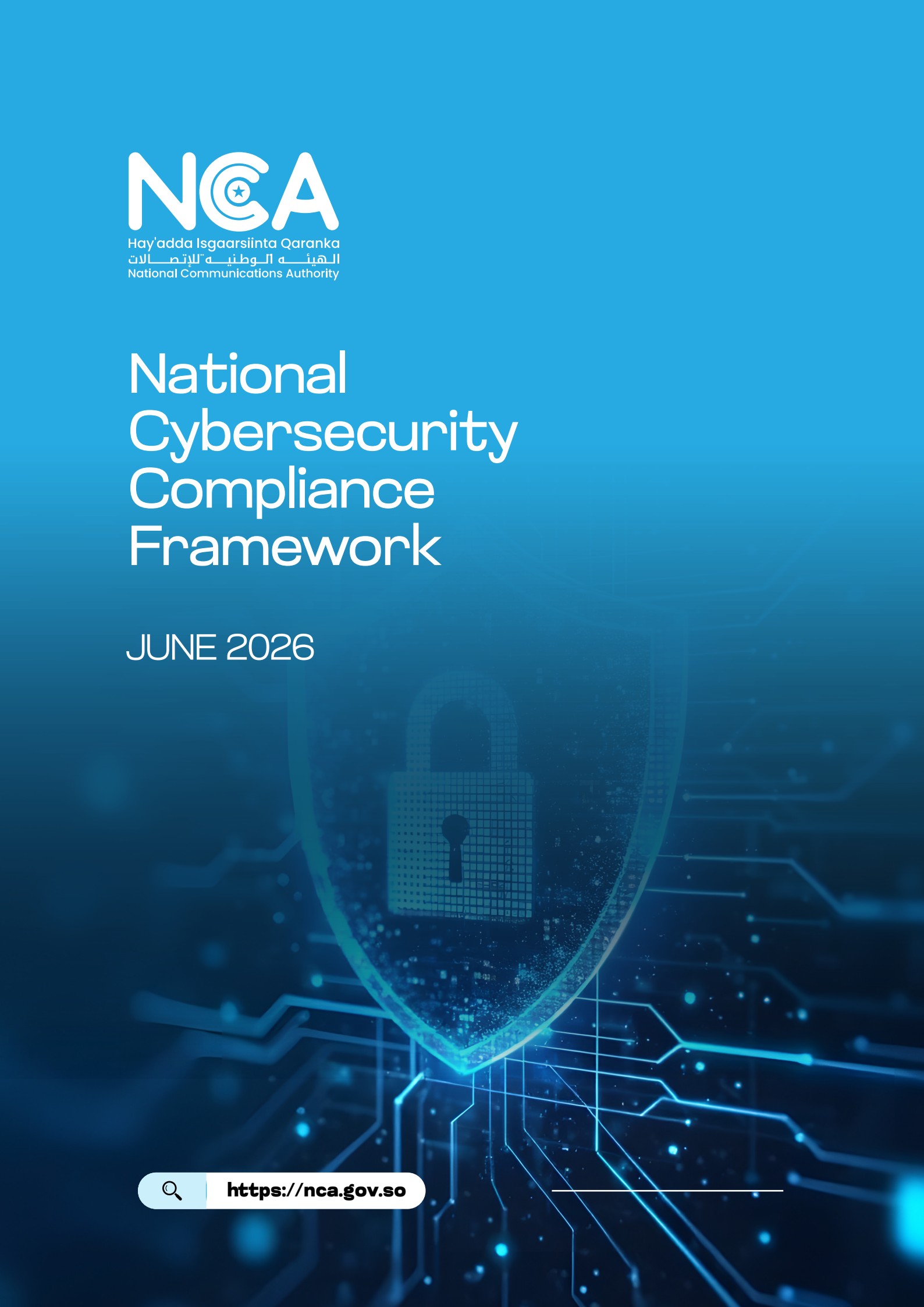
Hay'adda Isgaarsiinta Qaranka
الهيئة الوطنية للإتصالات
National Communications Authority

National Cybersecurity Compliance Framework

JUNE 2026



https://nca.gov.so

H.E. Mr. Mohamed Adam Moalim (Soomaali) Minister,

Ministry of Communication and Technology (MoCT)
Federal Republic of Somalia

Somalia's digital transformation and technological advancement is driven by the rapid adoption of digital services, mobile technologies, and innovation across government institutions, the private sector, and critical sectors. This growing digital ecosystem has further underscored the importance of strengthening cybersecurity measures to protect Critical Information Infrastructure, safeguard sensitive information, and maintain public trust and confidence in digital services. The Federal Government of Somalia remains firmly committed to building a secure, resilient, and trusted digital environment that supports national development, economic growth, and innovation.

In this regard, the National Communications Authority (NCA), continues to play a central role in strengthening Somalia's cybersecurity posture through the development the regulatory frameworks, cybersecurity awareness initiatives, technical capacity-building programmes, and national incident response capabilities, including the operationalization of SOMCERT. These efforts reflect the Government's commitment to enhancing national cybersecurity governance and protecting the country's digital infrastructure.

The National Cybersecurity Compliance Framework represents a significant milestone in strengthening Somalia's cybersecurity governance and regulatory landscape. The Framework establishes mandatory baseline cybersecurity requirements and compliance obligations for public and private sector institutions to enhance cybersecurity resilience, protect Critical Information Infrastructure, and promote accountability across all sectors. Developed in alignment with international standards and best practices, while taking into consideration Somalia's national priorities and operational environment, the Framework provides a structured approach for implementing effective cybersecurity controls and fostering a strong culture of cybersecurity compliance and continuous improvement. The successful implementation of this Framework requires strong collaboration and commitment from government institutions, private sector organizations, operators of Critical Information Infrastructure, and all relevant stakeholders. Cybersecurity is a shared national responsibility, and collective efforts are essential to safeguarding Somalia's digital ecosystem and strengthening trust and confidence in digital services nationwide.

I would like to commend and express my sincere appreciation to the National Communications Authority (NCA) and all stakeholders who contributed to the development of this important Framework. Their dedication and continued efforts are instrumental in advancing Somalia's national cybersecurity agenda and strengthening the resilience of the country's digital environment.

I therefore call upon all relevant public and private sector institutions and stakeholders to fully support and implement this Framework in order to strengthen Somalia's cybersecurity resilience and ensure a secure, trusted, and resilient national digital ecosystem.

Mr. Mustafa Yasin Sheikh

Director General National Communications Authority

As Somalia continues to advance its digital transformation across government, business, and society, the importance of establishing a strong and effective cybersecurity compliance framework has become critical. The growing dependence on digital platforms, interconnected systems, and online services requires organizations to comply with established cybersecurity requirements, standards, and regulatory obligations to protect Critical Information Infrastructure, secure sensitive data, and maintain public confidence in digital services.

The National Communications Authority (NCA) is committed to strengthening Somalia's cybersecurity posture through the development and enforcement of robust regulatory frameworks. The National Cybersecurity Compliance Framework represents a significant milestone in this effort. It establishes mandatory cybersecurity compliance requirements, baseline security controls, implementation guidelines, and regulatory obligations necessary to ensure that institutions across both the public and private sectors operate in a secure, accountable, and compliant manner.

This Framework has been carefully developed in alignment with international cybersecurity standards, best practices, and regulatory principles, while taking into consideration Somalia's national priorities, operational environment, and technological landscape. It provides organizations with a structured and measurable approach to cybersecurity compliance, enabling them to assess their level of compliance, implement appropriate security controls, and demonstrate accountability in fulfilling cybersecurity obligations. Furthermore, the Framework promotes consistency, transparency, regulatory oversight, and continuous enhancement of cybersecurity compliance practices across all sectors. The Cybersecurity Compliance Framework also strengthens the responsibilities of both regulators and regulated entities by ensuring that cybersecurity compliance becomes an integral component of organizational governance, operations, and service delivery rather than merely a procedural requirement. Through compliance assessments, audits, reporting obligations, monitoring mechanisms, and capacity-building initiatives, the NCA will work closely with stakeholders to support effective implementation, regulatory adherence, and sustained compliance nationwide.

The National Communications Authority is confident that the National Cybersecurity Compliance Framework will serve as a vital instrument for strengthening cybersecurity compliance, enhancing regulatory enforcement, promoting accountability, and increasing trust and confidence in Somalia's digital ecosystem. Its implementation will contribute significantly to the protection of national digital infrastructure and support the realization of a secure, resilient, and trusted digital future for Somalia.

Table of Contents

ABBREVIATIONS

BC	Business Continuity
BS	Baseline Security
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
CII	Critical Information Infrastructure
CISO	Chief Information Security Officer
CoCos	Codes of Connection
DR	Disaster Recovery
HR	Human Resources
ICT	Information and Communication Technology
IDS	Intruder Detection System
IS	Information Security
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Protection System
PDCA	Plan-Do-Check-Act
PIN	Personal Identification Number
SOMCIRT	Somalia Computer Incident Response Team

1 Introduction

1.1 Overview

This document establishes the National Cybersecurity Compliance Framework, which defines the mandatory baseline cybersecurity controls that all public and private sector organizations that use, own, and/or operate Critical Information Infrastructure (CII) shall implement to reduce their exposure and vulnerability to cyber threats. The implementation of the security measures prescribed under this Framework will strengthen the ability of organizations to prevent, respond to, and recover from cybersecurity incidents and cyber-attacks.

1.2 Applicability of the National Cybersecurity Compliance Framework

As noted above, this Framework is mandatory for all public and private sector organizations that use, own, and/or operate Critical Information Infrastructure (CII). The Somalia Cybersecurity Act (2026) defines CII as tangible and intangible digital assets, networks, and information systems designated by the National Communications Authority as essential to national security, economic stability, public safety, or the protection of the public interest. Official communications generally possess a lower level of security sensitivity than information processed or stored within CII systems. However, the loss, theft, compromise, or unauthorized disclosure of official communications may still result in significant operational, legal, reputational, or administrative consequences for Ministries, Departments, and Agencies (MDAs). Furthermore, the Data Protection Act (2023) defines personal data as any information relating to an identified or identifiable individual, whether directly or indirectly, by reference to identifiers such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual.

