountability for safeguarding the assets entrusted to them and expect to answer for and/or face sanctions for breaching security rules.

3.4 Risk Management/Proportionality

Organisations must adapt security controls to their circumstances in particular their business needs, risk appetite, value and sensitivity of their information.

3.5 Secure/Assured Sharing

This principle requires organisations to apply suitable security controls to enable the secure sharing of information regardless of its form and method of transfer.

3.6 Suitable, Trustworthy and Reliable Staff

Organisations must only hire staff after verifying that their character and personal circumstances are such that they can be trusted with access to vital IT assets.

3.7 Resilience

This principle requires organisations to build capacity to withstand and recover from cyber attacks and disruptions in a timely manner with minimal damage.

I.
Security Governance

4 Security Governance

4.1 Introduction

Security governance focuses on all the activities required to manage a functional area namely information, personnel and physical security. This policy adopts the US ISO/IEC 27001 Plan-Do-Check-Act (PDCA) continuous improvement model to structure all security governance processes as illustrated below.

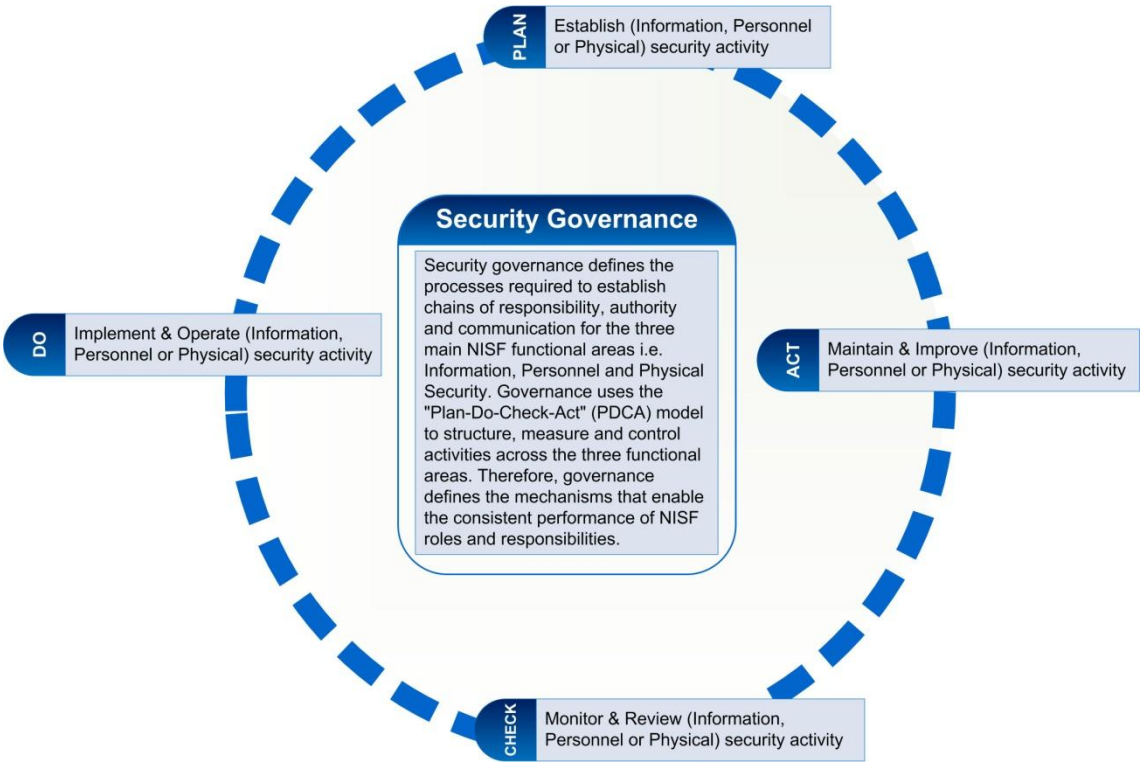


Figure 1 – Security Governance and the PDCA Model

Governance aims to ensure that security programmes support business goals. Thus, mandatory minimum security governance requirements are as follows:

4.2 Policy Statement on Information Security

Boards are supreme governing bodies that provide GoU and private sector organisations 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 organisations, 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.

GV1 – All Boards of organisations with critical infrastructure must issue a Policy Statement on Information Security. As a minimum requirement, the Statement must: (a) recognise information as a vital business asset; (b) acknowledge information risk management as a business enabler and an integral part of good corporate governance; (c) contain the Board's acceptance of ultimate accountability for information risk management; (d) set clear direction on information risk management by determining Risk Appetite; and, (e) assign management and employees security responsibilities..

To achieve the security outcomes mandated above, organisations must:

4.2.1 Issue Policy Statement on Information Security

The policy statement on information security:

- Recognises information – in all its forms – as a crucial business asset;
- Explains why information security matters and outline policy objectives;
- Is a Board commitment to protect organisational information from all threats – internal or external, deliberate or accidental;
- Assigns Accounting Officer accountability for information security; and
- Requires all employees (including contractors) to comply with the Statement.

4.2.2 Articulate Information Risk Appetite

Boards must articulate organisational information Risk Appetite. A statement of information Risk Appetite states the level and type of information risks that a given organisation is willing to accept, tolerate or survive in the pursuit of its strategic goals. The statement must:

- Explicitly note the Board's Risk Appetite in relation to information risk;
- Map the Risk Appetite on a spectrum e.g. low to very high; averse to hungry;
- Address information risk's relationship with corporate goals in the same way as other risks e.g. legal, financial, operational, compliance and reputational;

- Require that all project proposals and plans to demonstrate consistency with the Board articulated information Risk Appetite;
- Be read and understood in conjunction with the risk management strategy;
- Assign monitoring responsibility usually to the Audit Committee; and
- Be reviewed, debated and agreed at least annually.

4.3 Information Security Organisation

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

GV2 – All organisations with critical infrastructure must establish suitable information security management arrangements with clearly defined accountability at all levels. As a minimum requirement: (a) The Accounting Officer must accept personal accountability for embedding information risk management into the Internal Control system; (b) a senior executive must assume overall responsibility for information risk management at Board level; (c) organisation must establish a senior management committee to coordinate information risk management; (d) heads of business divisions must assume responsibility for named information assets; (e) every system must have a single responsible officer; and, (f) organisations must appoint trained staff to security roles.

To achieve the security outcomes mandated above, organisations must:

- Set up an Information Security Management System (ISMS) in accordance with US ISO/IEC 27001:2005. The organisation shall also adopt the "Plan-Do-Check-Act" (PDCA) model to structure all ISMS processes; and
- Create an information security organisation that is fully compliant with the requirements of US ISO/IEC 27001:2005.

As a minimum requirement, organisations should distribute roles as follows:

4.3.1 Responsibilities of Boards & Accounting Officers

The information security organisation must perform the roles below at Board-level:

- Treat information risk as a corporate-level risk;
- Review the information risk position at least quarterly; and
- Explicitly address information risk management in Annual Reports.

4.3.2 Responsibilities of Information Risk Owner

The security organisation shall appoint a Board-level official to the role of Information Risk Owner (IRO) with responsibilities including:

- Ownership of a plan to foster a culture of information security;
- Accountability for the organisational risk management policy;
- Alignment of the risk management programme with business processes;
- Advising on information risk sections of the Statement on Internal Control;
- Ensuring that all assets have skilled and empowered owners; and
- The production of quarterly and annual information risk assessments.

4.3.2.1 Choice of Information Risk Owner

It is important to stress that the IRO is a role not necessarily a job title. As such, organisations could appoint anyone with adequate standing and expertise to this role. However, guided by the Presidential Directive to create a programme to professionalise information security, the Chief Information Security Officer (CISO) or a similar title must be the first choice for the Board-level IRO role. Choosing a CISO for the IRO role would help ensure that the Board receives timely and effective advice about the impacts of their strategic and operational decisions on information security. Organisations may appoint an interim IRO during the hiring and/or training of a CISO or similar title to take over the role.

