DUS 2175

UGANDA STANDARD

First Edition
2019-11-05

Information Security — Requirements for Security Controls

Reference number
DUS 2175: 2019

Compliance with this standard does not, of itself confer immunity from legal obligations

A Uganda Standard does not purport to include all necessary provisions of a contract. Users are responsible for its correct application

The Executive Director
Uganda National Bureau of Standards
P.O. Box 6329
Kampala
Uganda
Tel: +256 414 333 250/1/2/3
Fax: +256 414 286 123
E-mail: info@unbs.go.ug
Web: www.unbs.go.ug

Contents

Page

Foreword v
Introduction vii
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Symbols (and abbreviated terms) 2
5 General Requirements 3
6 Specific Requirements 3
6.1 Security Governance 3
6.2 Information Security 5
6.2.1 General 5
6.2.2 Information Security and Security Governance 6
6.3 Personnel Security 6
6.3.1 General 6
6.3.2 Personnel Security and Risk Management 7
6.4 Physical Security 7
6.4.1 General 7
6.4.2 Physical Security, Governance and Risk Management 7
6.4.3 Physical Security Perimeter 7
Annex A (normative) Security Governance 9
A.1 Information Security Statement requirements 9
A.2 Statement of Information Risk Appetite 9
A.3 Information Security Management 10
A.3.1 Responsibilities of Boards & Accounting Officers 10
A.3.2 Responsibilities of Chief Information Risk Owner (CIRO) 10
A.3.3 Responsibilities of Information Asset Owners 10
A.3.4 Responsibilities of Information Security Coordination Group 11
A.3.5 Responsibilities of Operational Information Security team 11
A.4 Risk Management guide 11
A.5 Dissemination of information 12
A.6 business continuity (BC) and disaster recovery (DR) 12
A.7 Incident Management 13
A.8 Assurance & Compliance 13
Annex B (Normative) Information Security 15
B.1 Information Security Policy 15
B.2 Asset Management 15
B.3 Secure Information Sharing 16
B.4 Supply Chain Security 17
B.5 Access Management 17
B.6 Network Security Controls 18
B.7 Malicious Code Protection 19
B.8 Portable and Removable Media Security 20
B.9 Remote Access Security 21
B.10 Protective Monitoring 22
B.11 Information Back-Ups 23
B.12 information Security Accreditation 23
Annex C (Normative) Personnel governance 25
C.1 information Security Roles & Responsibilities 25

C.2 Baseline Security Clearance Defined 25
C.3 Ongoing Personnel Security Management 26
Annex D (Normative) Physical Security 28
D.1 Physical Security Perimeter 28
D.2 Physical Entry Controls 28
D.3 Internal Data Centre Physical Access Controls 29
D.4 Equipment Security 30
D.5 Secure Equipment Disposal & Re-Use 30
Bibliography 32

.

.

Foreword

Uganda National Bureau of Standards (UNBS) is a parastatal under the Ministry of Trade, Industry and Cooperatives established under Cap 327, of the Laws of Uganda, as amended. UNBS is mandated to co-ordinate the elaboration of standards and is

(a) a member of International Organization for Standardisation (ISO) and

(b) a contact point for the WHO/FAO Codex Alimentarius Commission on Food Standards, and

(c) the National Enquiry Point on TBT Agreement of the World Trade Organization (WTO).

The work of preparing Uganda Standards is carried out through Technical Committees (TC). A Technical Committee is established to deliberate on standards in a given field or area and consists of key stakeholders including government, academia, consumer groups, private sector and other interested parties.

Draft Uganda Standards adopted by the Technical Committee are widely circulated to stakeholders and the public for comments. The committee reviews the comments before recommending the draft standards for approval and declaration as Uganda Standards by the National Standards Council.

The committee responsible for this document is UNBS/TC 18, *[Information and Communication Technology]*.This the first edition DUS 2175:2019, which has been technically developed.

Introduction

Information security enables efficient, effective, safe and secure delivery of crucial public services. Information security also serves broader national security goals by protecting critical information infrastructure (CII) that operate and control the critical national sectors and their physical assets

In reality, many organizations would have to do more than simply apply the basic information security requirements. This is inevitable because protected computers or CII reside in sectors ranging from security, defence, international relations, banking and financial services to public utilities. Hence, organizations should determine the additional information security controls that they need to apply to mitigate, to acceptable levels, the relevant cyber threats. Organizations should reach a decision about the accompanying information security controls by considering their articulated risk appetite, business needs as well as the value, sensitivity and criticality of the information assets under consideration.

The standard is intended to provide reasonable confidence about efforts to protect CII assets nationwide

Information Security — Requirements for Security Controls

1 Scope

This draft Uganda standard specifies requirements for security controls that reduce vulnerability to information security such as cyber and other possible threats affecting protected computers and /or CII. This standard is applicable to public and private organizations that own or operate protected computers.

2 Normative references

The following referenced documents referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

US ISO/IEC 18028-4, *Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access*

US ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

US ISO/IEC 27002*, Information technology -- Security techniques -- Code of practice for information security controls*

US ISO/IEC 27039, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
accounting officer
individual whose responsibility it is to sign off the annual accounts of a Government Department or Office / Body

3.2
board or top management
supreme governing bodies that provide public and private sector organizations guidance on overall policy direction and strategies. They also facilitate, supervise and support the Executive in the implementation of their mandate and strategies.

3.3
cyberspace
interconnected digital environment of networks, services, systems, and processes

3.5
cyber attack
action by an individual or organization to breach a cyberspace

3.6
cyber threat
possibility of malicious attempt that exploits a cyber space

3.7
perimeter
whole area surrounding the building hosting protected computer assets including roads, footpaths and any other areas just outside the building.

3.8
protected computer
computer, program or data used directly in connection with or necessary for information security, defence or international relations of Uganda; law enforcement; the provision of services directly related to communications infrastructure, banking and financial services, public utilities; public key infrastructure and public safety.

3.9
risk appetite
level and type of information risks a given organization is willing to accept, tolerate or survive in the pursuit of its strategic goals.

3.10
sanctions
penalties or other deterrent measures used to enforce obedience with the law, or with rules and regulations.