1.3 Framework Review Cycle

The National Communications Authority will review this Framework every three (3) years to ensure that it remains relevant to evolving business requirements, emerging cyber threats, technological developments, and national approaches for preventing, detecting, responding to, and mitigating cybersecurity risks.

1.4 Structure of National Cybersecurity Compliance Framework

The framework presents a set of mandatory baseline cybersecurity requirements organized under the following four categories:

Security Governance

Information Security

Personnel Security

Physical Security

1.5 Adaptation of Security Controls

It is important to emphasize that the requirements contained in this Framework define baseline security controls only. In reality, organizations will need to implement security measures beyond these baseline requirements to address their specific operational, regulatory, and risk management needs. Accordingly, organizations shall adapt and enhance the security controls prescribed by this Framework based on their operational environment, threat landscape, and sector-specific risks. Such adaptation is necessary because Critical Information Infrastructure (CII) exists across multiple sectors with varying business functions, technologies, and risk exposures. Therefore, organizations shall identify and implement additional security controls necessary to reduce cyber risks to acceptable levels relevant to their business activities and operational context. Decisions regarding the appropriate level of security controls should be informed by the organization's risk appetite, business requirements, legal and regulatory obligations, and the value, sensitivity, and criticality of the information assets and systems concerned.

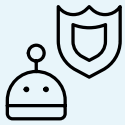
1.6 Authority

The duties and responsibilities of the National Communications Authority, established under Article 4 of the National Communications Act, 2017, were expanded under the Somalia Cybersecurity Act, which designates the Authority as the lead institution responsible for the governance and management of national cybersecurity. Accordingly, all designated Critical Infrastructure Operators are required to implement this Framework and submit annual copies of their risk assessment report to the Authority.

1.7 Applicable Legislation

The following legislation underpins this National Cybersecurity Compliance Framework:

2023 Data Protection Act



2026 Cybersecurity Act

2 Framework Context

The Federal Government of Somalia recognizes cybersecurity as a strategic pillar and enabler for the efficient, effective, safe, and secure delivery of public services. Cybersecurity also enhances the national security and resilience objectives through the protection of Critical Information Infrastructure (CII).

3 Guiding Principles

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

3.1 Top Leadership Accountability

The first principle is that the most senior person in the organization shall assume ultimate accountability for cybersecurity and ensure compliance with the reporting obligations and reporting cycle established under the Somalia Cybersecurity Act.

3.2 Collective Responsibility

This principle requires all individuals to accept a collective responsibility to support efforts aimed at ensuring that CII assets and services receive protection commensurate with their value, sensitivity, and criticality to their organizations.

3.3 Personal Accountability

Individuals shall 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

Organizations shall adapt security controls to their operational circumstances in particular their business needs, risk appetite, and the value, sensitivity, and criticality of their information assets.

3.5 Secure/Assured Sharing

This principle requires organizations to apply appropriate security controls to enable the secure sharing of information regardless of its form, classification and method of transmission.

3.6 Suitable, Trustworthy and Reliable Staff

Organizations shall only hire staff after verifying their character and personal circumstances are such that they can be trusted with access to critical IT assets and systems.

3.7 Resilience

This principle requires organizations to develop and maintain the capability to withstand, respond to, and recover from cybersecurity incidents and operational disruptions in a timely manner while minimizing operational, financial, and reputational impact.

4 Security Governance

4.1 Introduction

Security governance encompasses all activities required to manage the core security domains, namely information security, personnel security, and physical security. This Framework adopts the ISO/IEC 27001 **Plan-Do-Check-Act (PDCA)** continuous improvement model to structure and guide cybersecurity governance processes, as illustrated below.

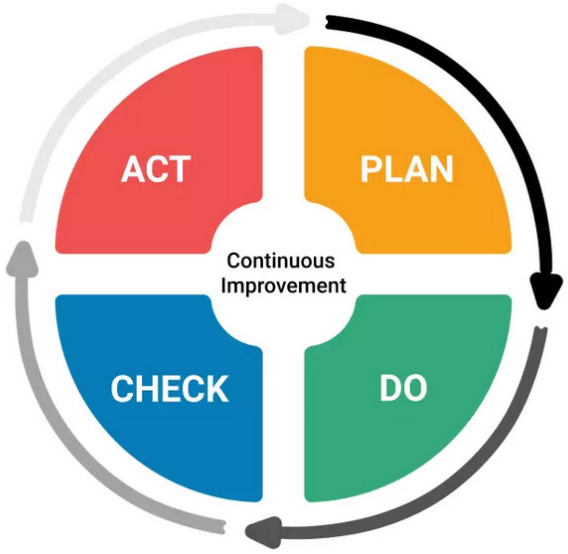


Figure 1 – PDCA Model

Governance aims to ensure that cybersecurity programmes support and align organizational and business goals. Thus, mandatory baseline security governance requirements are as follows:

4.2 Policy Statement on Cyber Security

Given that executive management within CII organizations must address all the major risks affecting their organizations, it is crucial that they issue a formal policy statement on cybersecurity. The purpose of the statement is to underline the importance of cyber risk management to effective and secure operations.

GV1 – All executive management of organizations with critical information infrastructure shall issue a Cybersecurity Policy Statement. As a minimum requirement, the Statement shall:

a) Recognize information as a critical organizational asset;

b) Acknowledge cyber risk management as a business enabler and an integral part of good corporate governance;

c) Contain Executive Management's acceptance of ultimate accountability for cyber risk management;

d) Set clear direction on cyber risk management by determining Risk Appetite; and

e) assign cybersecurity roles and responsibilities to management and employees.

To achieve the security outcomes mandated above, organizations shall:

4.2.1 Issue Policy Statement on Cyber Security

The policy statement on cyber security:

» Recognizes CII as a critical organizational asset;

» Explains why cyber security matters and outlines policy objectives;

» Reflects Executive Management's commitment to protecting organizational information against all threats, whether internal or external, deliberate or accidental;

» Assigns a senior role with accountability for cybersecurity; and

» Requires all employees (including contractors) to comply with the Statement.

4.2.2 Articulate Cyber Risk Appetite

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

» Explicitly note the Executive Management'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 cyber risk's relationship with organizational goals in the same way as other risks e.g. legal, financial, operational, compliance and reputational;

» Assign monitoring responsibility, typically to the Audit Committee; and

» Be reviewed, debated and agreed at least annually.

4.3 Cyber Security Organization

Organizations must have an effective governance structure to manage their cybersecurity activities. The Executive Management must establish such an organization with a view of achieving the mandatory minimum cybersecurity outcomes set out below.

GV2 – All organizations with CII must establish suitable cybersecurity governance arrangements with clearly defined accountability at all levels. As a minimum requirement:

a) The Executive Management must accept personal accountability for embedding cyber risk management into the organization's Internal Control systems;

b) A senior executive must assume overall responsibility for cyber risk management at Board level;

c) The organization must establish a senior management committee to coordinate cyber risk management;

d) heads of business divisions must assume responsibility for identified information assets;

e) every system must have a single responsible officer assigned; and,

f) organizations must appoint appropriately trained personnel to security roles.

To achieve the security outcomes mandated above, it is recommended that CII organizations do the following:

» Set up an Information Security Management System (ISMS) in accordance with ISO/IEC 27001. The organization shall also adopt the "Plan-Do-Check-Act" (PDCA) model to structure all ISMS processes; and

» Create an information security organization that is fully compliant with the requirements of ISO/IEC 27001

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

4.3.1 Responsibilities of Executive Management

The cybersecurity governance structure must perform the following roles at the Executive Management level:

» Treat cyber risk as an organisational risk;

» Review the organisation's cyber risk posture in accordance with the reporting requirements of the Somalia Cybersecurity Act; and

» Explicitly address cybersecurity and cyber risk management in annual reports.

4.3.2 Responsibilities of Information Risk Owner

The Executive Management shall appoint a senior official to the role of Chief Information Security Officer (CISO) with responsibilities including:

» Ownership of a plan to foster a culture of cybersecurity awareness;

» Accountability for the organization's cybersecurity programme;

» Alignment of the cyber risk management programme with organizational business processes;

» Ensuring that all information assets have skilled and empowered owners; and

» Overseeing the preparation of quarterly and annual cyber risk assessments.

4.3.2.1 Choice of Chief Information Security Officer (CISO)

It is important to stress that the CISO is a functional role and not necessarily a formal job title. As such, organizations may appoint an individual with the appropriate authority, experience, and expertise to perform this role. Appointing a CISO helps ensure that Executive Management receives timely and effective advice on the cybersecurity implications of strategic and operational decisions.

4.3.3 Responsibilities of Information Asset Owners

Information asset owners shall be heads of divisions or departments and shall perform the following functions:

» Understand and support the organization's cybersecurity culture;

» Know what information is held within the assets under their responsibility;

» Know who has access to the assets under

their responsibility and the purpose of such access;

» dentify and mitigate risks to the assets under their responsibility;

» Ensure that the assets under their responsibility are available for business use; and

» Provide the CISO with reasonable assurance, at least annually, that the assets under their responsibility are secure.

4.3.4 Responsibilities of Security Coordination Group

Led by the CISO, the Security Coordination Group shall perform the following functions:

» Ensure that effective cyber risk management processes are in place;

» Approve organizational cybersecurity policies and standards;

» Monitor compliance with approved security policies and standards; and

» Promote the professionalization of all cybersecurity functions.

4.3.5 Responsibilities of Operational Security team

Led by CISO or an equivalent role, the operational security team shall perform the following functions:

» Implement the organization's cybersecurity policies, standards and guidelines;

» Enforce cybersecurity requirements on all stakeholders including suppliers;

» Identify and report non-compliance with security policies and rules; and

» Report incidents to the Somalia Computer Incident Response Team (SOMCIRT)

4.4 Awareness, Education and Training

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

GV4 – Organizations must ensure that all users obtain cybersecurity awareness before gaining access to CII. As a minimum requirement, the awareness must: (a) as part of the induction process, explain to staff the cybersecurity risks associated with their work;

a) help staff gain awareness of the organization's cybersecurity policies;

b) remind staff of their personal responsibility for safeguarding assets entrusted to them;

c) Outline potential penalties for breaching security rules;

d) Be formally assessed formally; and;

e) Be conducted at least annually.