4.3.3 Responsibilities of Information Asset Owners

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

- Understand and support the organisation's security culture;
- Know what information the assets under their responsibility hold;
- Know who accesses the assets under their responsibility and why;
- Identify and mitigate risks to the assets under their responsibility;
- Ensure that assets under their responsibility are available for business use;
- Provide the Board-level Information Risk Owner reasonable assurance that the assets under their responsibility are secure at least annually.

4.3.4 Responsibilities of Security Coordination Group

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

- Ensure that effective information risk management processes are in place;

- Approve organisational security policies and standards;
- Monitor compliance with agreed security policies and standards; and
- Encourage the professionalisation of all security areas.

4.3.5 Responsibilities of Operational Security team

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

- Implement the organisation's information risk policy;
- Follow approved security policies and standards;
- Enforce security requirements on all stakeholders including suppliers; and
- Identify and report non-compliance with security policies and rules.

4.4 Risk Management

Risk management activities must show that the Board and Accounting Officer, acting with and through the Board-level Information Risk Owner, are complying with the mandatory minimum-security requirements below on mitigating risks to acceptable levels.

GV3 – All organisations with critical infrastructure must adopt a formal, consistent and policy-guided risk management approach to help ensure the security of critical infrastructure. Drawing on the guidance within the NISF, all organisations must: (a) have a suitable information risk policy to address threat sources and actors; (b) prioritise risks; and, (c) manage information risks during the ICT system's development, acceptance, operational and decommissioning and disposal phases.

To achieve the security outcomes mandated above, organisations must:

- Use the Board-issued information Risk Appetite as a guide for routine risk management decisions to ensure that the organisation avoids taking either too much or too little risk in pursuit of its business goals;
- Identify business critical assets and the impact of their compromise or loss;
- Have in place a Risk Register to record and audit risk management decisions by identifying risk owners, residual risk and risk treatment actions; and
- Comply with NISF guidance contained in the Security Standard No.1 – Technical Risk Assessment (SS1) and Security Standard No.2 – Risk Management and Accreditation (SS2).

4.5 Awareness, Education and Training

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

GV4 – Organisations must ensure that all users – including Ministers, Board members, senior executives, employees and third party users – obtain security awareness before gaining access to critical infrastructure. As a minimum requirement, the awareness must: (a) as part of the induction process, explain to staff the security risks associated with their work; (b) help staff gain awareness of the organisation's security policies; (c) remind staff of their personal responsibility for safeguarding assets entrusted to them; (d) articulate potential penalties for breaching security rules; (e) be assessed formally; and; (f) be repeated at least annually.

To achieve the security outcomes mandated above, organisations must:

- Conduct security induction training for all employees, including contractors and subcontractors, to ensure that they are conversant with organisational security policies and procedures as well their personal accountability for securing assets under their control and/or supervision;
- Allocate sufficient resources to finance a sustained user security awareness and education programme covering relevant risks, threats and vulnerabilities; acceptable usage; impacts of cyber attacks; incident response actions and the personal consequences of breaching security rules;
- Avail security policies to all staff, including contractors, internally;
- Ensure that all staff, including contractors, obtain appropriate briefings about how legislation identified in this policy, in particular, the Official Secrets, the Access to Information, the Computer Misuse, the Electronic Signatures and the Electronic Transactions Acts affect their work activities;
- Provide security cleared staff training matching their access privileges;
- Ensure that staff performing security roles receive suitable training; and
- Regularly review and re-evaluate the effectiveness of security awareness and education activities in light of a changing threat environment.

4.6 Business Continuity & Disaster Recovery

Business continuity activities aim to show that the organisation has the capacity to withstand interruptions to critical business activities and thereby achieve the mandatory minimum-security outcomes outlined below.

GV5 – All organisations must implement appropriate business continuity (BC) and disaster recovery (DR) programmes to minimise the impact of and ensure the timely recovery from interruptions that may result from natural disasters, accidents, equipment failures and deliberate actions. As a minimum requirement, organisations must have in place: (a) a BC management strategy that takes a long-term view of organisational continuity needs; (b) a policy outlining management direction and support for business continuity; (c) BC and DR plans for all locations; and, (d) systematic BC/DR testing, reporting and maintenance procedures for all critical infrastructure.

To achieve the security outcomes mandated above, organisations must:

- Address information security needs of organisational business continuity;
- Establish the criticality of different facilities, systems, sites and networks by performing a business impact analysis of the unavailability of each asset;
- Identify and assess the probability and the information security impacts of events that could cause interruptions to business operations e.g. fire, theft;
- Adopt a common business continuity planning framework to ensure that all plans address information security requirements consistently;
- Ensure that continuity plans support correct information security levels;
- Test, audit and update business continuity plans regularly to ensure their effectiveness in an event of an emergency;
- Have put in place up-to-date and effective disaster recovery plans for critical infrastructure systems to minimise the impact of security incidents; and
- Report on BC/DR activities at least once a year.

4.7 Incident Management

Incident management aims to demonstrate that the organisation 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 below.

GV6 – All organisations with critical infrastructure must have a formal security incident management process to enable the accurate and timely identification, communication, investigation and response to security events and weaknesses. As a minimum requirement, the process must: (a) formally establish management's accountability for incident management; (b) define roles and responsibilities; (c) include tested policies, plans and procedures; (d) ensure staff obtain specialist incident response training; (e) promote an incident reporting culture; and, (f) quantify, monitor and learn from incidents.

To achieve the security outcomes mandated above, organisations must:

- Obtain Board endorsement for incident management processes as part of the holistic business continuity management strategy approval;
- Have in place channels for reporting security events to management;
- Require all staff, including contractors, to record and report observed or suspected security weaknesses in systems or services;
- Have in place effective and orderly processes for responding to incidents;
- Put in place effective mechanisms for quantifying and monitoring the types, volumes and costs of information security incidents;
- Adopt procedures for reporting security incidents to GoU agencies such as the national Computer Emergency Response Team (CERT); and
- Ensure that the collection, retention and presentation of data about security incidents comply with relevant rules of evidence to enable follow-up action.

4.8 Assurance & Compliance

Assurance and compliance reporting aims to demonstrate that the organisation is achieving the mandatory minimum-security outcomes outlined below.

GV7 – Organisations must provide reasonable assurance that their security arrangements mitigate risks to critical infrastructure adequately. Using a range of compliance mechanisms, organisations must, as a minimum requirement: (a) provide the Board an assessment of the information risk position, including that of the supply chain, at least quarterly; (b) undertake an annual security assessment against the NISF and approved security policies declaring compliance status; (c) disclose areas of non-compliance with the NISF to their line Minister, Auditor General's Office, security organisations and President in a classified annual report; (d) address information risk within Statements on Internal Control; and, (e) cover information risk management issues including risks, actions and incidents in the Annual Report.

To achieve the security outcomes mandated above, organisations must:

- Provide evidence as to how their security operations comply with US ISO/IEC 27001:2005. In particular, organisations must produce a Statement of Applicability showing the controls implemented;
- Make information risk management a regular item on the Board's agenda;
- Disclose to the Board the main security risks affecting vital business assets in quarterly and annual assessments;
- Add the role of ensuring compliance with security policies and standards, in one's area of responsibility, to a manager's performance evaluation criteria;
- Establish a programme to check regularly that information systems comply with technical security implementation standards. In particular, the technical

compliance checks must identify and report insecure configurations; unauthorised installations; changes to system and application configuration;

- Have in place a comprehensive audit regime that includes penetration testing or ethical hacking and system security audits to identify and report potential gaps in the security of operational systems;
- Have in place a process for communicating additional security requirements to the Board and Accounting Officer in an event of newly identified security threats and vulnerabilities; and
- Have in place an effective process for showing the compliance of security activities with all statutory, regulatory, and contractual requirements.