3.11
sanitisation
general process geared at ensuring that organizations have removed data from storage media to extent mandated by business and security requirements

4 Symbols (and abbreviated terms)

BC -Business Continuity

CII - Critical Information Infrastructures

CIRO- Chief Information Risk Owner

CISO-Chief Information Security Officer

DR-disaster recovery

DVD- Digital Versatile Disc

GoU- Government of Uganda

HR- Human Resource

ICT-Information and Communications Technology

ISMS-Information Security Management System

IT-Information Technology

NISF - National Information Security Framework

PDA- Personal digital assistant

PDCA- Plan Do Check Act

PPDA -Public Procurement and Disposal of Public Assets Authority

SyOps -Security Operating Procedure

USB- Universal Serial Bus

5 General Requirements

5.1.1 The technical head of the organization shall assume ultimate accountability for information security, and for implementing the mandated NISF minimum requirements.

5.1.2 Organizations shall ensure that all users accept collective responsibility for applying proportionate measures to secure information assets.

5.1.3 Individuals shall understand and accept personal responsibility for safeguarding the assets entrusted to them and expect sanctions for breaching information security rules.

5.1.4 Organizations shall adapt information security controls appropriate to their circumstances in particular their business needs, risk appetite, value and sensitivity of their information.

5.1.5 All organizations shall have sound controls to enable the secure sharing of information regardless of its form and mechanism of transfer.

5.1.6 Organizations shall only hire staff after verifying that their character and personal circumstances are such that they can be trusted with access to vital Information Technology (IT) assets.

5.1.7 Organizations shall build capacity to withstand and recover from cyber-attacks and disruptions in a timely manner with minimal damage

6 Specific Requirements

6.1 Security Governance

Security governance focuses on all the activities required to manage a functional area namely information, personnel and physical security, and follow a PDCA cycle illustrated below

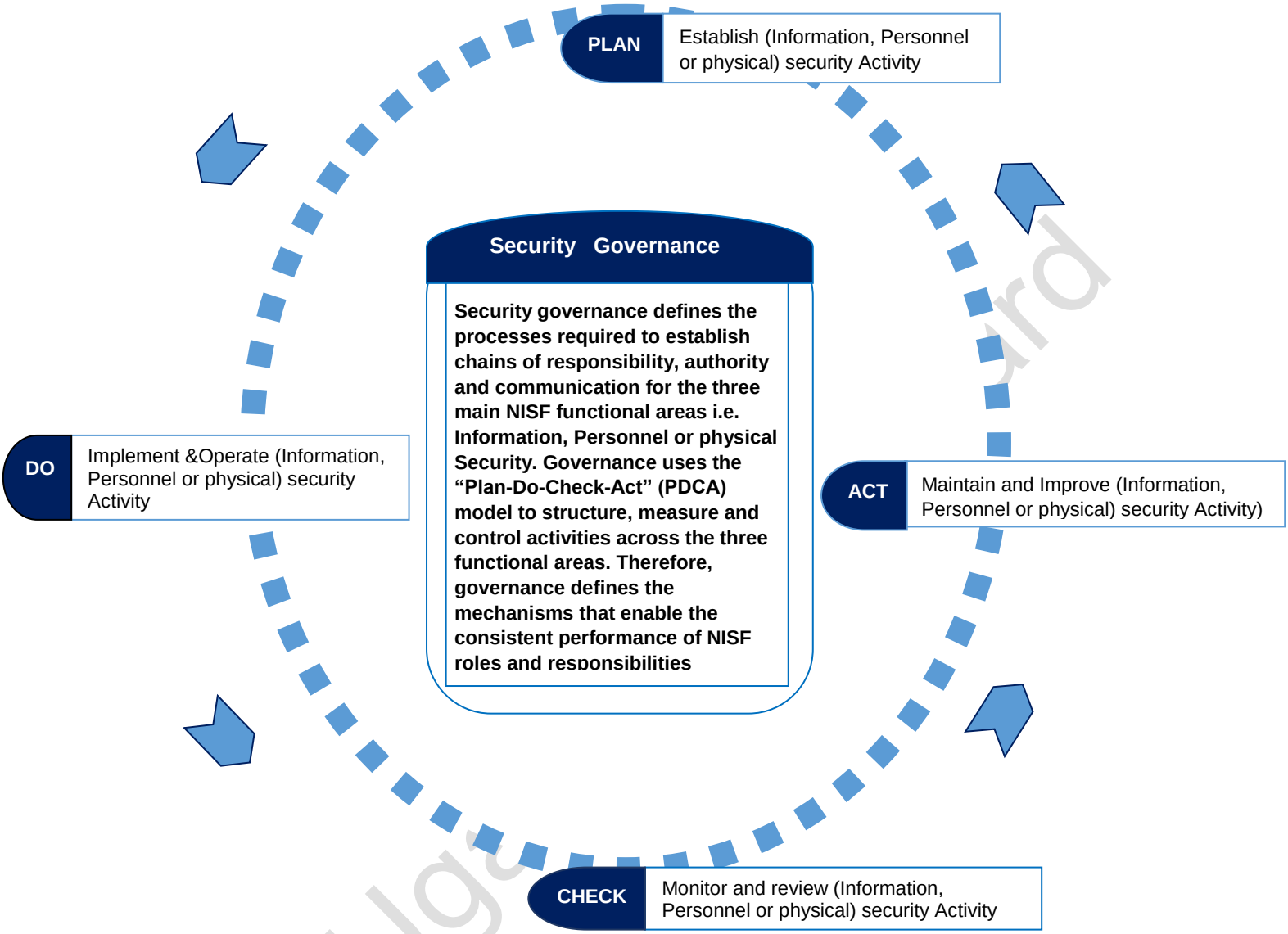

Figure 1 — Security Governance and PDCA Model

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

6.1.1 Boards or top management shall issue a policy statement on information security with requirements outlined in annex A.1, which underline the importance of information risk management to effective and secure operations.