To achieve the security outcomes mandated above, organizations must:

- Conduct cybersecurity induction training for all employees, including contractors and subcontractors, to ensure that they are conversant with organizational cybersecurity

policies and procedures as well their personal accountability for securing assets under their control and/or supervision;

» Allocate sufficient resources to support a sustained user security awareness and education programme covering relevant cyber risks, threats and vulnerabilities; acceptable use; the impacts of cyberattacks, incident response procedures, and the personal consequences of breaching security rules;

» Make cybersecurity policies and procedures available to all staff, including contractors;

» Provide security-cleared personnel with training appropriate to their access privileges;

» Ensure that staff performing security roles receive appropriate cybersecurity training; and

» Regularly review and evaluate the effectiveness of security awareness and education activities in light of the evolving threat environment.

4.5 Business Continuity and Disaster Recovery

Business continuity activities aim to ensure that the organization has the capacity to withstand disruptions to critical business operations and thereby achieve the mandatory minimum-security outcomes outlined below.

GV5 – All organizations must implement appropriate Business Continuity (BC) and Disaster Recovery (DR) programmes to minimize the impact of and ensure the timely recovery from disruptions that may result from natural disasters, accidents, equipment failures and deliberate actions. As a minimum requirement, organizations must have in place:

a) a BC management strategy that takes a long-term view of organizational continuity requirements;

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, organizations must:

» Address the information security requirements of organizational 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 impact 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 appropriate information security levels;

» Test, audit and update business continuity plans regularly to ensure their effectiveness in the event of an emergency;

» Maintain up-to-date and effective disaster

recovery plans for critical infrastructure systems to minimize the impact of security incidents; and

» Report on BC/DR activities at least annually.

4.6 Incident Management

Incident management aims to demonstrate that the organization is minimizing the likelihood and impact of security incidents and ensuring the timely restoration of business activities in line with the mandatory minimum security outcomes outlined below.

GV6 – All organizations with CII must have a formal cybersecurity incident management process to enable the accurate and timely identification, communication, investigation and response to security incidents and weaknesses in line with procedures established by the SOMCIRT. 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 receive specialist incident response training;

e) promote a security incident reporting culture; and,

f) identify, monitor, analyze and learn from security incidents.

To achieve the security outcomes mandated above, organizations must:

» Obtain Executive Management endorsement for incident management processes as part of the overall business continuity management strategy approval;

» Have in place channels for reporting security incidents 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 security incidents;

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

» Adopt procedures for reporting security incidents to the SOMCIRT; and

» Ensure that the collection, retention and presentation of data relating to security incidents comply with relevant rules of evidence to support follow-up actions.

4.7 Assurance and Compliance

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

GV7 – Organizations must provide reasonable assurance that their security arrangements mitigate risks to critical infrastructure adequately. Using a range of compliance mechanisms, organizations must, as a minimum requirement:

a) provide the Executive Management with an assessment of the cyber risk position, including supply chain risks, at least quarterly;

b) undertake an annual security assessment against this framework and approved security policies and declare their compliance status;

c) disclose areas of non-compliance with the framework to relavsnt Executive Management in a classified annual report;

d) address information risk within Statements of Internal Control; and,

e) address information risk management issues including risks, actions and incidents in the Annual Report.

To achieve the security outcomes mandated above, organizations must:

- Provide evidence demonstrating how their security operations comply with this framework
- Disclose to the Executive Management the main security risks affecting vital business assets in quarterly and annual assessments;
- Include responsibility for ensuring compliance with security policies and standards within managers' performance evaluation criteria;
- Establish a programme to check regularly verify that information systems comply with technical security implementation standards. In particular, the technical compliance checks must identify and report insecure configurations; unauthorized installations; changes to system and application configurations;
- 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 Executive Management in the event of newly identified security threats and vulnerabilities; and
- Have in place an effective process for demonstrating compliance of security activities with all statutory, regulatory, and contractual requirements.

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 operation and success of government and private sector organisations. Therefore, organisations must protect the information they handle internally and share with external partners. Ensuring the confidentiality, integrity, and availability of information is a corporate-level responsibility, as security incidents can adversely affect organisational reputation, legal standing, and the ability to conduct business operations.

5.1.1 Government information security commitment

The Government is committed to:

- Treating information security as a critical business issue and creating a security-awareness environment;
- Demonstrating to third parties that it manages information security proactively; and
- Applying the guiding principles outlined in section 3 such as, including the implementation of controls proportionate to risk.

5.1.2Applicability of information security requirements

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

- All staff within organizations with CII including contractors, consultants and temporary employees. The requirements also apply to third parties that access

and use of information handled by the critical infrastructures.

» All forms of information that is written, printed on paper, stored electronically or optically, transmitted by courier or using electronic means, recorded on magnetic disk or tape, or communicated verbally; and

» All information assets including those used by public and private sector critical infrastructure organizations under license or contract. This includes information in any form or media, as well as all computer hardware, software, and communications networks owned, operated, or managed by the organizations or on their behalf.

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 they apply to 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 must apply 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 when it is published, implemented, audited and regularly updated to reflect organizational requirements. A security policy aims to achieve the following mandated minimum-security requirements:

IS1 – Executive management must establish an information security policy that addresses the mandatory minimum requirements in line with the organization's business requirements, threat environment and risk appetite. As a minimum requirement, the policy must:

a) explain how the organization and its supply chain protect information and physical assets;

b) apply to all the activities linked to protection of information systems and computing resource;

c) define acceptance and compliance arrangements by its staff and the supply chain;

d) undergo regular review to ensure its continued relevance and effectiveness

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

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

» Identify and assign suitable security roles and responsibilities based on the organization's size, structure, business needs and threats environment;

» Require the creation of a manual guiding the implementation of an ISMS in compliance with applicable standards and policies;

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

» Contain or reference a guide that explaining the secure working practices that all users must adopt to comply with security policies and related documents;

» Require the generation of evidence demonstrating that the organization

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 breaches of the policy and related security measures;

» Be publicized and made readily available to all staff; and

» Specify a review cycle to ensure its continued applicability and effectiveness.

5.3 Asset Management

Organizations must achieve and maintain appropriate protection for information assets. Effective asset management helps achieve the mandatory minimum security outcomes outlined below.

IS2 – All organizations 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 organizations must:

a) use approved criteria to create and maintain a definitive register of business critical facilities, systems, sites and networks;

b) designate a suitably empowered owner for every asset;

c) use a Security Classification Framework to determine the appropriate procedures for labelling, handling, transmitting, storing and decommissioning assets;

d) audit the asset register regularly; and;

e) inform the Executive Management of the main security risks affecting vital business assets.

To achieve the security outcomes mandated above, organizations must:

» Conduct an inventory of their assets, establish and maintain a register of important assets as a prerequisite for risk management;

» Ensure that designated divisions own and secure identified information assets;

» Identify, document and enforce rules governing the acceptable use of information assets; and

» Label and handle information assets throughout their lifecycle.

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 CII organizations must require internal and external entities to demonstrate compliance with approved security policies before sharing or allowing connections to protected computer assets. As a minimum requirement, organizations must:

a) identify and record risks associated with external parties;

b) establish information exchange policies and procedures;

c) use formal information exchange agreements such as codes of connection and memoranda of understanding;

d) assess the compliance of exchange partners at least annually or when required; and,

e) disconnect or terminate information sharing with non-compliant entities.

To achieve the security outcomes mandated above, organizations 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 with the

underlying "trust" required to support authentication, integrity, confidentiality and non-repudiation security services for protecting collaborative tools and information exchanges;

- Establish exchange agreements requiring parties seeking access to critical infrastructure to have in place security measures commensurate with the security classification and handling requirements for the asset;
- Ascertain that exchange agreements with external parties are legally enforceable;
- Confirm that receiving parties understand and comply with their obligations to protect information assets appropriately;
- Adopt policies for handling information assets received from foreign countries and international bodies in line with applicable treaties and arrangements;
- Comply with obligations under exchange agreements such as Codes Of Connection (CoCos) and memoranda of understanding (MoUs); and
- Obtain authorization before granting third parties access to information and ICT systems owned by another organization.

5.5 Supply Chain Security

All organizations increasingly source ICT systems and software from a global network of suppliers, distributors and business partners. This global ICT supply chain offers advantages such as competitive prices, innovative products and flexibility. However, there is clear evidence that global ICT supply chains have increased risks to system and software security. Therefore, supply chain security measures aim to help achieve the mandatory minimum-security outcomes outlined below.

IS4 – All organizations must mitigate risks of intentional and unintentional supply chain compromise. As a minimum requirement, organizations must:

a) establish consistent supply chain security processes with clear lines of accountability;

b) ensure that suppliers are subject to, and successfully complete, a national security impact assessment;

c) include appropriate security clauses in service contracts;

d) ensure that supplied computer networks, products and services supplied do not introduce information security risks;

e) assess compliance with security requirements at least annually; and,

f) enforce sanctions for non-compliance.

To achieve the security outcomes mandated above, organizations must:

- Identify and evaluate the security risks related to outsourcing or offshoring before awarding contracts for critical infrastructure systems and services;
- Recognize that they retain accountability for managing information security risks, even where the ICT systems and services are outsourced to third parties;
- Ensure that they are fully acquainted and compliant with the national security impact assessment process for ICT suppliers;
- Require contractors to present an operational security management plan outlining their strategy for reducing security risks to acceptable levels; and
- Outline the processes for the development and maintenance of procedures, processes, instructions and plans for securing information systems.

5.6 Access Management

Access management focuses on controlling who is granted access to critical infrastructure. At its core, access management, or access control, aims to ensure that access to information, information processing facilities, and business processes is granted solely based on business and security requirements. Consequently, access control aims to achieve the minimum security outcomes outlined below.

IS5 – Organizations must ensure that only users, processes and devices with a legitimate business need and appropriate security clearances granted access to critical infrastructure. As a minimum requirement, access management must:

a) follow a formal access control policy linked to Human Resource (HR) processes;

b) use formal access registration, modification and revocation processes;

c) require appropriate identification and authentication techniques for all IT systems;

d) enable organizations to deter, detect, resist and respond to accidental or deliberate unauthorized actions; and,

e) Support the regular review of access rights.