II.
Information Security

5 Information Security

5.1 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, organisations 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 organisational reputations, legal positions and the ability to conduct business operations.

5.1.1 GoU information security commitment

The GoU is committed to:

- Achieving high standards of Information Security governance;
- Treating information security as a critical business issue and creating a security-conscious environment;
- Demonstrating to third parties that it deals with information security in a proactive manner; and
- Applying the guiding principles outlined in section 3 such as implementing controls that are proportionate to risk.

5.1.2 Applicability of information security requirements

Uganda is determined to thwart internal and external threat actors seeking to breach the security of information assets within the country. Therefore, the information security mandatory minimum-security requirements apply to:

i. All staff in organisations with critical infrastructure including public and civil servants, contractors, consultants, temporary employees, guests and volunteers. The requirements also apply to third parties that access and use of information that critical infrastructures handle;

ii. All types of information i.e. written, printed on paper, stored electronically or optically, transmitted by courier or using electronic means, recorded on magnetic disk or tape, or spoken in conversation;

iii. All information assets including that which public and private sector critical infrastructure organisations use under license or contract. The information can be in any form and recorded on any media, and all computer hardware, computer software and communications networks owned or operated by the organisations or on their behalf; and

iv. Any device, regardless of ownership and including equipment privately owned by public and civil servants, and citizens e.g., laptop computers, tablet computers, smartphones, MP3 players, USB storage devices, etc.

However, this is only with respect to the ways in which they connect to or access information assets and the activities they perform with the assets.

5.1.3 Information Security and Security Governance

The themes contained in "Part 1 – Security Governance" apply to the information security functional area in the same way as personnel and physical security. For example, the information security area must have effective leadership; adopt a credible risk management approach; conduct effective security awareness, education and training; handle security incidents and institute assurance and compliance reporting mechanisms. Moreover, the information security functional area adopts the PDCA continuous improvement model to all processes. The mandatory minimum information security requirements are as follows:

5.2 Information Security Policy

An information security policy helps improve security if published, enforced, audited and updated to reflect organisational requirements. A security policy aims to achieve the following mandated minimum-security requirements:

IS1 – Management must draft, obtain Board-approval and publish an information security policy that addresses the NISF mandatory minimum requirements in terms of the organisation's business requirements, threat environment and risk appetite. As a minimum requirement, the policy must: (a) explain how the organisation and supply chain protect information and physical assets; (b) apply to all the activities linked to protect computers; (c) define acceptance and compliance arrangements by its staff and the supply chain; (d) undergo regular review to ensure its continuing relevance.

To achieve the security outcomes mandated above, the policy must:

- Define the purpose, scope and approach to managing information security within the organisation;
- Identify and assign suitable security roles and responsibilities depending on the size, structure, business needs and threats to the organisation;
- Require the creation of a manual guiding the implementation of an ISMS in compliance with US ISO/IEC 27001;
- Contain or refer to a manual detailing how to apply information, personnel and physical security measures consistently across the organisation;
- Contain or reference a guide that explains the secure working practices that all users must adopt to comply with security policies and related documents;
- Require the generation of evidence showing that the organisation uses the security accreditation process to identify and manage risks to ICT systems;
- Outline the required business continuity roles, processes and procedures;

- Specify penalties for breaching the policy and related security measures;
- Be publicised and made readily available to all staff; and
- Specify a review cycle in order to ensure its continued applicability.

5.3 Asset Management

Organisations must achieve and maintain appropriate protection for information assets in compliance with US ISO/IEC 27001:2005. Effective asset management helps achieve the mandated NISF minimum security outcomes outlined below.

IS2 – All organisations must ensure that assets associated with critical infrastructure receive the level of protection appropriate to their value, sensitivity and criticality. As a minimum requirement, all organisations must: (a) use approved criteria to create a definitive register of business critical facilities, systems, sites and networks; (b) designate a suitably empowered owner for every asset; (c) use the Government Security Classification Standard to determine the acceptable procedures for labelling, handling, transmitting and decommissioning assets; (d) audit the asset register regularly; and; (e) inform the Board of the main security risks affecting vital business assets.

To achieve the security outcomes mandated above, organisations must:

- Conduct an inventory of their assets drawing up and maintaining a register of important assets as a prerequisite to risk management;
- Ensure that designated divisions own and secure named information assets;
- Identify, document and enforce rules of acceptable use of information assets;
- Label and handle information assets throughout their lifecycle in accordance with Security Standard No. 3 – Security Classification (SS3); and
- Use the Business Impact Tables in SS1 to determine the information asset labelling and handling levels.

5.4 Secure Information Sharing

Secure information sharing is about ascertaining that exchange partners have in place security controls that achieve the minimum-security outcomes below.

IS3 – All organisations, particularly those within and/or connecting to Government, must require internal and external entities to show compliance with mandated NISF requirements and approved security policies before sharing or allowing connections to protected computer assets. As a minimum requirement, organisations must: (a) identify and record risks involving external parties; (b) create information exchange policies and procedures; (c) use formal exchange agreements such as codes of connection and memoranda of understanding; (d) assess compliance of exchange partners at least annually or when required; and, (e) disconnect/end sharing with non-compliant entities.

To achieve the security outcomes mandated above, organisations must:

- Ensure that users are fully conversant and comply with approved information exchange policies, procedures, controls and relevant national legislation;
- Use cryptographic solutions to provide users and applications the underlying "trust" to operate authentication, integrity, confidentiality and non-repudiation security services to protect collaborative tools and information exchanges;
- Establish exchange agreements that require parties seeking access to GoU and other critical infrastructure to have in place security measures that match the security classification and handling requirements for the asset;
- Ascertain that exchange agreements with external parties are enforceable;
- Confirm that receiving parties grasp and are complying with their obligations to protect information assets appropriately;
- Adopt policies to handle information assets received from foreign countries and international bodies in line with applicable treaties and arrangements;
- Abide by their own obligations under exchange agreements such as codes of connection (CoCos) and memoranda of understanding (MoUs); and
- Obtain authorisation before granting third parties access to information and ICT systems owned by another organisation.

5.5 Supply Chain Security

All organisations increasingly source ICT systems and software from a global network of suppliers, distributors and business partners. The advantages of a global ICT supply chain including competitive prices, innovative products and flexibility. Regrettably, there is clear evidence that global ICT supply chains have heightened system and software risks. Thus, supply chain security measures aim to help achieve the mandated minimum-security outcomes below.

IS4 – All organisations must mitigate risks of intentional and unintentional supply chain compromise. As a minimum requirement, organisations must: (a) establish consistent supply chain security processes with clear lines of accountability; (b) ensure that suppliers are subject to and pass a national security impact assessment; (c) include security clauses in service contracts; (d) ensure that the computer networks, products and services supplied do not introduce information security risks; (e) assess compliance with requirements at least annually; and, (f) enforce sanctions for non-compliance.

To achieve the security outcomes mandated above, organisations must:

- Identify and evaluate the security risks related to outsourcing or offshoring before letting contracts for critical infrastructure and services;
- Recognise that they retain accountability for managing their information risks even where they outsource ICT systems and services to third parties;
- Ensure that they are fully acquainted and compliant with the national security impact assessment process for ICT suppliers;
- Abide by PPDA instructions to identify, document and incorporate security requirements into outsourcing contracts with suppliers and contractors;
- Require contractors to present an operational security management plan outlining their strategy for reducing security risks to acceptable levels;
- Outline the process for the development and maintenance of procedures, processes, instructions and plans for securing the system;
- Issue Security Aspects Letters (SAL) regularly to update contractors on the security conditions that govern their access to critical infrastructure assets;
- Require suppliers to obtain approval for physical facilities before the hosting of GoU and other critical infrastructure systems and services; and
- At least annually, obtain independent assurance that suppliers are complying with the mandated NISF requirements and other security policies.