6.1.2 The Board or top management shall articulate organizational information Risk Appetite in a statement given in annex A.2

6.1.3 All organizations with protected computers shall establish suitable information security management arrangements with clearly defined accountability at all levels outlined in annex A.3 by

a) Setting up an ISMS in accordance with US ISO/IEC 27001. The organization shall also adopt the PDCA model to structure all ISMS processes;

b) Having in place an internal information security organization that is fully compliant with US ISO/IEC 27001; and

c) Assigning roles and responsibilities to different individuals within the company following the minimum requirement in A.3.1 to A.3.5

6.1.4 All organizations with protected computers shall adopt a formal, consistent and policy-guided risk management approach to help ensure the security of protected computers following minimum information security requirements mandated in annex A.4

6.1.5 Organizations shall ensure that all users – including Ministers, Board members, senior executives, employees and third party users – obtain security awareness before gaining access to protected computers in order to foster an organizational culture that values, protects and handles information assets safely. As a minimum requirement, the awareness shall follow annex A.5.

6.1.6 All organizations shall 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 stipulated in annex A.6.

6.1.7 All organizations with protected computers shall have a formal security incident management process to enable the accurate and timely identification, communication, investigation and response to security events and weaknesses following minimum requirement in annex A.7

6.1.8 Organizations shall provide reasonable assurance that their security arrangements mitigate risks to protected computers adequately. Using a range of compliance mechanisms, organizations shall follow the minimum requirement in annex A.8

6.2 Information Security

The information security mandatory minimum-security requirements apply to:

a) Public and civil servants, contractors, consultants, temporary employees, guests and volunteers. The requirements also apply to third parties that access and use GoU information or information systems;

b) 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;

c) All information assets including those 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; and

d) 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.

6.2.1 General

All organizations shall commit to:

a) Achieve high standards of Information Security governance;

b) Treat information security as a critical business issue and create an information security-conscious environment;

c) Demonstrate to third parties that it deals with information security in a proactive manner; and

d) Apply the general requirements outlined in clause 5 such as implementing controls that are proportionate to risk.

6.2.2 Information Security and Security Governance

The themes contained in sub-clause 6.1 apply to the information security functional area in the same way as personnel and physical security. For example, the information security area shall have effective leadership; adopt a credible risk management approach; conduct effective awareness, education and training; handle information security incidents and institute assurance and compliance reporting mechanisms. Moreover, all information security functional areas shall adopt the PDCA continuous improvement model to structure their processes. The mandatory minimum information security requirements are as follows:

6.2.2.1 Management shall draft, obtain Board-approval and publish an information security policy that addresses the NISF mandatory minimum requirements outlined in annex B.1 in terms of the organization's business requirements, threat environment and risk appetite.

6.2.2.2 All organizations shall ensure that assets associated with protected computers receive the level of protection appropriate to their value, sensitivity and criticality by following requirements in annex B.2

6.2.2.3 All organizations, particularly those within and/or connecting to Government, shall 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, organizations shall follow annex B.3

6.2.2.4 All organizations shall mitigate risks of intentional and unintentional supply chain compromise following minimum requirement in annex B.4.

6.2.2.5 Organizations shall ensure that only users, processes and devices with a business need and suitable security clearances gain access to protected computers. As a minimum requirement, access management shall follow annex B.5.

6.2.2.6 All organizations shall apply technical security controls appropriate to the protected computer's value, sensitivity and criticality. As a minimum requirement, the controls shall follow annex B.6.

6.2.2.7 All organizations with protected computers shall apply appropriate controls against malicious code by following annex B.7

6.2.2.8 All organizations using portable and removable media shall adopt formal procedures to prevent the unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities by following minimum requirement in annex B.8

6.2.2.9 All organizations shall implement appropriate security measures to mitigate remote access risks by following minimum requirement in annex B.9

6.2.2.10 All organizations shall implement measures to detect, and tie to users, unauthorised information processing activities by following minimum requirement in annex B.10

6.2.2.11 All organizations shall adopt formal policies and procedures to backup and regularly test copies of information and software required to recover from major disruptions by following minimum requirement in annex B.11

6.2.2.12 all protected Government computers shall be accredited and the mandated minimum information security outcomes in annex B.12 would assure stakeholders that the organization has identified and adequately addressed major risks to the system.

6.3 Personnel Security

6.3.1 General

People are the most important asset for any organization. However, people can also become big threat sources and actors. This clause of the standard outlines the steps that organizations shall take to establish the

trustworthiness, integrity and reliability of individuals before granting them access to sensitive CII or protected computer assets.

6.3.2 Personnel Security and Risk Management

The themes contained in in sub-clause 6.1 apply to the personnel security functional area in the same way as information and physical security. The personnel security area requires a credible risk management approach as follows.

6.3.2.1 To reduce the risk of theft, fraud or misuse of facilities, organizations shall ensure that all users understand their information security responsibilities by following annex C.1.

6.3.2.2 All organizations shall 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 protected computers by following minimum requirements in annex C.2

6.3.2.3 Individuals requiring access to computers necessary for Uganda's security, defense, diplomacy, public safety, public utilities and economic stability shall undergo national security vetting thus as minimum requirements, organization shall follow annex C.3

6.4 Physical Security

6.4.1 General

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. Physical security measures work alongside and indeed are the bedrock of other areas of security such as information and personnel security.

6.4.2 Physical Security, Governance and Risk Management

The themes contained in sub-clause 5.2 apply to the physical security functional area. 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 organizational security programme. Like other areas of security, physical security also complies with the mandated minimum requirements on risk management contained in the governance section of this standard. Thus, good physical security measures match business and security needs.

6.4.3 Physical Security Perimeter

Organizations need to put in place an adequate physical perimeter around sensitive information processing facilities to stop unauthorised physical access. 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 shall align with business needs and be cost-effective. By minimising the risk of theft, destruction and unauthorised access, the security perimeter can help achieve the following mandated minimum information security outcomes.

6.4.3.1 All organizations shall have appropriate security perimeters to shield facilities hosting protected computers against a range of physical security threats including crime, natural disasters and acts of terrorism by following minimum requirement in annex D.1

6.4.3.2 Organizations shall use appropriate entry controls to protect secure areas against physical security threats by following minimum requirement in annex D.2.

6.4.3.3 Organizations shall implement appropriate internal physical security controls to defend protected computers against physical attacks by following minimum requirement in annex D.3:

6.4.3.4 Organizations shall implement appropriate measures to prevent the physical loss, damage, theft or compromise of equipment and infrastructure supporting protected computers by following minimum requirement inannex D.4

6.43.5 All organizations shall adopt formal procedures to enable the secure disposal and re-use of storage media. To minimize the risk of unauthorized retrieval or reconstruction of erased data, organizations shall follow minimum requirement in annex D.5.