To achieve the security outcomes mandated above, organizations must:

» Define and document business requirements for access control, and restrict access to critical infrastructure to individuals and entities that satisfy those 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 implement an appropriate access control model, including Discretionary Access Control (DAC), Role-Based Access Control (RBAC), or Mandatory Access Control (MAC);

» Apply the principle of uniform access management, i.e. the use of authentication and authorisation services to control access to resources;

» Have in place a formal process for user password management;

» Ensure that users are aware of, and comply with, their responsibilities for maintaining access controls, including passwords;

» Enforce the recommendations arising from access rights reviews, e.g. disabling unnecessary or inactive user accounts; and

» Harden and secure 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 minimum security outcomes outlined below.

IS6 – All organizations 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 cybersecurity protection;

b) the segregation of networks handling information of different business impact classifications;

c) the enforcement of service minimization principles;

d) the use of centralized authentication and authorization services;

e) the matching of security levels with information protection needs; and,

f) the adoption of the defense-in-depth security principle.

To achieve the security outcomes mandated above, organizations must:

» Adopt a security architecture that provides end-to-end network security by enabling the detection, identification, and remediation of security vulnerabilities;

» Ensure that users are granted access to network services, e.g. web browsing and file upload services, only where there is a legitimate business requirement for such access;

» Enforce sufficient network segregation, zoning, or layered security controls to separate network segments, information services, and information systems handling data of different security classification levels;

» Implement boundary protection measures for shared networks, particularly those extending across organizational boundaries, in compliance with the access control policy and business application requirements;

» Enforce network routing controls to ensure that network connections and information flows do not violate the access control policy governing business applications;

» Apply the principle of service minimization consistently across the network by disabling services that do not meet business and security requirements;

» Adopt solutions that use techniques such as encryption to provide protection for converged voice, data, and video communications appropriate to their security requirements;

» Adopt the "defense-in-depth" or layered approach to network security through the use of multiple technical security controls and security products to collectively mitigate security threats;

» Install Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS) to monitor network traffic for unusual or suspicious activity and prevent cyberattacks; and

» Build survivability into networks to ensure that technical solutions continue to deliver a minimum level of essential functionality in a timely manner, even where parts of the network are unreachable or have failed due to an attack.

5.8 Malicious Code Protection

Malicious code, such as viruses, worms, ransomware, spyware, and Trojan horses, remains a common attack vector used by threat actors seeking unauthorized access to sensitive ICT systems and the information they process, store, and transmit. Threat actors use techniques such as malicious e-mail attachments, compromised websites, instant messaging platforms, chat rooms, and social media to deceive users into accessing malicious links or content. Malicious code exploits vulnerabilities in ICT hardware, software, and applications to compromise security. Therefore, understanding malicious code risks and implementing appropriate security countermeasures can help achieve the mandatory minimum security outcomes outlined below.

IS7 – All organisations with critical infrastructure must apply appropriate controls against malicious code. As a minimum requirement, organisations must:

a) assess the risks associated with malicious code;

b) adopt a malicious code protection policy that considers organisational business requirements and the prevailing threat environment;

c) deploy appropriate malicious code detection and prevention mechanisms;

d) educate users on malicious code risks and safe security practices;

e) ensure that authorised mobile code complies with the organisation's security policy; and

f) address published technical vulnerabilities in a timely manner.

To achieve the security outcomes mandated above, organizations must:

» Mandate that all users, regardless of location, comply with a malicious code protection policy which, among other requirements, mandates the installation of anti-virus or anti-malware software on all devices, regular updates of anti-virus or anti-malware signatures, system scanning, secure handling of file attachments, secure file sharing, removable media scanning, and the generation and review of malicious code logs;

» Identify and block all direct and indirect malicious code attack vectors, including e-mail attachments, social media content, and malicious websites;

» Ensure that network boundary devices have the capability to inspect inbound and outbound traffic and content for malicious code, including viruses, worms, Trojan horses, and mobile code such as Java, JavaScript, ActiveX, or other executable code capable of compromising networks, applications, and data;

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

» Install host-based security software to scan, quarantine, clean, and generate alerts for suspicious files and malicious content prior to access;

» Provide users with appropriate security awareness and education on the impacts of, preventive measures against, and response actions for malicious code attacks;

» Routinely patch ICT systems, security enforcement products, and applications against known vulnerabilities to reduce exposure to malicious code;

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

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

» Maintain effective and up-to-date contingency, recovery, investigation, and reporting procedures to enable timely response to malicious code incidents.

5.9 Portable and Removable Media Security

Portable and removable media devices increase workplace productivity by enabling access to corporate network resources anytime and anywhere. As a result, such

devices are widely used to access corporate network resources. In addition to organization issued devices, IT departments increasingly face pressure to support the Bring Your Own Device (BYOD) trend, where staff use personally owned devices for work purposes. However, portable devices expose sensitive information assets to security risks greater than those typically encountered in office environments, often due to limited physical security controls. Therefore, portable and removable media security aims to achieve the security outcomes outlined below by balancing the benefits and risks associated with mobile devices.

IS8 – All organizations using portable and removable media must adopt formal procedures to prevent the unauthorized disclosure, modification, removal or destruction of assets, and interruption of business activities. As a minimum requirement, organizations must:

a. perform a formal risk-benefit analysis before the use of such media;

b. as part of a formal policy, require authorization for the use and transfer of portable and removable media;

c. use baseline system configurations that, by default, restrict access to media drives;

d. encrypt portable devices and removable media to deter unauthorized access;

e. enforce security policies on portable and removable media to detect and prevent unauthorized use;

f. conduct user security awareness training.

g. audit and monitor user activities; and

h. prohibit the storage and processing of sensitive information on personal devices.

To achieve the security outcomes mandated above, organizations must:

» Lock down host devices to prevent users from changing default configurations and thereby enabling malicious actors to execute privileged commands;

» Use full-disk encryption for devices processing sensitive data;

» Ensure that users understand that maintaining physical custody of devices is a primary form of defense;

» Prohibit the use of privately owned devices to process, store, or remotely access critical infrastructure systems, applications, and data, except in emergency or short-term situations where issuing official equipment is impractical;

» Define procedures for the timely termination of emergency use of privately owned devices for processing, storing, or remotely accessing critical infrastructure;

» Prevent devices that do not comply with organizational security policies, including hardened configuration requirements, from connecting to the corporate network;

» Provide users with appropriate training on the handling of authentication credentials, including encryption keys, hardware tokens, smart cards, and passwords;

» never leave devices unattended, and store devices separately from authentication credentials, among other protective measures;

» ensuring that user devices store only the data necessary to perform authorized business activities at any given time;

» Adopt anti-virus and anti-malware procedures, including the use of stand-alone systems (“sheep dips”), to scan portable and removable media for

malicious code before data import or export; and

» Ensure that users are familiar with mobile device incident response and reporting procedures, including when to report device loss to the law enforcement agencies.

5.10 Remote Access Security

Remotely connecting a computer to another computer or network over public networks, such as the Internet, increases staff flexibility and productivity. Staff with remote access capabilities can perform business activities, access e-mail, and transfer files from remote locations. However, remote access introduces significant security risks to organizations. Firstly, remote access requires additional security measures because communications occur over potentially insecure public networks. Secondly, because remote access often takes place in less controlled environments, such as homes or while travelling, it increases exposure to risks including equipment theft, unauthorized disclosure of information, unauthorized access to internal systems, and misuse of organizational resources. Therefore, organizations must not authorize remote access or teleworking arrangements unless appropriate security controls and safeguards are in place and comply with applicable information security policies. Effective remote access security measures can help achieve the following mandatory 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 associated with remote access;

c) use security controls e.g. encryption to protect data both at rest and in transit;

d) educate users on remote access risks and secure remote working practices;

e) security accredit remote access solutions handling sensitive or classified information; and,

f) align the remote access policy with incident management and business continuity plans.

To achieve the security outcomes mandated above, organizations must:

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

» Demonstrate that adequate authentication, access control, communication security, and availability measures are in place to reduce the risks of unauthorized access, disruption, and modification of remote access servers, clients, and applications;

» Enforce a remote access policy requirement that users and devices are granted access only to network services for which they are authorized;

» Grant remote access only for the period necessary to fulfil approved business purposes;

» Use encryption of appropriate strength to secure communication links and the information processed over them against interception and eavesdropping;

» Encrypt remote access client devices to protect information in the event of loss or theft;

» Ensure that users understand, accept, and comply with the Security Operating Procedures for mobile devices, including

powering off devices when not in use;

- Ensure that users understand and accept their personal accountability for protecting remote access devices against threats and risks in insecure environments, including snatching, shoulder surfing, and eavesdropping;
- Ensure that remote access servers are provided with appropriate security measures, including protection against unauthorized physical access, assured power supply, secure configuration and administration, and backup and recovery procedures;
- Conduct a formal risk assessment and obtain approval from relevant authorities before permitting the remote administration of critical infrastructure systems, applications, and data from overseas locations, given the risks posed by threat actors, including foreign intelligence services; and
- Sanitize and dispose of remote access devices in accordance with secure Equipment Disposal and Re-Use requirements.

5.11 Protective Monitoring

Protective monitoring comprises technical and procedural security measures aimed at detecting and preventing attempts to exploit information system vulnerabilities. Organizations should adopt a risk-based approach when determining the level of protective monitoring required. Accordingly, the level of protective monitoring should align with business requirements, exposure to threats and risks, and the potential business impact of security breaches. The mandatory minimum security outcomes outlined below support the establishment of an effective protective monitoring regime.

IS10 – All organizations must implement measures to detect, monitor, and attribute unauthorized information processing activities to specific users or entities. As a minimum requirement, organizations must:

a) define a protective monitoring strategy;
b) adopt an audit logging and accounting policy;
c) generate and retain audit logs, for an agreed retention period, recording user activities, exceptions, faults, and security events;
d) establish procedures for reviewing and analyzing monitoring results;
e) train staff to interpret and respond to monitoring results;
f) protect audit logging facilities and log data from unauthorized access, modification, or deletion; and
g) align protective monitoring activities with incident management and human resource (HR) policies.