5.6 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 below.

IS5 – Organisations must ensure that only users, processes and devices with a business need and suitable security clearances gain access to critical infrastructure. As a minimum requirement, access management must: (a) follow a formal access control policy linked to HR processes; (b) use formal access registration and revocation processes; (c) require appropriate identification and authentication techniques for all IT systems; (d) enable organisations to deter, detect, resist and defend against accidental or deliberate unauthorised actions; and, (e) enable regular review of access rights.

To achieve the security outcomes mandated above, organisations must:

- Define and document business requirements for access control and restrict access to critical infrastructure to those who satisfy these requirements;
- Adopt an access control policy that enforces the principle of least privilege;
- Restrict and control the allocation and use of privileges in accordance with the Need-to-Know principle;
- Select and apply a suitable access control model amongst Discretionary, Role Based and Mandatory Access Control;
- Apply the principle of uniform access management i.e. use of authentication and authorisation services to control resource use;
- Have in place a formal process for user password management;
- Ensure that users are aware of and abide by their responsibilities to maintain access controls such as passwords;
- Enforce recommendations of access rights reviews e.g. disable users; and
- Harden and lockdown user applications such as web browsers and office productivity applications to reduce exposure to software vulnerabilities.

5.7 Network Security Controls

Proportionate risk-based technical security controls can help achieve the mandated NISF minimum-security outcomes outlined below.

IS6 – All organisations must apply technical security controls appropriate to the protected computer's value, sensitivity and criticality. As a minimum requirement, the controls must include: (a) a formally documented security architecture providing end-to-end network security; (b) the segregation of networks handling information of different business impact levels; (c) the enforcement of service minimisation; (d) the use of unified authentication and authorisation services; (e) the matching of security levels with information protection needs; and, (f) the adoption of the defence-in-depth principle.

To achieve the security outcomes mandated above, organisations must:

- Adopt a security architecture that provides end-to-end network security by enabling the detection, identification and correction of security vulnerabilities;
- Ensure that users only gain access to network services e.g. web browsing and file upload if they have a legitimate business reason for the access;
- Enforce sufficient segregation, zoning or variable depth security to separate specific areas of the network, groups of information services and information systems handling data of different security classification levels;
- Implement boundary protection measures for shared networks, especially those extending across organisational boundaries, in compliance with the access control policy and requirements of the business applications;
- Enforce network routing controls to ensure that connections and information flows do not breach the access control policy of the business applications;
- Apply the principle of service minimisation consistently across the network by disabling services that do not satisfy business and security needs for access;
- Adopt solutions that use techniques such as encryption to offer converged voice, data and video packets protection appropriate to their security needs;
- Adopt the "defence in depth" or "layered" approach to network security through the use of different technical security controls and security products to mitigate security threats collectively; and
- In accordance with ISO/IEC 18043, install network intrusion detection (NIDS) and network intrusion protection (NIPS) devices to monitor network traffic for unusual or suspicious activity and prevent cyber attacks; and
- Build survivability into networks to ensure that technical solutions continue to deliver a minimum set of essential functionality in a timely manner even if parts of the network are unreachable or have failed due to an attack.

5.8 Malicious Code Protection

Malicious code such as such as viruses, worms, spyware and Trojan Horses are popular attack vectors for a range of threat actors seeking to gain unauthorised access to sensitive ICT systems and the information they store and handle. The threat actors use e-mail attachments, infected websites, instant messages, chat rooms and social media to trick users into clicking on infected links. Malicious code exploits vulnerabilities in ICT hardware and applications to breach security. Therefore, understanding malicious code risks and applying appropriate security countermeasures can achieve the mandated minimum-security outcomes below.

IS7 – All organisations with critical infrastructure must apply appropriate controls against malicious code. As a minimum requirement, the organisations must: (a) assess the risk of malicious code; (b) adopt a malicious code policy that considers their business needs and threat environment; (c) deploy suitable malicious code detection mechanisms; (d) educate users about malicious code risks; (e) ensure that authorised mobile code complies with security policy; and (f) address published technical vulnerabilities in a timely manner.

To achieve the security outcomes mandated above, organisations must:

- Mandate that all users, regardless of location, abide by a malicious code policy that should, amongst other issues, require the installation of anti-virus or anti-malware software on all devices; update of anti-virus or anti-malware software signatures; system scanning; secure file attachment handling; secure file sharing; removable media scans; virus log generation and review;
- Identify and block all direct e.g. e-mail attachments, social media, malicious websites and indirect e.g. unauthorised personal laptops, PDA, USB, CD/DVD routes that threat actors could use to inject malicious code;
- Ensure that network boundary devices have the capacity to check inbound and outbound content for malicious code such as viruses, worms and Trojan horses and mobile code such as Java, JavaScript, ActiveX, or any other executable code with potential to damage networks, applications, and data;
- Use measures such as logically segregated environments (i.e. sandboxes) and application-specific controls to manage the execution of mobile code;
- Install host-based software to scan, clean, quarantine and raise alerts about suspicious files, including malicious websites, prior to access;
- Provide users suitable security awareness and education about the impacts, preventative measures and actions against malicious code attacks;
- Routinely patch ICT systems, security enforcing products and applications against known vulnerabilities to reduce exposure to malicious code;
- Conduct regular vulnerability assessments to identify potential weaknesses that could enable the introduction of malicious code;
- Build adequate capacity to identify, deter, resist and defend against known and unknown (zero-day) malicious code attacks; and

- Have in place effective and current contingency, recovery, investigatory and reporting procedures to enable timely response to malicious code attacks.

5.9 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 organisations that organisations supply, IT departments face pressures to accept the trend of bring your own device (BYOD) where staff seeks to use personally owned devices at work. However, the portable devices expose sensitive information assets to security risks greater than one would expect in office environments usually due to the lack of physical security measures. Thus, portable and removable media security aims to achieve the outcomes below by balancing the benefits and risks of mobile devices.

IS8 – All organisations using portable and removable media must adopt formal procedures to prevent the unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities. As a minimum requirement, organisations must: (a) perform a formal risk/benefit analysis before use of the media; (b) as part of a formal policy, require authorisation to use and transfer the media; (c) use baseline builds that, by default, lock down access to media drives; (d) encrypt devices to deter unauthorised access; (e) enforce security policy on media to detect and resist unauthorised use; (f) conduct user awareness training; (g) audit user actions; and, (h) prevent the holding, storage and processing of sensitive information on personal devices.

To achieve the security outcomes mandated above, organisations must:

- Lock down host devices to stop users changing default configurations and thereby enabling malicious actors to execute privileged commands;
- Use full disk hardware encryption for devices processing sensitive data;
- Ensure that users understand that maintaining physical custody of the device is the best form of defence;
- Not allow the use of privately owned devices to process, store or remotely access critical infrastructure, programs and data except in emergency, short-term situations where it is not practical to issue official equipment;
- Define procedures for the timely termination of emergency use of privately owned devices to process, store or remotely access critical infrastructure;
- Prevent devices that do not comply with organisational policy, such as the use of hardened configurations, from connecting to the corporate network;
- Give users appropriate training in the handling of authentication credentials such as encryption keys, hardware tokens, smartcards and passwords;

- Defend against random and targeted attacks by requiring users to power off devices when not in use; never to leave devices unattended; requiring that users store devices separately from credentials, amongst other measures;
- Minimise data aggregation risks by ensuring that user devices only store data required to perform approved business activities at any given time;
- Adopt anti-virus or anti-malware procedures including stand-alone systems (i.e. 'sheep dips') to scan portable and removable media for malicious code before their use for data import and export; and
- Make sure that users are conversant with mobile device incident response and reporting procedures such as when to report device loss to the Police.