Annex A
(normative)

Security Governance

A.1 Information Security Statement requirements

The Statement shall:

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 or top management'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 information security responsibilities.

f) Explain why information security matters and outline policy objectives;

g) Require all employees (including contractors) to comply with the Statement.

h) Assign Accounting Officer accountability for information security

A.2 Statement of Information Risk Appetite

The statement shall:

a) Explicitly note the Board or top management's Risk Appetite in relation to information risk;

b) Map the risk appetite on a spectrum e.g. low to very high, averse to hungry;

c) Address information risk's relationship with corporate goals in the same way as other risks e.g. legal, financial, operational, compliance and reputational;

d) Require that all project proposals and plans demonstrate consistency with the articulated information Risk Appetite;

e) Be read and understood in conjunction with risk management strategy;

f) Assign monitoring responsibility usually to the Audit Committee; and

g) Be reviewed, debated and agreed at least annually.

A.3 Information Security Management

As a minimum requirement:

a) The Accounting Officer shall accept personal accountability for embedding information risk management into the Internal Control system;

b) A senior executive shall assume overall responsibility for information risk management at Board or top management level;

c) Organization shall establish a senior management committee to coordinate information risk management;

d) Heads of business divisions shall assume responsibility for named information assets;

e) Every system shall have a single responsible officer; and

f) Organizations shall appoint trained staff to information security roles.

A.3.1 Responsibilities of Boards & Accounting Officers

At Board or top management level, the information security organization shall perform the following roles:

a) Treat information risk as a corporate-level risk;

b) Review information risk position at least quarterly; and

c) Explicitly address information risk management in Annual Reports.

A.3.2 Responsibilities of Chief Information Risk Owner (CIRO)

The information security organization shall appoint a Board or top management level official to the role of CIRO with responsibilities including:

a) Ownership of a plan to foster a culture of information security;

b) Accountability for organizational risk management policy;

c) Alignment of risk management programme with business processes;

d) Advising on risk parts of Statement on Internal Control;

e) Ensuring that all assets have skilled and empowered owners; and

f) The production of quarterly and annual risk assessments.

The choice of the CISO for the CIRO role would help ensure that the Board or top management receives timely and effective advice about the business impacts of their strategic and operational security decisions.

A.3.3 Responsibilities of Information Asset Owners

Information asset owners shall be heads of division, department, directorate or equivalent unit and perform the following functions:

a) Understanding and supporting the organization’s information security culture;

b) Knowing the information that the assets under their responsibility hold;

c) Knowing who accesses the assets under their responsibility and why;

d) Identifying and mitigating risks to the assets under their responsibility;

e) Ensuring that assets under their responsibility are available for business use;

At least annually, providing the CIRO reasonable assurance that the assets under their responsibility are secure. This shall be in form of a checklist that details all the assets, their condition, and date of inspection. This inspection shall therefore be periodic customised to the needs of the organization

A.3.4 Responsibilities of Information Security Coordination Group

Led by the CIRO, the information security coordinators shall perform the following functions:

a) Ensure that effective information risk management processes are in place;

b) Approve organizational information security policies and standards;

c) Monitor compliance with agreed information security policies and standards; and

d) Encourage the professionalization of all information security areas.

A.3.5 Responsibilities of Operational Information Security team

Led by CISO or similar role, the operational information security team shall perform the following functions:

a) Implement the organization’s information risk policy;

b) Follow approved information security policies and standards;

c) Enforce information security requirements on all departments including suppliers; and

d) Identify and report non-compliance.

A.4 Risk Management guide

All organizations shall:

a) Use the board or top management issued information Risk Appetite as a guide for routine risk management decisions to ensure that the organization avoids taking either too much or too little risk in pursuit of its business goals;

b) Identify business critical assets and the impact of their compromise or loss;

c) Have in place a Risk Register to record, support and audit risk management decisions by identifying risk owners, risk treatments and residual risks; and

d) Have a suitable information risk policy to address threat sources and actors;

e) Prioritise risks; and

f) Manage information risks during the ICT system's development, acceptance, operational and decommissioning and disposal phases.

A.5 Dissemination of information

As a minimum requirement, the awareness shall:

a) Undertake information security induction training for all employees, including contractors and subcontractors, to ensure that they are conversant with organizational security policies and procedures as well as their personal responsibility for securing and safeguarding assets under their control and/or supervision;

b) Allocate sufficient resources to finance a sustained user information security awareness training programme, as well as technical training addressing all relevant risks, threats and vulnerabilities, acceptable usage, impacts of successful cyber-attacks, incident response actions and the personal consequences of breaching information security rules;

c) Avail information security policies to all staff, including contractors, internally;

d) Ensure that all staff, including contractors, obtain appropriate briefings about how legislation identified in this standard among others the Official Secrets, the Access to Information, the Computer Misuse, the Electronic Signatures and the Electronic Transactions Acts affects their work activities and articulate potential penalties for breaching information security rules;

e) Provide information security cleared staff training matching with their access privileges;

f) Ensure that staff performing information security roles receive suitable training; and

g) Formally assess and regularly review and re-evaluate the effectiveness of information security awareness, education and training activities in light of a changing threat environment.

A.6 business continuity (BC) and disaster recovery (DR)

As a minimum requirement, organizations shall have in place:

a) Address information security needs of organizational BC;

b) Establish the criticality of different facilities, systems, sites and networks by performing a business impact analysis of the unavailability of each asset;

c) Identify and assess the probability and the information security impacts of events that could cause interruptions to business operations e.g. fire, theft;

d) Adopt a common BC planning framework to ensure that all plans address information security requirements consistently;

e) Ensure that continuity plans support correct information security levels;

f) Test, audit and update BC plans regularly to ensure their effectiveness in an event of an emergency; and

g) Put in place up-to-date and effective DR plans for critical ICT systems to minimise the impact of adverse information security incidents.

h) Put in place a BC management strategy that takes a long-term view of organizational continuity needs;

i) Put in place a policy outlining management direction and support for business continuity;

j) Put in place a BC and DR plans for all locations; and

k) Put in place a Systematic BC/DR testing, reporting and maintenance procedures for all protected computers.