To achieve the security outcomes mandated above, organizations must:

- 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;
- Have in place an accounting and audit policy that complies with business requirements for real-time security accounting and auditing. The policy shall assist developers and product teams in ensuring that technical solutions incorporate appropriate accounting and audit capabilities;
- Ensure that the network security architecture contains appropriate capabilities to identify, record, alert, and generate security audit reports;
- Ensure that accounting activities align with the required level of logging for each security classification. IT teams must not deviate from the accounting requirements without conducting a risk assessment and obtaining management approval confirming that the revised level of logging provides adequate assurance for business activities;
- Standardize accounting and audit log data to facilitate correlation and analysis

in accordance with ISO/IEC 27002;

- Have in place effective procedures for reviewing recorded logs and alerts to help identify and hold accountable individuals who misuse information assets;
- Recruit and maintain a competent team to administer the technological solutions and supporting infrastructure used to collect, store, and log suspicious events;
- Enforce access control measures guided by the principle of least privilege to ensure that no user or application process gains access to accounting and audit data without explicit authorization and a clearly defined role;
- Prevent system administrators from erasing or disabling logs relating to their own activities;
- Separate accounting and audit logs supporting routine security activities from evidential logs that may contain sensitive or confidential personal data and may be admissible in legal proceedings;
- Ensure that, where protective monitoring activities collect data relevant to legal proceedings, it is possible to verify the evidential integrity and admissibility of the data in courts of law;
- Have in place a process for escalating alerts generated by real-time accounting and audit systems to management representatives to support decisions on whether to trigger the incident management process; and
- Update the accounting and audit policy to reflect changes in the threat environment and the results of technical risk assessments.

5.12 Back-Ups

Achieving the mandatory minimum information security outcomes outlined below helps ensure the integrity and availability of data, software, and documentation, and enables timely recovery from disasters, system failures, or media failures. Backup processes should cover all information processing environments, including production and pre-production environments.

IS11 – All organisations must adopt formal policies and procedures to back up and regularly test copies of information and software required to recover from major disruptions. As a minimum requirement, organizations must:

a) define the required backup levels and retention requirements;
b) base the frequency of backups on the value, criticality, and sensitivity of data;
c) maintain accurate and complete records of backup copies;
d) store backup data at a secure location sufficiently separated from the primary site;
e) provide backup information with appropriate physical and environmental protection; and
f) test backup media regularly to ensure recoverability and integrity.

To achieve the security outcomes mandated above, organizations must:

- Define the extent, e.g. full or differential backups, and the frequency of backups based on business requirements, as well as the security classification and criticality of the information to the continued operation of the organization;
- Regularly test backup arrangements for individual information systems to help ensure that they meet the requirements of business continuity plans;
- Backups for critical systems must cover all system information, applications, and data required to recover the entire system in the event of a disaster;
- Regularly check and test restoration procedures to help ensure their

effectiveness and confirm whether recovery can be completed within the timeframes specified in the operational recovery procedures; and

» Apply appropriate safeguards to maintain the required security properties of backups, such as the use of encryption to maintain confidentiality.

5.13 Security Accreditation

There must be a clear plan to provide stakeholders with relevant information on how an organization complies with this framework. Organizations demonstrate compliance with security requirements by creating a body of evidence containing procedures, processes, instructions and plans for maintaining the security of information systems throughout their Lifecyle. The mandatory minimum information security outcomes outlined below demonstrate that the organization has identified and addressed major risks to critical systems.

IS12 – As a minimum requirement, organizations must:

a) accept and retain accountability for system accreditation;

b) ensure that every IT project has a designated senior responsible owner;

c) define and document the accreditation boundary;

d) develop and maintain an accreditation roadmap;

e) create and maintain accreditation plans;

f) document all procedures, processes, instructions, and plans for securing the system;

g) conduct appropriate system acceptance testing, including penetration testing; and

h) identify and allocate resources for through-life accreditation costs.

To achieve the security outcomes mandated above, organizations must:

» Show compliance with this framework, corporate policies and legislation applicable to the system's security accreditation scope. This may include engaging an external auditor.

6 Personnel Security

6.0.1 Introduction

Employees are among the most valuable assets of any organization. However, personnel may also present significant insider threat risks, whether intentional or unintentional. Indeed, changes in national information security policies worldwide have often been driven by high-profile accidental and deliberate disclosures of sensitive national security and personal information. Therefore, it is essential to reduce the likelihood of personnel exploiting legitimate access to critical infrastructure facilities, sites, information, and personnel for unauthorized purposes. Personnel security is particularly important in protecting the cyber supply chain against state-sponsored and industrial espionage threats. This section outlines the measures that organizations that use, own, and/or operate critical infrastructure must implement to establish the trustworthiness, integrity, and reliability of individuals before granting them access to sensitive information assets.

6.0.2Personnel Security and Risk Management

The themes contained in "Part I – Security Governance" apply to the personnel security functional area in the same way as they apply to information and physical security. For example, the personnel security area requires a credible risk management approach for managing personnel-related security risks. There are no absolute guarantees in security,

particularly in relation to personnel security. It is impossible to guarantee that individuals will always behave reliably. For example, changes in personal circumstances or lifestyle may affect an individual's reliability. In other instances, reckless personal behavior or entrapment may increase susceptibility to blackmail. Therefore, organizations must apply the risk management principles and mandatory security requirements presented in Part 1 to determine the acceptable level of personnel security risk at any given time. Accordingly, the mandatory minimum-personnel security requirements are as follows:

6.2 Security Roles & Responsibilities

Achieving the mandatory minimum information security outcomes outlined below helps organizations demonstrate that they have exercised due care in ensuring that individuals understand their security responsibilities and expectations.

PS1 – To reduce the risk of theft, fraud, or misuse of facilities, organizations must ensure that all users understand their information security responsibilities. As a minimum requirement, organizations must:

a) communicate security expectations to all prospective employees and employment candidates;

b) include information security responsibilities and obligations in employment contracts that all staff must review, agree to, and sign;

c) require staff to sign and comply with Security Operating Procedures for specified critical infrastructure systems or services;

d) inform staff that non-compliance with approved security policies and signed security documents may result in disciplinary action; and

e) enforce sanctions for non-compliance, including dismissal and legal prosecution.

To achieve the security outcomes mandated above, organizations must:

» Require all employees, including contractors and subcontractors to formally accept their security roles and responsibilities formally. Such acceptance shall include an undertaking to:

» Protect assets under their control and/or supervision from unauthorized access, disclosure, modification, destruction and interference;

» Comply with organizational security processes and activities; and,

» Report security events, suspected security incidents or other security risks to the organization;

» Ensure that individuals agree to comply with all organizational policies, standards, protocols and guidelines for protecting information, personnel and physical assets against security threats regardless of their 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 comply with User Acceptance Rules.

6.3 Baseline Security Clearance

Baseline Security (BS) clearance provides reasonable assurance that individuals seeking access to critical infrastructure are reliable and trustworthy. Therefore, all candidates seeking employment or contractual roles requiring access to critical infrastructure must undergo and successfully complete BS vetting checks. The extent of the checks conducted should depend on business requirements, identified risks, and the value, sensitivity, and criticality of the information assets involved. Accordingly, BS vetting checks apply to all users of critical infrastructure.

6.3.1 Baseline Security Clearance Defined

This clearance applies to individuals who require access to information classified up to and including RESTRICTED, and/or occasional, controlled, and supervised access to information classified up to and including SECRET. Achieving the mandatory minimum security outcomes outlined below enhances confidence in the trustworthiness and reliability of individuals accessing sensitive assets.

PS2 – PS2 – All organizations must perform Baseline Security (BS) checks to ensure that the character, integrity, and personal circumstances of individuals seeking employment are such that they can be trusted with access to critical infrastructure. As a minimum requirement, organizations must:

a) satisfactorily verify the identity of all applicants;

b) validate academic, employment, and financial records;

c) conduct criminal record checks;

d) establish that applicants are legally entitled to undertake the employment in question; and

e) document and risk manage cases where it is not possible to perform all required checks.

To achieve the security outcomes mandated above, organizations must:

» Ensure that Human Resource (HR) processes do not permit individuals to commence work on critical infrastructure projects without undergoing appropriate recruitment and security vetting checks;

» Verify the identity of candidates through independent checks using government-issued or recognized third-party identity documents, such as passports or other official photographic identification documents;

» Establish whether applicants have the legal right to work in Somalia, including compliance with residency requirements applicable to the sensitivity of the position;

» Verify the candidate's employment history by validating the completeness and accuracy of the curriculum vitae and supporting documentation;

» Obtain satisfactory character references for the applicant, including at least one professional reference and one personal reference;

» Establish whether the applicant is suitably qualified for the role by confirming claimed academic and professional qualifications; and

» Based on a risk assessment, determine whether the applicant should undergo additional national security vetting.

6.4 National Security Vetting

A security clearance is a status granted to individuals that authorises access to specific categories of sensitive or classified information. Security clearance is particularly important for critical positions because individuals occupying such positions who successfully commit acts such as illegal site access, espionage, unlawful interception, data interference, or system interference can cause significant harm to national security and national interests, compared to individuals in less sensitive roles. Therefore, national security vetting seeks to prevent individuals intending to subvert, compromise, or damage the stability and security of Somalia from occupying sensitive positions associated with critical infrastructure. The national security vetting process involves more rigorous checks than Baseline Security (BS) vetting and uses two clearance levels, as follows:

6.4.1 SECRET Clearance

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

6.4.2 TOP SECRET Clearance

This clearance level applies to individuals in privileged and highly sensitive managerial, technical, and information security roles who require frequent and uncontrolled access to information classified up to and including TOP SECRET. Organizations must limit such roles to the minimum number of personnel necessary to support operational requirements. It is important to emphasize that, as with all forms of security, national security vetting provides no absolute guarantee regarding the future reliability or trustworthiness of vetted individuals. However, effective national security vetting can help achieve the mandatory minimum-security outcomes outlined below.

PS3 – Individuals requiring access to systems and information essential to Somalia's national security, defence, diplomacy, public safety, public utilities, and economic stability must undergo national security vetting. As a minimum requirement, organisations must:

a) submit all applicants for positions identified on the Government list of security-vetted roles for national security vetting;

b) not initiate the national security vetting process before successfully completing recruitment and baseline security checks; and

c) seek advice from the Security Controller regarding the appropriate clearance level before making employment offers.