5.10 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 access presents unique security challenges to organisations. Firstly, remote access calls for additional security measures given that it occurs over insecure public networks. Secondly, because remote access occurs in exposed environments such as homes or when travelling, it increases exposure to risks such as theft of equipment and information, the unauthorised disclosure of information, unauthorised remote access to internal systems or misuse of facilities. Therefore, in accordance with ISO/IEC 27002, organisations must not authorise remote access or teleworking unless satisfied that suitable security arrangements and controls are in place and that the measures comply with relevant information security policies. Good remote access security can help achieve the following mandated information security outcomes.

IS9 – All organisations must implement appropriate security measures to mitigate remote access risks. As a minimum requirement, organisations must: (a) adopt a formal remote access policy; (b) assess the risks, threats and vulnerabilities of remote access; (c) use security controls e.g. encryption to protect data whilst at rest and in transit; (d) educate users about remote access risks; (e) security accredit remote access solution handling classified data; and, (e) align remote access policy with incident management plans.

To achieve the security outcomes mandated above, organisations must:

- Adopt a formal remote access policy that defines roles and responsibilities for management, users, administrators and security personnel guided by business needs, conditions, threats and the impacts of security breaches;
- Demonstrate that adequate authentication, access control, communication and availability measures are in place to reduce the risks of unauthorised access, disruption and modification of remote access solution servers, clients and applications in accordance with ISO/IEC 18028-4;

- Enforce a remote access policy requirement that users and devices only gain access to network services for which they authorisation for;
- Grant remote access only for as long as is necessary for business purposes;
- Use encryption of suitable strength to secure communication links and the content that they process against eavesdropping;
- Encrypt remote access clients to make them inaccessible if lost or stolen;
- Ensure that users accept and comply with the Security Operating Procedures (SyOPs) for mobile devices such as powering off devices when not in use;
- Ensure that users know and accept their personal accountability for guarding remote access devices against threats and risks in insecure environments such as snatching, shoulder-surfing, eavesdropping etc;
- Provide remote access servers satisfactory security including protection against unauthorised physical access; assured power supply; secure set-up, configuration and administration; back-up and recovery procedures;
- Present a formal risk assessment and obtain approval from relevant security agencies before permitting the remote administration of critical infrastructure, programs and data from overseas locations given the risk posed by threat actors and sources such as foreign intelligence services to such access;
- Ensure that remote access solutions, including contracts with IT suppliers, comply with applicable legislative or regulatory constraints in particular the Official Secrets Act, 1964 and the Access to Information Act, 2005 regarding the handling of information, which is likely to prejudice the security of the State or interfere with the right to the privacy of any other person;
- Submit remote access solutions to a formal security accreditation process to provide assurance about the adequacy of information security measures e.g. baseline builds; personnel and physical security controls in the context of the unique threats, vulnerabilities and risks such solutions face; and
- Sanitise and dispose of remote access devices in accordance with the NISF Secure Equipment Disposal and Re-Use requirements.

5.11 Protective Monitoring

Protective monitoring comprises of technical and procedural measures geared at detecting and stopping attempts to exploit information system vulnerabilities. Organisations 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. The mandated minimum security outcomes outlined below would help create an effective protective monitoring regime.

IS10 – All organisations must implement measures to detect, and tie to users, unauthorised information processing activities. As a minimum requirement, organisations must: (a) define a monitoring strategy; (b) adopt an accounting and audit policy; (c) produce, and preserve for an agreed time, audit logs recording user activities, exceptions, faults and security events; (d) establish procedures for reviewing monitoring results; (e) train staff to interpret monitoring results; (f) protect audit and logging facilities and log data; and, (g) align protective monitoring with incident management and HR policies.

To achieve the security outcomes mandated above, organisations must:

- Define and adopt a protective monitoring strategy that defines the objectives, approaches and resources required to support consistent organisation-wide accounting, audit and monitoring activities;
- Have in place an accounting and audit policy that complies with business requirements for real-time security accounting and audit. The policy shall help developers and product teams ensure that technical solutions consist of suitable accounting and audit points. In addition, it should help information assurance teams to verify the extent to which the implemented accounting and audit features comply with NISF security accreditation requirements;
- Ensure that the network security architecture contains suitable features to identify, record, alert and generate security audit reports;
- Ensure that accounting activities match the level of logging for each security classification. IT teams must not deviate from the accounting requirements before presenting a risk assessment and convincing management that the new level of logging adequately assures the security of business activities;
- Standardise accounting and audit log data to ease correlation in accordance with ISO/IEC 27002;
- Have in place effective procedures to review recorded logs and alerts to help identify and hold to account those who misuse information assets;
- Hire and maintain a competent team to administer the technological solutions and supporting infrastructures that collect, store and log suspicious events;

- Enforce access control measures guided by the least privilege principle to help ensure that no user or application process gains access to accounting and audit data without explicit authorisation and a clearly defined role;
- Deny system administrators the access privileges to erase or de-activate logs of their own activities;
- Separate accounting and audit logs that support routine security activities from evidential logs that have legal ramifications because they might contain intrusive and confidential personal data and may be admissible in Court;
- Ensure that, where protective monitoring activities collect data of relevance in legal proceedings, it is possible to verify and demonstrate the evidential weight of the data and ensure its legal admissibility in Courts of Law;
- Have in place a process for escalating to management representatives alerts from real-time accounting and audit systems to enable decisions on whether or not to trigger the incident management process; and
- Update the accounting and audit policy to reflect changes in the threat environment and results of technical risk assessments.

5.12 Information Back-Ups

Achieving the mandated minimum information security outcomes outlined below can ensure the integrity and availability of data, software and documentation and enable quick recovery from disasters or media failures. Back-ups should cover all information processing environments such as live and pre-production.

IS11 – All organisations must adopt formal policies and procedures to backup and regularly test copies of information and software required to recover from major disruptions. As a minimum requirement, organisations must: (a) define the required back-up levels; (b) base the frequency of back-ups on the value, criticality and sensitivity of data; (c) produce accurate and complete records of back-up copies; (d) store back-up data a safe distance away from the main site; (e) afford back-up information suitable physical and environmental protection; and, (f) test back-up media regularly to ensure its recoverability.

To achieve the security outcomes mandated above, organisations must:

- Define the extent e.g. full or differential backup and frequency of backups that reflect business requirements as well as security and criticality of the information to the continued operation of the organisation;
- Regularly test back-up arrangements for individual information systems to help ensure that they meet the requirements of business continuity plans;
- Back-ups for critical systems must cover all systems information, applications and data needed to recover the entire system in the event of a disaster;

- Regularly check and test restoration procedures to help ensure their effectiveness and ascertain whether they can be completed within the time allotted in the operational procedures for recovery; and
- Apply appropriate safeguards to maintain mandated security properties for the back-ups such as the use of encryption to maintain confidentiality.

5.13 Security Accreditation

There must be a clear plan to provide stakeholders relevant information about how an organisation complies with the mandated NISF minimum security requirements. Organisations demonstrate compliance with security requirements by creating a body of evidence containing procedures, processes, instructions and plans for maintaining the security of an information system throughout its life. The mandated minimum information security outcomes below would show that the organisation has identified and addressed major risks to vital systems.