A.7 Incident Management

All organizations shall:

a) Obtain board or top management endorsement and accountability for incident management processes as part of the holistic BC management strategy approval;

b) Define roles and responsibilities;

c) Include tested policies, plans and procedures;

d) Ensure staff obtain specialist incident response training;

e) Have in place channels for reporting information security events to management;

f) Require all staff, including contractors, to note and report observed or suspected information security weaknesses in systems or services;

g) Have in place quick, effective, and orderly response to information security incidents;

h) Put in place effective mechanisms for quantifying and monitoring the types, volumes, and costs of information security incidents;

i) Promote an incident reporting culture adopting procedures for reporting information security incidents to bodies responsible for information security; and

j) Ensure that the collection, retention and presentation of data about information security incidents comply with relevant rules of evidence to enable follow-up action.

A.8 Assurance & Compliance

Organizations shall

a) Provide the Board or top management an assessment of the information risk position, including that of the supply chain, at least quarterly;

b) Undertake an annual information security assessment against the NISF and approved information security policies declaring compliance status;

c) Disclose areas of non-compliance with the NISF to their line Minister, Auditor General's Office, information security organizations 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.

f) Provide evidence to the board or top management as to how its information security operations comply with US ISO/IEC 27002.In particular, the organization shall produce a Statement of Applicability showing the controls implemented;

g) Make information risk management a regular item on the Board's or top management's agenda;

h) Disclose to the Board the main information security risks affecting vital business assets in quarterly and annual assessments;

i) Add ensuring compliance with information security policies and standards, in one's area of responsibility, to a manager's performance evaluation criteria;

j) Establish a programme to check regularly that information systems comply with technical security implementation standards. In particular, the technical compliance checks shall seek to identify and report insecure configurations; unauthorised installations; changes to system and application configuration;

k) Have in place a comprehensive audit regime that includes penetration testing and system security audits to identify and report potential gaps in the information security of operational systems;

l) Have in place a process for informing the Board or top management and Accounting Officer about additional information security requirements in an event of newly identified information security threats and vulnerabilities; and

m) Have in place an effective process for showing the compliance of information security activities with all statutory, regulatory, and contractual requirements.

Annex B
(Normative)
Information Security

B.1 Information Security Policy

The policy shall:

a) Explain how the organization 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.

e) Define the purpose, scope and approach to managing information security within the organization;

f) Identify and assign suitable information security roles and responsibilities depending on the size, structure, business needs and threats to the organization;

g) Require the creation of a manual guiding the implementation of an ISMS in compliance with US ISO/IEC 27001;

h) Contain or refer to a manual detailing how to apply information, personnel and physical security measures consistently across the organization;

i) Contain or reference a guide that explains the secure working practices that all users shall adopt to comply with information security policies and related documents;

j) Require the generation of evidence showing that the organization uses the information security accreditation process to identify and manage risks to ICT systems;

k) Outline the required BC roles, processes and procedures;

l) Specify penalties for breaching the policy and related information security measures;

m) Be publicised and made readily available to all staff; and

n) Specify a review cycle in order to ensure its continued applicability.

B.2 Asset Management

All organizations shall:

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 board or top management issued information Risk Appetite as a guide for routine risk management decisions to ensure that the organization avoids taking either too much or too little risk in pursuit of its business goals;

d) Have in place a Risk Register to record, support and audit risk management decisions by identifying risk owners, risk treatments and residual risks; and

e) Use the Security Classification Standard to determine the acceptable procedures for labelling, handling,

f) Audit the asset register regularly; and

g) Inform the Board of the main information security risks affecting vital business assets.

h) Conduct an inventory of assets drawing up and maintaining a register of important assets as a prerequisite to risk management;

i) Ensure that designated divisions own and secure named information assets;

j) Identify, document and apply rules of acceptable use of information assets;

k) Label and handle information assets throughout their lifecycle according to the Security Classification Standard; and

l) Use business impact of loss – resulting from the value, legal requirements, sensitivity, and criticality – to determine asset labelling and handling levels.

B.3 Secure Information Sharing

Organizations shall:

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.

f) Ensure that users are fully conversant and comply with approved information exchange policies, procedures, controls and relevant national legislation;

g) Use cryptographic solutions to provide users and applications the underlying “trust” to operate authentication, integrity, confidentiality and non-repudiation information security services to protect collaborative tools and information exchanges;

h) Establish exchange agreements that require parties seeking access to other organizations ICT systems to have in place information security measures that match the information security classification and handling requirements for the asset;

i) Ascertain that exchange agreements with external parties are enforceable;

j) Confirm that receiving parties grasp and are complying with their obligations to protect information assets appropriately;

k) Adopt policies to handle information assets received from foreign countries and international bodies in line with applicable treaties and arrangements;

l) Abide by their own obligations under exchange agreements such as codes of connection (CoCos) and memoranda of understanding (MoUs); and

m) Obtain authorisation before granting third parties access to ICT systems owned by another organization.

B.4 Supply Chain Security

All organizations shall:

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 information security clauses in service contracts;

d) Ensure that the computer networks, products and services supplied do not introduce information security risk;

e) Assess compliance with requirements at least annually; and

f) Enforce sanctions for non-compliance.

g) Identify and evaluate the information security risks related to outsourcing or offshoring before letting contracts for protected computer systems and services;

h) Recognise that they retain accountability for managing their information risks even where they outsource ICT system and services delivery;

i) Ensure that they are fully acquainted and compliant with the national security impact assessment process for ICT suppliers;

j) Abide by PPDA instructions to identify, document and incorporate security requirements into outsourcing contracts with suppliers and contractors;

k) Require the contractor to present an operational security management plan outlining their strategy for reducing information security risks to acceptable levels;

l) Outline the process for the development and maintenance of procedures, processes, instructions and plans for securing the system;

m) Issue Security Aspects Letters (SAL) regularly to update contractors on the information security conditions that govern their access to protected computer assets;

n) Require the supplier to obtain organizations approval for their physical facilities before the hosting organization’s protected computer systems and services; and

o) At least annually, obtain independent assurance that suppliers or contractors comply with the mandated NISF requirements and other information security policies.