To achieve the security outcomes mandated above, organizations must:

- Create and maintain a process for complying with the national security vetting requirements of the relevant vetting authorities;
- Ensure that the Security Controller maintains the current list of Government security-vetted positions and that all candidates for positions on the list undergo national security vetting before commencing work;
- Ensure that possession of a valid security clearance is not a routine prerequisite for applying for positions or contracts listed as Government security-vetted positions;
- However, in exceptional circumstances, for example where the security clearance process may take longer than the duration of the contract, organizations may make a valid security clearance a condition of engagement. Organizations must document such exceptions for audit and legal purposes;
- Recognize that security vetting may occur during recruitment or at any stage where business requirements, identified risks, or the sensitivity and value of information assets require additional assurance regarding an employee's character and personal circumstances;
- Ensure that all security clearance applications are sponsored by an authorized Government Ministry, Department, or Agency;
- Subject to national security considerations and guided by the Need-to-Know principle, sponsoring Government entities should inform individuals when their names are submitted for national security vetting;

- Ensure that candidates understand that, although no individual is obligated to undergo national security vetting, appointment to positions on the Government list of security-vetted roles depends on obtaining and maintaining a valid security clearance;
- Use risk assessments to determine the necessity for, and level of, security vetting required for candidates seeking sensitive positions. For example, support and ancillary staff may require appropriate vetting depending on the results of the risk assessment;
- For sensitive positions, organizations may, in accordance with applicable laws, regulations, and ethical requirements, assess an applicant's susceptibility to pressure, coercion, or inducement to misuse legitimate access to premises, information, or personnel for unauthorized purposes by conducting detailed financial background checks, including credit references, assets, financial commitments, and unpaid liabilities;
- In strict compliance with applicable laws, regulations, and ethical requirements, organizations may consider whether an individual's personal circumstances, including medical history, criminal history, or behavioral factors, could pose a security risk if that individual were employed in a sensitive position;
- Work with vetting authorities to resolve delayed security clearances. For example, an employee may work "at risk" for a defined period, provided that the individual is undergoing vetting and operates under appropriate supervision;
-
- Only disclose information collected during the security clearance process to organizations or individuals with a legitimate Need-to-Know. In addition, organizations must retain security clearance information only for as long as necessary and in accordance with applicable legal and regulatory requirements;
- Make a risk-based decision on whether to rely on security vetting results obtained from another organization for a candidate under consideration, restart the vetting process, or conduct additional checks;
- Subject to national security considerations, establish a mechanism for informing individuals of the reasons for the refusal of a security clearance; and
- Establish a policy for managing existing employees who are unable to continue in their current position or assume a new position due to an adverse security vetting outcome. The policy must address redeployment, appeals procedures, and lawful, ethical, and transparent dismissal procedures for personnel occupying positions that require a valid security clearance.

6.5 Ongoing Personnel Security Management

Baseline and national security vetting checks provide assurance regarding an individual's security reliability only at a specific point in time. In practice, baseline and national security vetting is typically conducted before an individual joins an organization and/or assumes a new role. However, these screening processes may not fully identify an individual's susceptibility to misconduct, undue influence, coercion, or other behavioral risks. Therefore, ongoing personnel security management aims to achieve the mandatory minimum security outcomes outlined below.

PS4 – All organizations must monitor the continued security reliability and trustworthiness of individuals holding a Government security clearance. As a minimum requirement, organizations must:

a) maintain an accurate and up-to-date record of security-cleared individuals;

b) ensure that only individuals with a legitimate business need retain access to protected computer assets;

c) identify and assess significant changes in personal circumstances that may affect security reliability;

d) inform individuals that failure to notify Government vetting authorities of significant changes in personal circumstances may result in disciplinary action;

e) conduct periodic security reviews and appraisals;

f) investigate any matter that may affect an individual's suitability to access critical infrastructure; and

g) enforce sanctions for non-compliance.

To achieve the security outcomes mandated above, organizations 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 organizations of any security incidents that may affect the individual's continued suitability to hold a Government 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 organizations 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 behavior, personal circumstances and attitudes to risk. Common warning signs include 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, organizations 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.

7 Physical Security

Physical security focuses on preventing unauthorized physical access to, damage to, and interference with information, premises, and resources arising from a range of threats, including crime, espionage, natural disasters, and acts of terrorism. It also protects personnel from violence and other forms of physical harm.

7.0.1 Physical Security, Governance and Risk Management

The themes contained in "Part I – Security Governance" also apply to the physical security functional area. For example, physical security adopts the Plan-Do-Check-Act (PDCA) continuous improvement model to structure its governance processes. Indeed, physical security measures are most effective when integrated into all phases of the broader organisational security programme. Physical security controls are more difficult and costly to implement retrospectively after systems and facilities have been established. Physical security must also comply with the mandatory minimum security requirements for risk management contained in the Governance section of this policy. Accordingly, effective physical security measures should align with business requirements and security needs.

7.0.2 Physical Security in Context

Physical security measures operate alongside, and form the foundation of, other security domains such as information security and personnel security. Historically, physical security accounted for most security controls during the mainframe computing era. Organizations invested substantial resources in restricting physical access to personnel, implementing locks and alarm systems, and deploying environmental controls to regulate the operating conditions of large computing systems. This changed significantly as computers became smaller, more affordable, and more widely distributed.

7.2 Physical Security Perimeter

This policy requires organizations to establish and maintain an appropriate physical security perimeter around sensitive information processing facilities to prevent unauthorized physical access. A perimeter includes the entire area surrounding the building hosting protected computer assets, including roads, footpaths, parking areas, and other adjacent external spaces. The physical security perimeter forms the first layer of a "layered" or "defense-in-depth" security approach, which progressively increases the strength and complexity of security controls closer to areas containing sensitive information assets. As noted earlier, physical security controls implemented at the perimeter must align with business requirements and remain cost-effective. The cost of implementing security controls should not significantly exceed the potential impact of loss. Where the costs outweigh the potential impact of loss, organizations should consider alternative risk treatment options, such as relocating assets to secure data centers that are easier to protect and manage. By minimizing the risks of theft, destruction, damage, and unauthorized access, the security perimeter can help achieve the mandatory minimum-security outcomes outlined below.

PH1 – All organizations must establish and maintain appropriate security perimeters to protect facilities hosting critical infrastructure against a range of physical security threats, including crime, natural disasters, sabotage, and acts of terrorism. As a minimum requirement, organizations must:

a) assign physical security roles and responsibilities, including the designation of a Security Controller;

b) conduct physical security risk assessments before site selection and facility development;

c) incorporate physical security requirements into site design or implement necessary security enhancements to existing sites;

d) implement effective physical access control measures;

e) maintain, monitor, and regularly review physical access logs; and

f) establish procedures to prepare for, detect, respond to, and recover from physical security incidents.

To achieve the security outcomes mandated above, organizations must:

» Allocate physical security roles and responsibilities for facilities hosting critical infrastructure;

» physical security policy that describes, in appropriate detail, how the organization defines, implements, and demonstrates physical security controls across all locations and facilities;Carefully select data center sites by considering factors such as visibility, proximity to crime and hazardous areas, exposure to natural disasters, transportation access, and the availability of environmental controls and emergency services;

» Ensure that facilities are securely designed with due consideration for wall height and fire ratings, ceiling fire resistance and load-bearing capacity, door and window design and strength, electrical systems, and environmental control systems;

» Clearly define the physical security perimeter and ensure that its location, design, and strength correspond to the security requirements of the assets within the boundary and the results of physical security risk assessments; and

» Ensure that security perimeters are physically robust and free from gaps or weaknesses that could facilitate unauthorized entry. In addition, external walls must be of solid construction, and all external doors must be adequately protected against unauthorized access through appropriate control mechanisms such as bars, alarms, locks, and surveillance systems.

7.3 Physical Entry Controls

Secure areas within information processing facilities must implement appropriate physical entry controls to prevent unauthorized individuals from gaining access. In accordance with the risk management and proportionality principles, physical entry controls must be commensurate with business requirements, security requirements, and the sensitivity of the protected assets. Effective physical entry controls can help achieve the mandatory minimum security outcomes outlined below.

PH2 – Organizations must use appropriate physical entry controls to protect secure areas against physical security threats. As a minimum requirement, organizations must implement:

a) baseline physical security controls such as security guards, perimeter fencing, surveillance systems, and external monitoring;

b) access card or electronic access control systems to identify employees, log access activities, and manage access rights;

c) visitor management processes to support visitor registration, identification badge allocation, escorting, and visitor pass verification; and

d) employee access management processes, including requirements for personnel to wear identification badges, carry authorized access cards, and control the movement of equipment and assets.

To achieve the security outcomes mandated above, organizations must:

» Ensure that all facilities implement baseline physical access controls to safeguard information resources, including an on-duty security guard force, perimeter fencing (e.g. fences, gates, turnstiles, and mantraps), external security patrols, closed-circuit television (CCTV) surveillance systems, or an appropriate combination of these controls. In addition, organizations must require the use of access cards or electronic credentials to gain access to buildings;

» Ensure that all visitors report to the security reception and present valid proof of identification before gaining access to sensitive facilities. Visitors must sign in and sign out and wear an appropriate visitor badge, such as escorted or unescorted, at all times;

» Record the date and time of entry and departure for all visitors. In addition, visitors must only be granted access to premises supporting critical infrastructure for authorized and legitimate purposes;

» Ensure that visitors receive a security briefing covering the procedures applicable to the secure facility, including emergency and evacuation procedures;

» Restrict access to areas designated for processing or storing sensitive information to authorized personnel only;

» Implement appropriate authentication controls, such as access control cards combined with personal identification numbers (PINs), to manage and validate access and maintain secure audit trails of all access activities;

» Require all staff and visitors to wear visible identification at all times. All personnel at a facility must report unescorted visitors or individuals not displaying visible identification to security personnel;

» Grant third-party support service personnel restricted access to secure areas or sensitive facilities only when required and ensure that such access is monitored and supervised; and

» Regularly review, update, and revoke access rights to secure areas.