IS12 – All protected Government computers must be accredited to the NISF Risk Management and Accreditation Standard. As a minimum requirement, organisations must: (a) accept and retain accountability for accreditation; (b) ensure that every IT project has a senior responsible owner; (c) define an accreditation boundary; (d) develop an accreditation roadmap; (e) create accreditation plans; (f) record all procedures, processes, instructions and plans for securing the system; (g) conduct suitable system acceptance testing notably penetration testing; and, (h) identify through-life accreditation costs.

To achieve the security outcomes mandated above, organisations must:

- Adopt the US ISO/IEC 27001:2005 controls set, select appropriate and applicable countermeasures to reduce risks;
- Agree with the Accreditor, the approach for measuring compliance with the NISF;
- Show compliance with the corporate policies and legislation applicable to the system's security accreditation scope;
- Describe how the security accreditation process met applicable business and security requirements;
- Demonstrate how the risk management strategy for the system helped establish the business impact of compromising the security of key assets;
- Assess threats and risks to the information system, develop a risk treatment plan and countermeasures against identified risks; and
- Present a detailed plan for managing security risks to the system throughout its lifecycle until decommissioning.

III.
Personnel Security

6 Personnel Security

6.1.1 Introduction

Employees are the most important asset for any organisation. However, staff could also be potent threat sources and actors. Indeed, changes in national information security policies worldwide have roots in high-profile accidental and deliberate disclosures of sensitive national security and personal information. Therefore, it is vital to reduce the likelihood of staff exploiting legitimate access to critical infrastructure facilities, sites, information and staff for unauthorised use. Personnel security is important in the context of defending the cyber supply chain against State and industrial espionage threats. This section outlines the steps that organisations that use, own and/or operate critical infrastructure must take to establish the trustworthiness, integrity and reliability of individuals before granting them access to sensitive information assets.

6.1.2 Personnel Security and Risk Management

The themes contained in “Part I – Security Governance” apply to the personnel security functional area in the same way as information and physical security. For example, the personnel security area requires a credible risk management approach as follows. There are no guarantees in security. This is more so concerning personnel security. It is impossible to guarantee that people would always behave reliably. For example, honest individuals experience changes in lifestyle, which could affect their reliability. Changes such as new spouses and starting a family could put individuals under financial pressure challenging their integrity. In other instances, reckless personal behaviour and entrapment could increase susceptibility to blackmail. Therefore, organisations must follow the risk management principle and the mandatory security requirement presented in part 1, to decide the level of acceptable personnel security risk at any given time. As a result, mandatory minimum personnel security requirements are as follows:

6.2 Security Roles & Responsibilities

National legislation such as the Official Secrets Act, 1964 and newer laws such as the Computer Misuse Act, 2011 generally aim to reduce unlawful misuse of information, in particular that has been entrusted in confidence to Government officers, employees and contractors. However, it is difficult to enforce such laws in Courts of Law if organisations fail to demonstrate that employees, contractors and third party users understood their responsibilities. Achieving the mandated minimum information security outcomes below would help an organisation show that it has taken due care to ensure that the individuals understand expectations.

PS1 – To reduce the risk of theft, fraud or misuse of facilities, organisations must ensure that all users understand their information security responsibilities. As a minimum requirement, organisations must: (a) communicate security expectations to all employment candidates; (b) include security duties in the employment contracts that all staff must agree and sign; (c) require staff to sign

and abide by Security Operating Procedures (SyOps) for specified critical infrastructure or services; (e) inform staff that non-compliance with the signed security documents may lead to disciplinary action; and, (f) enforce sanctions for non-compliance including dismissal and prosecution.

To achieve the security outcomes mandated above, organisations must:

- Require all employees, including contractors and subcontractors to accept their security roles and responsibilities formally. The acceptance shall include an undertaking to: (i) protect assets under their control and/or supervision from unauthorised access, disclosure, modification, destruction and interference; (ii) comply with security processes and activities; and, (iii) report security events or potential events or other security risks to the organisation;
- Ensure that individuals agree to abide by all GoU and organisational policies, standards, protocols and guidelines for protecting information, personnel and physical assets against security threats regardless of type and origin; and
- Confirm that, as part of the HR process, all employees, including contractors and subcontractors, accessing and/or operating critical infrastructure sign declaration forms acknowledging their obligation to abide by the Official Secrets Act, 1964 and related laws during and after their employment.

6.3 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.

6.3.1 Baseline Security Clearance Defined

This clearance is for individuals that would have access to information up to and including RESTRICTED, and/or occasional, controlled and supervised access to information up to and including SECRET. Achieving the mandated minimum-security outcomes below boosts confidence in the reliability of people accessing sensitive assets.

PS2 – All organisations must perform Baseline Security checks to ensure that the character and personal circumstances of individuals seeking employment are such that they can be trusted with access to critical infrastructure. As a minimum requirement, organisations must: (a) satisfactorily validate the identity of all applicants; (b) confirm academic, employment and financial

records; (c) undertake criminal record checks; (d) establish that applicants are entitled to undertake the employment in question; and, (e) record and risk manage cases where it is impossible to perform all the required checks.

To achieve the security outcomes mandated above, organisations must:

- Ensure that HR processes do not allow anyone to commence work on critical infrastructure projects without undergoing appropriate recruitment checks;
- Verify the identity of the candidate by conducting independent checks using Government or third party issued documents such as passports or similar photographic identity documents;
- Establish whether the applicant has the right to work in Uganda including meeting residency requirements based on the sensitivity of the position;
- Check the candidate's employment record by validating the completeness and accuracy of the curriculum vitae;
- Obtain satisfactory character references about the applicant e.g. one business and one personal;
- Establish whether the applicant is qualified for the job by confirming the claimed academic and professional qualifications; and
- Based on risk assessment, determine whether the applicant is liable to undergo additional national security vetting described in section 7.4.

6.4 National Security Vetting

A security clearance is a status granted to individuals that allows them to access certain information. Security clearance is important for critical positions because occupants of such positions who successfully commit acts such as illegal site access, data espionage, illegal interception, data and system interference cause more significant damage to national security and interests that those in less sensitive positions. Therefore, national security vetting seeks to stop individuals wishing to subvert or damage the stability of Uganda from occupying sensitive positions dealing with critical infrastructure. The national security vetting process involves tougher checks than BS vetting using two clearance levels as follows:

6.4.1 SECRET Clearance

This security clearance level is for individuals who require frequent and uncontrolled access to information up to and including SECRET.

6.4.2 TOP SECRET Clearance

This clearance level is for individuals in privileged and sensitive managerial, technical and information security roles who require frequent and uncontrolled access to information marked or labelled up to and including TOP SECRET. Organisations must keep such roles to a minimum number of staff. It is important to emphasise that, in common with all forms of security, national security vetting provides no guarantees about the future reliability of vetting subjects. However, effective national security vetting can help achieve the outcomes below.

PS3 – Individuals requiring access to computers necessary for Uganda's security, defence, diplomacy, public safety, public utilities and economic stability must undergo national security vetting. As a minimum requirement, organisations must: (a) submit for security vetting all applicants for roles on the list of GoU security vetted positions; (b) not initiate the national security vetting process before completing recruitment checks; and, (c) seek Security Controller advice on the required clearance levels before making job offers.

To achieve the security outcomes mandated above, organisations must:

- Create a process to comply with the national security vetting requirements of appropriate vetting organisations;
- Ensure that the Security Controller has the current list of GoU security vetted positions and that all candidates for positions on the list undergo national security vetting before starting work;
- Ensure that the holding of a valid security clearance is not a routine condition for applying for posts or contracts on the list GoU security vetted positions.