B.5 Access Management

As a minimum requirement, access management shall:

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 organizations to deter, detect, resist and defend against accidental or deliberate unauthorised actions; and

e) Enable regular review of access rights.

f) Define and document business requirements for access control and restrict access to protected computers to those who satisfy these requirements;

g) Adopt an access control policy that enforces the principle of least privilege;

h) Restrict and control the allocation and use of privileges in accordance with the Need-to-Know principle;

i) Select and apply a suitable access control model amongst Discretionary, Role Based and Mandatory Access Control;

j) Apply the principle of uniform access management i.e. use of authentication and authorisation services to control resource use;

k) Have in place a formal process for user password management;

l) Implement a process for ensuring that users are aware of and abide by their information security responsibilities for maintaining effective access controls, particularly regarding to passwords and the information security of user equipment;

m) Enforce the outcomes of the user access rights review; and

n) Harden and lockdown user software applications such as web browsers and office productivity applications to stop threat actors exploiting vulnerabilities.

B.6 Network Security Controls

As a minimum requirement, the controls shall include:

a) A formally documented information 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.

g) Adopt an information security architecture that provides end-to-end network security by enabling the detection, identification and correction of information security vulnerabilities;

h) 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;

i) Enforce sufficient segregation, zoning or variable depth information security to separate specific areas of the network, groups of information services and information systems handling data of different classification levels;

j) Implement boundary protection measures for shared networks, especially those extending across organizational boundaries, in compliance with the access control policy and requirements of the business applications;

k) Enforce network routing controls to ensure that connections and information flows do not breach the access control policy of the business applications;

l) Apply the principle of service minimisation consistently across the network by disabling services that do not satisfy business and information security needs for access;

m) Adopt solutions that use techniques such as encryption to offer converged voice, data and video packets protection appropriate to their information security needs;

n) Adopt the “defence in depth” or “layered" approach to network security through the use of different technical security controls and information security products to mitigate information security threats collectively;

o) In accordance with ISO/IEC 27039 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

p) Build survivability into networks to ensure that solutions 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.

B.7 Malicious Code Protection

All organizations shall:

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 information security policy; and

f) Address published technical vulnerabilities in a timely manner.

g) Mandate that all users, regardless of location, abide by a malicious code policy that shall define the requirements for antivirus signature update; regular system scanning; file attachment handling; file sharing; removable media scans; virus log generation and review;

h) Identify and block all direct (e.g. e-mail attachments, social media, malicious websites) and indirect (unauthorised personal laptops, PDA, USB, CD/DVD) mechanisms/routes that threat actors could use to inject malicious code;

i) 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;

j) Use measures such as logically segregated environments (i.e. sandboxes) and application-specific controls to manage the execution of mobile code;

k) Install host-based software to scan, clean, quarantine and raise alerts about suspicious files, including malicious websites, prior to access;

l) Provide users suitable awareness training about the impacts, preventative measures and actions to take in an event of a malicious code attack;

m) Routinely patch ICT systems, information security enforcing products and applications against known vulnerabilities to reduce exposure to malicious code;

n) Conduct regular vulnerability assessments to identify potential weaknesses that could enable the introduction of malicious code;

o) Build adequate capacity to identify, deter, resist and defend against known and unknown (zero-day) malicious code attacks; and

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

B.8 Portable and Removable Media Security

All organizations shall:

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 information 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.

i) Lock down host devices to stop users changing default configurations and thereby enabling malicious actors to execute privileged commands;

j) Use full disk hardware encryption for devices processing sensitive data;

k) Ensure that users understand that maintaining physical custody of the device is the best form of defence;

l) Not allow the use of privately-owned devices to process, store or remotely access protected computers, programs and data except in emergency, short term situations where it is not practical to issue official equipment;

m) Prevent devices that do not comply with organizational policy such as use of a hardened configuration from connecting to the corporate network;

n) Give users appropriate training in handling authentication credentials such as encryption keys, hardware tokens, smartcards and passwords;

o) Defend against random and targeted attacks by requiring users to power off devices when not in use; never leaving devices unattended; storing information security credentials separately from device; amongst other measures;

p) Minimise data aggregation risks by ensuring that the devices only store data required to perform approved business activities at any given time;

q) Adopt anti-virus 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

r) Make sure that users are conversant with mobile device incident response and reporting procedures such as when to report device loss to the Police.

B.9 Remote Access Security

All organizations shall implement appropriate information security measures to mitigate remote access risks. As a minimum requirement, organizations shall:

a) Adopt a formal remote access policy;

b) Assess the risks, threats and vulnerabilities of remote access;

c) Use information 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

f) Align remote access policy with incident management plans.

g) Adopt a formal remote access policy that defines roles and responsibilities for management, users, administrators and information security personnel guided by business needs, conditions, threats and the impacts of information security breaches;

h) Consider the communication media out of control and possibly in a hostile environment and 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;

i) Enforce a remote access policy requirement that users only gain access to network services to which they have obtained specific authorisation to use;

j) Grant remote access only for as long as is necessary for business purposes;

k) Use encryption of suitable strength to secure communication links and the content they process against eavesdropping. In addition, apply encryption on remote access clients to make them inaccessible if they are lost or stolen;

l) Ensure that users accept and comply with the information Security Operating Procedures (SyOPs) for mobile devices such as powering off devices when not in use and storing authentication credentials separate from the device given that portable and removable media devices usually enable remote access;

m) 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.;

n) Provide the remote access server satisfactory security including protection against unauthorised physical access; assured power supply; secure set-up; configuration and administration; back-up and recovery procedures;

o) Present a formal risk assessment and obtain approval from Mo ICT&NG before permitting the remote administration of protected computers, programs and data from overseas locations given the risk posed by threat actors and sources such as foreign intelligence services to such access;

p) Ensure that remote access solutions, including contracts with IT suppliers, comply with any 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 information security of the State or interfere with the right to the privacy of any other person;

q) Submit remote access solutions to a formal information security accreditation process to provide assurance about adequacy and the enforcement of information e.g. baseline builds; personnel and physical security controls in the context of the unique threats, vulnerabilities and risks such solutions face; and

r) Sanitise and dispose of remote access devices in accordance with the NISF Secure Equipment Disposal and Re-Use requirements.