7.4 Internal Data Centre Physical Access Controls

Internal areas within information processing facilities require additional physical security controls because they host environments where sensitive information is processed, transmitted, or stored. These internal areas include data centers, communications and switching centers, server rooms, and end-user work areas. Such areas require more stringent physical and personnel security controls to safeguard the information and systems operating within them. Organizations must develop and implement a general access control policy for secure internal areas, particularly data centers, to achieve the mandatory minimum security outcomes outlined below.

PH3 – Organizations must implement appropriate internal physical security controls to protect critical infrastructure against physical attacks, unauthorized access, and environmental threats. As a minimum requirement, organizations must align the value, sensitivity, and criticality of assets with:

a) appropriate data center classification levels;

b) secure data center location requirements;

c) infrastructure protection and perimeter security measures;

d) physical access control mechanisms;

e) access control logging and monitoring requirements;

f) secure package handling and inspection procedures;

g) visitor management and monitoring systems; and

h) secure media and tape handling procedures.

To achieve the security outcomes mandated above, organizations must:

» Classify data centers according to their criticality to the continued operation of one or more critical business activities;

» Ensure that sites processing, storing, or handling classified information implement secure rooms equipped with an Intruder Detection System (IDS). Security personnel must respond to IDS alerts in a timely and documented manner;

» Ensure that personnel are informed of the existence of, or activities within, secure areas strictly on a Need-to-Know basis;

» Prohibit unsupervised work within secure areas, except where explicitly authorized, in order to reduce opportunities for malicious activity and enhance personnel safety;

» Physically secure and periodically inspect vacant secure areas; and

» Unless specifically authorized for legitimate business purposes, prohibit the use of photographic, video, audio, or other recording devices, including cameras integrated into mobile devices, within sensitive secure areas. Based on security requirements, organizations may require users to surrender such devices at the security desk before entering secure areas.

7.5 Equipment Security

Organizations must protect equipment against physical and environmental threats. These security measures help reduce the risks of unauthorized access to information, service disruption, and the loss, theft, or damage of equipment. Such measures are particularly important for equipment used outside organizational premises. Organizations must also protect supporting utilities and infrastructure, including power supplies, communication cabling, and environmental control systems. Effective equipment security measures help achieve the mandatory minimum security outcomes outlined below.

PH4 – Organizations must implement appropriate measures to prevent the physical loss, damage, theft, compromise, or disruption of equipment and infrastructure supporting critical infrastructure operations. As a minimum requirement, organizations must:

a) locate all production equipment within access-controlled data center boundaries;

b) protect power, telecommunications, and network cabling against interception, interference, tampering, or physical damage;

c) ensure the availability of reliable and resilient electrical power supplies; and

d) manage security risks associated with off-site equipment, information, software, and storage media.

To achieve the security outcomes mandated above, organizations must:

» Host all production computer systems, such as servers, firewalls, and network devices, within secure areas of the data center to prevent unauthorized physical access;

» Position devices processing sensitive data, such as display screens and terminals, in a manner that reduces the risk of unauthorized viewing during use;

» Protect power lines supporting IT services and telecommunications cabling against unauthorized access, interception, damage, or disruption, including through cable tapping. Where practicable, organizations should route cabling underground and apply appropriate protective shielding;

» Implement controls to minimize risks arising from physical threats, including theft, fire, explosives, smoke, water damage or water supply failure, dust, vibration, chemical exposure, electrical power interference, communications interference, electromagnetic radiation, and vandalism;

» Establish and enforce policies governing eating, drinking, and smoking in proximity to information processing facilities and equipment;

» Monitor environmental conditions, including temperature and humidity, to detect conditions that could adversely affect information processing facilities and equipment;

» Implement measures to protect power and telecommunications cabling against interception or damage, including the installation of lightning protection systems for buildings and surge or lightning filters on incoming power and communications lines; and

» Assess and manage security risks associated with off-site equipment, information, software, and storage media.

7.6 Secure Equipment Disposal and Re-Use

Organizations must have in place appropriate measures to manage the security risks associated with the disposal, re-use, transfer, and recycling of computer storage media containing sensitive information. These measures must address the secure sanitization, handling, transportation, disposal, and re-use of storage assets moving between secure and less secure environments for purposes such as repair, maintenance, exchange, and recycling. Timely, secure, and cost-effective equipment disposal and media re-use procedures can help achieve the following mandatory minimum-security outcomes.

PH5 – All organizations must adopt formal procedures to enable the secure disposal and re-use of storage media. To minimize the risk of unauthorized retrieval, disclosure, or reconstruction of erased data, organizations must, as a minimum requirement:

a) define secure disposal criteria and procedures;

b) define secure sanitization levels commensurate with the sensitivity and classification of information;

c) categories storage media requiring the same sanitization or disposal treatment;

d) define criteria to guide decisions relating to repair, re-use, exchange, recycling, or physical destruction of storage media;

e) validate and document the effectiveness of sanitization activities; and

f) maintain audit logs of decommissioning, sanitization, and disposal activities.

To achieve the security outcomes mandated above, organizations must:

» Ensure that all media used to store and process sensitive information, including storage devices and networking equipment, are sanitized and disposed of in accordance with organizational policies, procedures, and applicable legal or regulatory requirements;

» define secure sanitization levels to ensure that all relevant stakeholders understand the degree of data wiping or destruction required to provide reasonable assurance that data from decommissioned assets cannot be retrieved, reconstructed, or disclosed;

» Adopt a formal process to govern sanitization activities, including asset classification verification, sanitization and post-sanitization procedures, validation of sanitization effectiveness, audit logging, and final authorization or sign-off; and

» Ensure that, where it is not possible to securely destroy assets handling sensitive data, appropriate procedures are implemented to enable their secure storage, transportation, return to the owner, or disposal through authorized third parties.

APPENDIX 1

1.0 National Incident Management Response Plan

Information and Communications Technology (ICT) is a critical enabler of effectiveness and efficiency across organisational and business processes. ICT also enables organisations to optimise operations and improve service delivery through smarter and more efficient processes. As a result, organisations have become increasingly dependent on the availability, reliability, and resilience of ICT infrastructure to support critical operations and services. Consequently, any incident affecting the normal operation of ICT infrastructure may negatively impact the delivery of supported services and business processes. Such incidents may arise from natural events, system failures, human error, or malicious activities. Although considerable effort has been invested in developing controls to reduce risks arising from natural events, the effectiveness of controls designed to manage risks from malicious or human-induced threats continues to evolve in response to the changing threat landscape. This evolution is driven by two key factors. Firstly, the level of technological advancement

and sophistication of malicious actors has increased significantly over time. Secondly, the motivations of threat actors have evolved beyond merely gaining unauthorised access to systems and now include financial gain, cyber espionage, disruption of services, cyber warfare, and hacktivist objectives.

Globally, there has been a significant increase in cyber incidents affecting both public and private sector entities. These incidents have resulted in financial losses, operational disruption, loss of productivity, compromise of personal and classified information, theft of intellectual property, reputational damage, and, in extreme cases, organisational collapse. Given this environment, organisations must recognise that cyber incidents are inevitable and that effective incident response capabilities are essential to contain active attacks, support investigations and attribution efforts, and restore services and operations in a timely manner. Mature incident response frameworks also incorporate lessons learned processes to reduce the likelihood of recurrence, strengthen organisational resilience, and improve future response capabilities. In addition, proactive security monitoring and threat detection capabilities are essential for the early identification and mitigation of malicious activities before they escalate into major incidents.

In light of the above, and recognising the increasing adoption of ICT across public and private sector entities in Somalia, the Government, through the National Communications Authority (NCA), sets out its approach to national cyber incident management in this document. This approach recognises that:

a) cyber incidents are inherently cross-border in nature; and

b) effective incident management at both organisational and national levels requires coordinated collaboration among Government agencies, private sector entities, and other relevant stakeholders.

Accordingly, this plan provides overarching guidance for incident management across various sectors to strengthen national cyber risk management. It further establishes the framework through which Government institutions, private sector entities, and industry stakeholders will collaborate to ensure an effective and coordinated response to cyber incidents in Somalia.

1.1 Rationale

There are varying levels of cyber incident management capability maturity across different sectors, with some organizations operating at mature, advanced, intermediate, or start-up levels. In addition, the cross-sector and cross-border nature of cyber incidents requires effective collaboration to support timely and efficient incident response. Effective national incident management coordination also contributes to achieving a repeatable and mature national cybersecurity posture, particularly where interdependencies exist among critical sectors. Furthermore, this Plan promotes proactive incident management, information sharing, and collaboration with international partners and industry stakeholders. These elements are essential to demonstrate national preparedness and resilience in responding to cyber incidents.
The Plan is built around the following two key aspects:

a) Strategic/National Level: The need for a national coordination structure to guide inter-agency cooperation and collaboration with international partners in managing cyber incidents of national significance or impact.
b) Operational/Organizational Level: The need for defined, tested, and regularly updated incident management processes and procedures at the organizational level, guided by business impact assessments and organizational risk profiles. This recognizes that each organization has unique operational risks, critical services, and business continuity requirements.

1.3 Objectives

The objectives for the National Incident Response Plan are:

a) Define the governance structure for national cyber incident management;

b) Define processes for systematic, coordinated, and efficient cyber incident management, including operational-level response and inter-agency collaboration;

c) Provide guidance for managed and coordinated incident response communications; and

d) Establish mechanisms to monitor progress, evaluate performance, and measure the effectiveness of incident management activities at the national level.

2.0 Development Context

The National Incident Response Plan was developed in the context of the following national policies, strategies, frameworks, and standards.

2.1 The Somalia Cybersecurity Act

The Somalia Cybersecurity Act establishes a formal national framework for cybersecurity incident coordination by designating the National Communications Authority (NCA) as the lead government institution responsible for national cybersecurity governance. The Act centralises national coordination by empowering the NCA to establish information-sharing mechanisms between public and private sector entities and by requiring Critical Infrastructure (CI) operators to report cybersecurity incidents within 24 hours. To operationalise this framework, the Act establishes the Somalia Computer Emergency Response Team (SOMCIRT) as the national focal point for receiving incident reports, issuing early warnings and advisories, and providing technical support to public and private sector entities. SOMCIRT is further mandated to coordinate Sectoral CERTs, support digital forensic investigations for law enforcement agencies, and represent Somalia in regional and international cybersecurity cooperation initiatives, including the exchange of technical information on emerging cyber threats and vulnerabilities.