However, in exceptional situations, for example where the clearance process would take longer than the contract, organisations might make it a condition. Organisations must record the exceptions for audit and legal reasons;

- Be aware that security vetting can occur either during recruitment or at any stage when business requirements, perceived risks, sensitivity and value of information warrants more assurances about the employee's character and personal circumstances;
- Have a GoU Ministry, Department, Agency sponsor for all security clearance applications;
- Subject to national security considerations and guided by the Need-to-Know principle, the sponsoring GoU entities should inform individuals when they submit their names for national security vetting;
- Ensure that candidates understand that, whilst no one is obliged to undergo national security vetting, occupancy of posts on the GoU list of security vetted positions is reliant upon obtaining and keeping a security clearance;
- Rely on risk assessment to determine the necessity for, and the level of, security vetting undertaken for candidates aiming for sensitive positions. For example, support and ancillary staff may have to undergo appropriate vetting depending on the results of the risk management exercise;
- For sensitive positions, organisations may in accordance with relevant laws, regulations and ethics, evaluate the applicant's likelihood to succumb to pressure and/or inducement to exploit their legitimate access to premises, information and staff for unauthorised use by conducting detailed checks of the applicant's financial matters such as credit references, assets held individually and with family members, financial commitments, unpaid bills etc;
- In strict adherence with relevant laws, regulations and ethics, organisations may consider whether the personal circumstances of the individuals such as medical and criminal history as well as behaviour could pose a security risk were that person to gain employment in a sensitive position;
- Work with vetting organisations to find solutions to delayed clearances. For example, an employee may work "at risk" for a specified time, as long as the individual is being vetted and is working under supervision;
- Only disclose the information gathered for the security clearance application to organisations with a legitimate Need-to-Know. In addition, organisations must only retain the security clearance information for as long as necessary;
- Make a risk-based decision on whether to rely on the security vetting results obtained from another organisation on a candidate under consideration, re-start the vetting process or conduct more checks;
- Subject to national security considerations, have in place a mechanism for providing individuals reasons for the refusal of a security clearance;
- Have in place a policy for dealing with existing employees who cannot continue in their existing position and/or take up a new position because of an adverse security vetting result. The policy must address issues such as re-deployment and appeal procedures. Additionally, organisations must have

clear, legal and ethical dismissal procedures for staff who fail a vetting check but whose occupancy of positions requires a valid security clearance.

6.5 Ongoing Personnel Security Management

Baseline and national security vetting checks only provide assurance about the individual's security reliability at a given point in time only. In reality, baseline and national security vetting occurs before the individual joins a new organisation and/or changes jobs. Both screening exercises may not expose the vetting subject's full susceptibility to personal misbehaviour and/or amenability to influence. Therefore, ongoing personnel security management aims to achieve the mandated outcomes below.

PS4 – All organisations must monitor the continued security reliability of individuals holding a GoU security clearance. As a minimum requirement, organisations must: (a) maintain a record of security cleared individuals; (b) ensure that only those with a business need maintain access to protected computer assets; (c) identify changes in personal circumstances; (d) inform individuals that failure to advise GoU vetting agencies of any significant changes in personal circumstances may lead to disciplinary action; (e) undertake periodic security appraisals; (f) investigate anything that may affect an individual's suitability to access critical infrastructure; and, (g) sanction non-compliance.

To achieve the security outcomes mandated above, organisations must:

- Maintain up to date personnel security records of security cleared individuals as well as refused and withdrawn security vetting applications;
- Ensure that security clearances undergo regular review and/or when material facts or changes come to light to ensure that records are updated and re-affirm the individual's suitability to hold a security clearance at a given level;
- Inform national vetting organisations of any security incidents that may affect the individual's continued suitability to hold a GoU security clearance;
- Submit individuals to pro-active security appraisals, annually and/or when circumstances dictate, during which the vetting subject shall declare changes in professional and personal circumstances and any security concerns that might materially affect their suitability to retain a security clearance at a given level. Individuals must understand that vetting organisations would regard any failure to disclose material and security relevant changes to personal circumstances as unreliability to the detriment of their security clearances;
- Line managers and other staff have a duty to work with HR to identify, report and investigate significant changes to the individual's behaviour, personal circumstances and attitudes to risk. Common warning signs include drug and alcohol abuse, changes in working patterns, lateness etc;

- Ensure that access control measures maintain adherence to the Need-to-Know principle to make sure, that all times, individuals only have access to premises, information and staff they need to perform their jobs. In keeping with the mandated access management security outcome, organisations must review the appropriateness of access rights regularly; and
- Have in place formal processes for investigating suspected non-compliance with security rules. Any such investigations, legal or disciplinary cases must comply with relevant laws, regulations and ethics.

NITA UGANDA
- Driving the IT Revolution -

IV.
Physical Security

7 Physical Security

Physical security is about stopping unauthorised physical access, damage, and interference to information, premises and resources by a range of physical security threats including crime, espionage, natural disasters and acts of terrorism. It also protects personnel against violence and other sorts of harm.

7.1.1 Physical Security, Governance and Risk Management

The themes contained in “Part I – Security Governance” apply to the physical security functional area. For example, physical security also adopts the PDCA continuous improvement model to structure all its governance processes. Indeed, physical security measures are more effective when considered at all phases of the broader organisational security programme. Physical security is harder and more expensive to ‘bolt-on’ after the event. Physical security also complies with mandated minimum security requirements on risk management contained in the Governance section of this policy. Thus, good physical security measures match business and security needs.

7.1.2 Physical Security in Context

Physical security measures work alongside and indeed are the bedrock of other areas of security such as information and personnel security. Physical security represented the bulk of security measures in the mainframe era. Organisations invested substantial sums of money to restrict personnel access, used locks and alarms and implemented environmental controls to cool the giant machines. It all changed when computers became cheaper and smaller. For example, section 6.10 shows that remote access increases the risks of equipment and data theft because it occurs in exposed environments such as homes or when travelling.

7.2 Physical Security Perimeter

This policy requires organisations to put in place an adequate physical perimeter around sensitive information processing facilities to stop unauthorised physical access. A perimeter is the whole area surrounding the building hosting protected computer assets including roads, footpaths and any other areas just outside the building. The physical security perimeter is the first layer of a ‘layered’ or ‘defence-in-depth’ approach to security that progressively increases the difficulty of security controls the closer one gets to areas containing sensitive information assets. As noted earlier, the physical security controls that the perimeter enforces must align with business needs and be cost-effective. The costs of the controls must not substantially outstrip the impact of loss. If the costs outstrip the impact of loss, organisations should consider avoiding the risk, for example by moving the assets to data centres that are easier to secure. By minimising the risk of theft, destruction and unauthorised access, the security perimeter can help achieve the following mandated minimum security outcomes.

PH1 – All organisations must have appropriate security perimeters to shield facilities hosting critical infrastructure against a range of physical security threats including crime, natural disasters and acts of terrorism. As a minimum requirement, organisations must: (a) allocate physical security roles and responsibilities in particular designate a security controller; (b) conduct physical security risk assessments before site selection; (c) design into or require changes to a site's security; (d) have effective access controls; (e) log and review access; (f) prepare for, detect and respond to physical incidents.

To achieve the security outcomes mandated above, organisations must:

- Allocate physical security roles to facilities hosting critical infrastructure. In common with information and personnel security, the Information Risk Owner shall have overall responsibility for physical security risk management at Board-level. The Information Risk Owner should appoint a Security Controller to oversee day-to-day security aspects of a facility or group of facilities. The Controller shall be Ugandan and either full-time or part-time depending on business needs, costs and risks including national security;
- Have in place a physical security policy that describes in appropriate detail how the organisation would define, apply and evidence physical security controls in all its locations in accordance with US ISO/IEC 27001:2005;
- Ensure that no classified GoU data is processed, stored or transmitted to and from any facility without a full risk assessment and formal approval from the GoU client and relevant GoU national security agencies;
- Choose the data centre site carefully taking into consideration issues such as its visibility; proximity to hazards and crime; natural disasters; transportation; access to environmental controls and emergency services;
- Ensure that the site is designed securely with careful consideration for wall height and fire rating; ceiling fire and weight bearing ratings; door and window design and strength; electricity and environmental controls;
- Clearly define the perimeter and ensure that its location and strength corresponds with the security requirements of the assets within the boundary and the results of a risk assessment;
- Ensure that the perimeters are physically sound with no gaps to enable easy break-in. In addition, external walls of the site must be of solid construction with all external doors suitably protected against unauthorised access with control mechanisms, e.g. bars, alarms, locks etc; and
- Ensure that Security Standard No. 5 – Physical Security (SS5) and referenced material therein are the main source of guidance on physical security matters.