B.10 Protective Monitoring

All organizations shall define a monitoring strategy;

a) Adopt an accounting and audit policy;

b) Produce, and preserve for an agreed time, audit logs recording user activities, exceptions, faults and information security events;

c) Establish procedures for reviewing monitoring results;

d) Train staff to interpret monitoring results;

e) Protect audit and logging facilities and log data; and

f) Align protective monitoring with incident management and HR policies.

g) Define and adopt a protective monitoring strategy that defines the objectives, approaches and resources required to support consistent organization-wide accounting, audit and monitoring activities;

h) 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;

i) Ensure that the network security architecture contains suitable features to identify, record, alert and generate information security audit reports;

j) Ensure that accounting activities match the level of logging for each information security classification. IT teams shall not deviate from the accounting requirements before presenting a risk assessment and convincing management that the new level of logging adequately assures the information security of business activities;

k) Standardise accounting and audit log data to ease correlation in accordance with ISO/IEC 27002;

l) Have in place effective procedures to review recorded logs and alerts to help identify and hold to account those who misuse information assets;

m) Hire and maintain a competent team to administer the technological solutions and supporting infrastructures that collect, store and log suspicious events;

n) 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;

o) Where possible, deny system administrators the access privileges to erase or de-activate logs of their own activities;

p) Separate accounting and audit logs that support routine information security activities from evidential logs that have legal ramifications because they might contain intrusive and confidential personal data and may be admissible in Court;

q) 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;

r) Have in place a process for escalating to management representatives' alerts from real-time accounting and audit to enable decisions on whether to trigger the incident management process; and

s) Update the accounting and audit policy to reflect changes in threats and results of technical risk assessments more accurately.

B.11 Information Back-Ups

All organizations shall define the required back-up levels;

a) Base the frequency of back-ups on the value, criticality and sensitivity of data;

b) Produce accurate and complete records of back-up copies;

c) Store back-up data a safe distance away from the main site;

d) Afford back-up information suitable physical and environmental protection; and

e) Test back-up media regularly to ensure its recoverability.

f) Define the extent (e.g. full or differential backup) and frequency of backups that reflect business requirements as well as information security and criticality of the information to the continued operation of the organization;

g) Regularly test back-up arrangements for individual information systems to help ensure that they meet the requirements of BC plans;

h) Back-up activities for critical systems should cover all systems information, applications and data needed to recover the entire system in the event of a disaster;

i) Regularly check and test restoration procedures to help ensure that their effectiveness and whether they can be completed within the time allotted in the operational procedures for recovery; and

a) Apply appropriate safeguards to maintain mandated information security properties for the back-ups such as the use of encryption to maintain confidentiality.

B.12 information Security Accreditation

Organizations shall:

b) Accept and retain accountability for accreditation;

c) Ensure that every IT project has a senior responsible owner;

d) Define an accreditation boundary;

e) Develop an accreditation roadmap;

f) Create accreditation plans;

g) Record all procedures, processes, instructions and plans for securing the system;

h) Conduct suitable system acceptance testing notably penetration testing; and

i) Identify through-life accreditation costs.

j) Adopt the ISO/IEC 27002 controls set, select appropriate and applicable countermeasures to reduce risks;

k) Agree approach to measuring compliance with the NISF with the accreditor;

l) Show compliance with the corporate policies and legislation applicable to the system's security accreditation scope;

m) Describe how the information security accreditation process met applicable business and information security requirements;

n) Demonstrate how the risk management strategy for the system helped establish the business impact of compromising the security of key assets;

o) Assess threats and risks to the information system, develop a risk treatment plan and countermeasures against identified risks; and

a) Present a detailed plan for managing information security risks to the system throughout until decommissioning. The plan shall show that the development process followed secure practices to prevent errors, loss, unauthorised modification or misuse of data in applications.

Annex C
(Normative)
Personnel governance

C.1 information Security Roles & Responsibilities

Organizations shall:

a) Communicate information security expectations to all employment candidates;

b) Include information security duties in the employment contracts that all staff shall agree and sign;

c) Require staff to sign and abide by information SyOps for specified protected computers or services;

d) Inform staff that non-compliance with the signed information security documents may lead to disciplinary action; and

e) Enforce sanctions for non-compliance including dismissal and prosecution.

a) Require all employees, including contractors and subcontractors to accept their information security roles and responsibilities formally. The acceptance shall include an undertaking to:

1) Protect assets under their control and/or supervision from unauthorised access, disclosure, modification, destruction and interference;

2) Comply with information security processes and activities; and

3) Report information security events or potential events or other security risks to the organization;

b) Ensure that individuals agree to abide by all organizational policies, standards, protocols and guidelines for protecting information, personnel and physical assets against information security threats regardless of type and origin; and

c) Confirm that, as part of the human resource (HR) process, all employees, including contractors and subcontractors, accessing and/or operating organizations' protected computers sign declaration forms acknowledging their obligation to abide by the Official Secrets Act, 1964 during and after their employment.

C.2 Baseline Security Clearance Defined

All organizations shall satisfactorily validate the identity of all applicants;

a) Confirm academic, employment and financial records;

b) Undertake criminal record checks;

c) Establish that applicants are entitled to undertake the employment in question; and

d) Record and risk manage cases where it is impossible to perform all the required checks.

e) Ensure that HR processes do not allow anyone to commence work on CII projects without undergoing appropriate recruitment checks;

f) 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;

g) Establish whether the applicant has the right to work in Uganda including meeting residency requirements based on the sensitivity of the position;

h) Check the candidate's employment record by validating the completeness and accuracy of the curriculum vitae;

i) Obtain satisfactory characters references about the applicant e.g. one business and one personal;

j) Establish whether the applicant is qualified for the job by confirming the claimed academic and professional qualifications; and

k) Based on risk assessment, determine whether the applicant is liable to undergo additional national security vetting.