7.3 Physical Entry Controls

Secure areas within information processing facilities must have appropriate entry controls to stop unauthorised personnel from gaining access. In keeping with the

risk management/proportionality principle, the physical entry controls in place must be commensurate with business and security requirements. Physical entry controls can help achieve the following mandated minimum-security outcomes.

PH2 – Organisations must use appropriate entry controls to protect secure areas against physical security threats. As a minimum requirement, organisations must have: (b) baseline security controls such as guards, fencing and external monitoring; (b) access card systems to identify employees, log and manage access rights; (c) visitor management processes to enable visitor sign-in, badge allocation, escorting and pass verification; and, (d) employee management processes including requirement to wear identification and carry access cards and the control of equipment movements.

To achieve the security outcomes mandated above, organisations must:

- Ensure that all facilities have in place baseline physical access controls to safeguard information resources therein including an on-duty security guard force; fencing (i.e. fences, gates, turnstiles and mantraps) and external security guard patrols, outside Closed Circuit Television (CCTV) monitoring or a combination of both. In addition, organisations must mandate the use of access cards for access to buildings;
- Ensure that all visitors report to the security reception and produce proof of identification before gaining access to sensitive facilities. The visitors must sign-in and sign-out and must wear an appropriate badge e.g. unescorted or escorted at all times;
- Record the date and time of entry and departure for all visitors. In addition, visitors must only gain access to premises supporting critical infrastructure for specific and authorised purposes;
- Visitors receive a briefing on the security procedures of the secure facility including emergency procedures;
- Control and restrict access to areas designated for processing or storing sensitive information to authorised persons only;
- Have in place appropriate authentication controls e.g. access control cards plus PIN to manage and validate access and securely maintain an audit trail of all access;
- Require all staff and visitors to wear visible identification at all times. All staff at a facility have a duty to notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;
- Grant third party support service personnel restricted access to secure areas or sensitive facilities when required only and monitor the access; and
- Review, update and revoke access rights to secure areas regularly.

7.4 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 centre, communication and switching centres and end-user areas. The areas require more stringent personnel security controls to safeguard the information processed therein. Organisations must develop a general access control policy for use in the data centre to achieve the following mandated minimum security outcomes.

PH3 – Organisations must implement appropriate internal physical security controls to defend critical infrastructure against physical attacks. As a minimum requirement, organisations must match the value, sensitivity and criticality of assets with: (a) data centre classifications; (b) data centre location requirements; (c) infrastructure and perimeter security measures; (d) access controls; (e) access control logging levels; (f) package handling mechanisms; (g) visitor management systems; and, (h) tape handling approach.

To achieve the security outcomes mandated above, organisations must:

- Classify data centres according to their criticality to the continued operation of one or major business activities. The categories may be as simple as A (TOP SECRET); B (SECRET); and C (RESTRICTED);
- Use the data centre classifications to guide location decisions. For example, due to their criticality, class A data centres may be located in a separate building with a fenced perimeter etc. Based on business needs an organisation may specify the minimum distance, for example a Class C data centre may be in the same building or city as the production site;
- Use the data centre classifications to determine data centre infrastructure, access control and access logging, package, visitor and tape handling requirements. For example, class A data centre may require security staff to monitor activity via CCTV, limited interior and external visibility from the computer and motion detection;
- Ensure that sites processing, storing or handling classified information have secure rooms with an Intruder Detection System (IDS) installed. Security must respond to IDS alerts in a timely manner;
- Ensure that personnel only know of the existence of, or activities within, a secure area on a Need-to-Know basis;
- Avoid unsupervised working in secure areas both for safety reasons and to reduce opportunities for malicious activities;
- Physically lock and periodically check vacant secure areas; and
- Unless authorised for a business purpose, ban the use of photographic, video, audio or other recording equipment, such as cameras on mobile devices in sensitive secure rooms. Based on security needs, users may have to surrender such devices at the security desk when visiting secure areas.

7.5 Equipment Security

In accordance with US ISO/IEC 27001, organisations must protect equipment against physical and environmental threats. The security measures help reduce the risk of unauthorised access to information and loss or damage to equipment. The measures have strong importance to equipment used offsite. Organisations must also protect supporting facilities such as electrical supply and cabling infrastructure. Equipment security aims to achieve the security outcomes below.

PH4 – Organisations must implement appropriate measures to prevent the physical loss, damage, theft or compromise of equipment and infrastructure supporting critical infrastructure. As a minimum requirement, organisations must: (a) locate all production equipment within the access-controlled boundaries of the data centre; (b) protect power and telecom cabling against interception or damage; (c) use reliable electrical power supply; and, (d) manage risks to off-site equipment, information or software.

To achieve the security outcomes mandated above, organisations must:

- Host all production computer systems such as servers, desktops, firewalls, etc in the secure areas of the data centre to prevent unauthorised access;
- Position devices processing sensitive data such as displays in a way that reduces the viewing opportunities of unauthorised persons during their use;
- Protect power lines supporting IT services and telecommunications wiring against unauthorised access, damage or disruption through tapping. Where possible, locate cabling underground and use protective shielding;
- Have in place controls to minimise the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;
- Establish and enforce guidelines for eating, drinking, and smoking in proximity to information processing facilities;
- Monitor environmental conditions, such as temperature and humidity for conditions, which could adversely affect information processing facilities;
- Have in place measures to protect power and telecom cabling against interception or damage by installing lightning protection to all buildings and fitting lightning filters to incoming power and communications lines; and
- Address risk of off-site equipment, information and software in accordance with the guidelines outlined in section 6.10 – Remote Access Security.

7.6 Secure Equipment Disposal & Re-Use

Organisations 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 sanitisation and disposal of storage assets into secure and less secure environments for repair, exchange and recycling. Timely and cost-effective secure equipment disposal and re-use procedures can help achieve the following mandated security outcomes.

PH5 – All organisations must adopt formal procedures to enable the secure disposal and re-use of storage media. To minimise the risk of unauthorised retrieval or reconstruction of erased data, organisations must, as a minimum requirement: (a) define secure disposal criteria; (b) define secure sanitisation levels commensurate with information sensitivity; (c) group storage media that requires the same treatment; (d) define criteria to guide repair, re-use, exchange or physical destruction decisions; (e) validate the success of sanitisation exercises; and, (f) log decommissioning activities.

To achieve the security outcomes mandated above, organisations must:

- Ensure that all media used to store and process sensitive information such as networking devices; magnetic disks and tapes; office equipment; solid state devices (SSDs); and optical disks is sanitised and disposed of in accordance with organisational policies and procedures;
- Have in place policies and processes that define secure sanitisation levels to help all relevant stakeholders understand the degree of wiping required to provide reasonable assurance that data from a decommissioned asset would not be retrieved or reconstructed;
- Adopt a process to guide sanitisation activities including asset classification verification; sanitisation and post-sanitisation activities; validation of the success of the sanitisation activities and final sign-off; and
- Ensure that where it is not possible to destroy assets handling sensitive data securely, procedures are in place to enable their secure storage and/or return to its owner.