C.3 Ongoing Personnel Security Management

All organizations shall:

a) Maintain a record of information 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 organizations vetting agencies of any significant changes in personal circumstances may lead to disciplinary action;

e) Undertake periodic information security appraisals;

f) Investigate anything that may affect an individual's suitability to access protected computers; and

g) Sanction noncompliance.

h) Maintain up to date personnel security records of security cleared individuals as well as refused and withdrawn security vetting applications;

i) Ensure that security clearances undergo regular review and/or when material facts or changes come to light to ensure that records are updated and reaffirm the individual's suitability to hold a security clearance at a given level;

j) 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 shall understand that vetting organizations would regard any failure to disclose material and security relevant changes to personal circumstances as unreliability to the detriment of their security clearances;

k) Line managers and other staff have a duty to work with HR to identify report and investigate significant changes to individual behaviours, personal circumstances and attitudes to risk. Common warning signs include drug and alcohol abuse, changes in working patterns, lateness etc.;

l) 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 require performing their jobs. In keeping with the mandated access management security outcome, organizations shall review the appropriateness of access rights regularly; and

m) Have in place formal processes for investigating suspected noncompliance with information security rules. Any such investigations, legal or disciplinary cases shall comply with relevant laws, regulations and ethics.

Annex D
(Normative)
Physical Security

D.1 Physical Security Perimeter

All organizations shall:

a) Allocate physical security roles to facilities hosting protected computers. In common with information and personnel security, the CIRO shall have overall responsibility for physical security risk management at Board-level. He shall also appoint a Security Controller to oversee day-to-day information 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 identified risks;

b) Have in place a physical security policy that describes in appropriate detail how the organization shall define, apply and evidence physical security controls in all its locations in accordance with US ISO/IEC 27001;

c) Ensure that no classified organization data is processed, stored or transmitted to and from any facility without a full risk assessment and formal approval from the organization's client and relevant national security agencies. Conduct physical security risk assessments before site selection;

d) 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 such as fire;

e) 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. Design into or require changes to a site's security;

f) 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;

g) Ensure that the perimeters are physically sound with no gaps to enable easy break-in. In addition, external walls of the site shall be of solid construction with all external doors suitably protected against unauthorised access with control mechanisms, e.g. bars, alarms, locks etc.; and

h) Ensure that the organization's Physical Security Standard and referenced material therein are the main source of guidance on physical security matters.

i) Have effective access controls;

j) Log and review access;

k) Prepare for, detect and respond to physical incidents.

D.2 Physical Entry Controls

Organizations shall have:

a) 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.

e) 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, organizations shall mandate the use of access cards for out-of-hours access to buildings;

f) Ensure that all visitors report to the information security reception and produce proof of identification before gaining access to sensitive facilities. The visitors shall sign-in and sign-out and shall wear an appropriate badge i.e. unescorted or escorted at all times;

g) Record the date and time of entry and departure for all visitors. In addition, visitors shall only gain access for specific and authorised purposes. Visitors shall also receive a briefing on the security procedures of the area including emergency procedures;

h) Control and restrict access to areas designated for processing or storing sensitive information to authorised persons only. Organizations shall have in place authentication controls e.g. access control card plus PIN to manage and validate access and securely maintain an audit trail of all access;

i) Require all staff and visitors to wear some form of visible identification. All staff at the facility have a duty to notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

j) Grant third party support service personnel restricted access to secure areas or sensitive facilities when required only and monitor the access; and

k) Regularly review, update and revoke access rights to secure areas when necessary.

D.3 Internal Data Centre Physical Access Controls

Organizations shall implement appropriate internal physical security controls to defend protected computers against physical attacks. As a minimum requirement, organizations shall 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.

D.4 Equipment Security

Organizations shall:

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.

e) of the data centre to prevent unauthorised access;

f) Position information processing facilities handling sensitive data in a way that reduces the viewing opportunities of unauthorised persons during their use;

g) Isolate and accord the required level of protection to assets that require special protection;

h) 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;

i) 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;

j) Establish and enforce guidelines for eating, drinking, and smoking in proximity to information processing facilities;

k) Monitor environmental conditions, such as temperature and humidity for conditions, which could adversely affect information processing facilities;

l) 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

m) Address risk of off-site equipment, information and software in accordance with the guidelines outlined in sub clause 7.10 – Remote Access Security.

D.5 Secure Equipment Disposal & Re-Use

All organizations shall

a) Adopt a process to guide secure sanitisation activities including asset classification verification; sanitisation and post-sanitisation activities; validation of the success of the sanitisation activities and final sign-off;

b) 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 organizational policies and procedures;

c) 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 will not be retrieved or reconstructed;

d) Ensure that where it is not possible to destroy assets handling sensitive data securely, procedures shall be in place to enable their secure storage and/or return to its owner

e) Define secure disposal criteria;

a) Define secure sanitisation levels commensurate with information sensitivity;

b) Group storage media that requires the same treatment;

c) Define criteria to guide repair, re-use, exchange or physical destruction decisions;

d) Validate the success of sanitisation exercises; and Log decommissioning activities

Bibliography

[1] Executive Handbook

[2] Uganda (1964), *The Official Secrets Act, The Government of Uganda, Entebbe, Uganda*.

[3] Uganda (1987), *The Security Organizations Act, 2005, The Government of Uganda, Entebbe, Uganda*.

[4] Uganda (2005a), *"The Access to Information Act, 2005", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda*

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

[6] Uganda (2006), *The Police (Amendment) Act, 2006, The Government of Uganda, Entebbe, Uganda*

[7] Uganda (2009a), *"The National Information Technology Authority, Uganda Act, 2009", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda.*

[8] Uganda (2009b), *The National Security Council Act, The Government of Uganda, Entebbe, Uganda*

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

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

[11] Uganda (2011b), "*The Electronic Signatures Act, 2011", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda*

[12] Uganda (2011c), *"The Electronic Transactions Act, 2011", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda*

Certification marking

Products that conform to Uganda standards may be marked with Uganda National Bureau of Standards (UNBS) Certification Mark shown in the figure below.

The use of the UNBS Certification Mark is governed by the Standards Act, and the Regulations made thereunder. This mark can be used only by those licensed under the certification mark scheme operated by the Uganda National Bureau of Standards and in conjunction with the relevant Uganda Standard. The presence of this mark on a product or in relation to a product is an assurance that the goods comply with the requirements of that standard under a system of supervision, control and testing in accordance with the certification mark scheme of the Uganda National Bureau of Standards. UNBS marked products are continually checked by UNBS for conformity to that standard.

Further particulars of the terms and conditions of licensing may be obtained from the Director, Uganda National Bureau of Standards.

ICS nn.nnn.nn

Price based on nn pages