2.2 Incident contextualization

An incident is defined as "a single or series of unwanted or unexpected information security events that have a significant likelihood of compromising business operations and threatening information security." Incident management processes include, at a minimum, the following activities:

Sn.	Activity	Description
1.	Detect and Analyze	Initial detection of activity for an organization requires prior deployment of malicious code protection and protective monitoring solutions. Based on these detections, an initial analysis is conducted.
2.	Begin Notification	Depending on the initial analysis, notifications are sent to responsible stakeholders and affected parties.
3.	Setup Communications	This involves the establishment and use of secure communication channels between responsible actors during the incident response process.
4.	Contain	This involves taking appropriate actions to contain and prevent the spread of the incident. The Incident Response Team must balance containment measures with the need to conduct digital forensic investigations in accordance with the organization's Incident Response (IR) policy. Depending on the severity of the incident, external technical assistance may be sought.
5.	Identify	This step follows containment and involves further investigation to determine the root cause, scope, and impact of the incident. Depending on the severity of the incident, external digital forensic support may be required.
6.	Security Incident Record	The response team creates and maintains an accurate and complete record of the incident within an incident tracking system. Relevant information may be shared with the National CERT/SOMCIRT for coordination and information sharing purposes.
7.	Return to Operations	This activity involves the restoration and resumption of operations to normal or agreed service levels in accordance with business continuity requirements and service level agreements (SLAs). Affected business units must confirm that services have been fully restored.
8.	Document and Review	At this stage, lessons learned are identified, documented, and reviewed. This includes assessing the effectiveness of the incident response process, identifying challenges encountered, and updating security controls, policies, procedures, and response plans to improve future incident response capabilities.

In order to guide the incident response teams in determining the classification levels, alignment has been achieved with the National Cyber Risk Management Framework as indicated below:

Incident Severity	Description	Response Time
Trivial	Incident causing negligible or no operational impact on systems, services, or business operations.	As appropriate
Low	Incident causing limited impact on systems, services, or users, manageable within normal operational procedures.	Within 48 hours
Medium	Incident causing moderate operational disruption or affecting multiple systems, users, or services, requiring coordinated response actions.	Timely response / Within 1 hour
High	Incident causing significant disruption to critical services or compromise of sensitive information, requiring urgent containment and management attention.	Urgent Response. These should be reported within 6 hours to SOMCIRT
Critical	Incident causing severe or widespread disruption to critical infrastructure, national security, public safety, or the economy, requiring immediate national-level coordination and emergency response measures.	Immediately / National Level Response

In line with the above, Article 17 of the Somalia Cybersecurity Act stipulates the following cybersecurity incident reporting obligations for all Critical Infrastructure Operators in Somalia:

- Collect information relating to the incident or threat, including the nature, scope, impact, and potential consequences of the cybersecurity incident;
- Assess the risks posed to critical infrastructure, customers, suppliers, dependent services, and other relevant stakeholders;
- Take appropriate preventive, mitigation, containment, response, and remedial measures to minimise the impact and associated risks;
- Report to SOMCIRT, and any other relevant authorities or institutions, all key information relating to the cybersecurity incident within twenty-four (24) hours of detecting the incident;
- Provide any additional information relating to the cybersecurity incident that the National Communications Authority (NCA) or other relevant institutions may lawfully request; and
- Allow the NCA and other relevant institutions authorised under the Act to access relevant networks, systems, and information infrastructure for the purposes of analysing the cybersecurity incident, identifying related threats or vulnerabilities, assessing disruptions to dependent services, and advising on appropriate preventive, mitigation, response, and remedial measures.
- In considering the importance and

potential impact of the infrastructure affected by the cybersecurity incident referred to above, Critical Infrastructure Operators shall take into account the following factors:

- The nature, severity, and operational impact of any disruption to services dependent on the critical infrastructure;
- The number of individuals, organisations, businesses, or essential services affected by the disruption;
- The duration, scale, and potential persistence of the cybersecurity incident; and
- The geographical scope and extent of the areas affected by the cybersecurity incident.

2.3 The Guiding Principles

The guiding principles for this plan include the following:

a) Enhancing mutual inter-agency collaboration, coordination, and information sharing in cybersecurity incident response;

b) Strengthening public-private partnerships and sector-wide cooperation in incident response activities;

c) Promoting standardization, harmonization, and consistency of incident response processes across Government institutions and Critical Infrastructure Operators; and

d) Promoting the sharing and efficient utilization of resources, expertise, threat intelligence, and incident response capabilities to strengthen national cyber resilience.

3.0 Organization

The national incident management approach takes into consideration the inter-agency roles, responsibilities, capabilities, and the need for centralised coordination. Various Government institutions possess different authorities, responsibilities, technical capabilities, and resources that can be leveraged in responding to cyber incidents. Effective coordination among these entities is essential to ensure a timely, coordinated, and efficient national response. As the lead government institution responsible for national cybersecurity governance, the National Communications Authority (NCA) shall rapidly notify relevant Government agencies and stakeholders to facilitate a unified and coordinated response and ensure that the appropriate combination of agencies responds to a particular cyber incident. In responding to cyber incidents affecting the private sector, a unity of effort approach shall be adopted to synchronise the overall Government response, minimise duplication of efforts, close operational gaps, and improve information sharing and service coordination among all relevant stakeholders.

3.1 Governance

The governance structure for National Incident Management is aligned with the Somalia Cybersecurity Act, which establishes the National Cybersecurity Committee as the national coordination and oversight body for cybersecurity matters. The governance structure is further organized into three levels as outlined below.

Level	Description
Strategic Level	Provides national policy direction, governance oversight, and high-level coordination for cybersecurity incident management, including decision-making and coordination for incidents of national significance.
Operational Level	Coordinates national and sectoral cyber incident response activities, information sharing, technical support, and inter-agency collaboration during cybersecurity incidents.
Technical Level	Focuses on technical incident handling, detection, analysis, containment, eradication, recovery, and incident reporting activities carried out by incident response teams and Critical Infrastructure Operators.

In line with the above, the incident several table provided for below includes escalation criteria.

Incident Severity	Description	Highest Escalation	Response Time	Notification Required
Trivial	These incidents have no signnificant harmful impacts. However, they must be analyzed to prevent significant incidents in the future	Institutional Incident Response Team within the organization.	As appropriate	No
Low	Incidents causing moderate disruption to services, including temporary loss of availability to some services. These incidents may cause group embarrassment, reduced efficiency, or limited operational impact.	Institutional Incident Response Team.	Within 48 hours	No
Medium	Incidents causing moderate disruption to services, including temporary loss of availability to some services. These incidents may cause group embarrassment, reduced efficiency, or limited operational impact.	Sectoral CERT Team when the Institutional Incident Response Team fails to contain the spread of the incident or where a sector does not have a CERT Team	Within 1 hour	Yes

High	Incidents causing significant disruption to critical services, affecting the organization's ability to achieve business objectives. The incidents may cause major operational disruption or compromise of sensitive information.	Sectoral CERT Team when the Institutional Incident Response Team fails to contain the spread of the incident or where a sector does not have a CERT Team. Escalation to SOMCIRT where external assistance and/or inter-agency response is required.	Immediately or as soon as possible	Yes
Catastrophic	Incidents causing severe or widespread disruption to critical infrastructure, national security, public safety, or essential national services. These incidents may result in significant economic impact, compromise of classified or sensitive information, or prolonged disruption of essential services.	Immediate escalation to SOMCIRT, the National Communications Authority (NCA), relevant Government agencies, and the National Cybersecurity Committee, where necessary.	Immediately / Highest Priority Response	Yes

3.2 Operational

Building on the incident severity and escalation levels described above, the following table outlines the minimum required operational capabilities and response expectations for effective cybersecurity incident management.

Entity	Required Capability
National Cybersecurity Committee	a) Facilitate information sharing, coordination, and cooperation among the institutions listed under Article 7 of the Somalia Cybersecurity Act b) Approve policies to protect critical infrastructure and other cybersecurity matters, or any other matter related to the implementation of the Act. c) Propose and approve regulations and procedures to strengthen the cybersecurity strategy and related policies, and to ensure the effective implementation of the Act. d) Support centralized national cyber incident management and coordination for defense forces during critical or catastrophic cybersecurity incidents.

National Communications Authority	a) Host and operate the national SOMCIRT on a 24/7/365 basis. b) Build SOMCIRT operational capabilities in incident response, malware analysis, digital forensics, situational awareness, and cyber threat intelligence. c) Receive, assess, and coordinate reports of cybersecurity incidents and threats from Critical Infrastructure Operators and other reporting entities. d) Maintain periodic national cyber incident reporting and situational updates to the National Cybersecurity Committee for information sharing and national security purposes. e) Establish collaborative structures and partnerships with regional and international CERTs/CSIRTs, FIRST, and other cybersecurity organisations. f) Coordinate and manage escalated or nationally significant cyber incidents. g) Provide assurance, coordination, and specialised training for incident responders and institutional incident response teams, including assurance of organisational Incident Response Plans. h) Provide incident response coordination, early warning, and cyber threat alerting services. i) Define and maintain national incident management standards, processes, procedures, and digital forensic requirements. j) Support and coordinate cybersecurity incident response training and national cyber exercises for all response teams. k) Promote cybersecurity information sharing and inter-agency collaboration in cyber incident management. l) Develop cybersecurity best practices and organise national cyber drills and simulation exercises. m) Maintain active coordination and communication channels with Sectoral and Sub-sectoral CERTs/CSIRTs.
Somalia Police Force	a) Investigate cybercrime and cyber-enabled offences. b) Detect, prevent, and respond to organized cybercrime activities. c) Maintain active coordination and information sharing mechanisms with SOMCIRT and relevant national cybersecurity stakeholders.

Sector Regulator	a) Define and enforce mandatory cybersecurity requirements, cyber breach reporting obligations, and incident reporting procedures within sector licensing and regulatory frameworks. b) Establish and maintain effective risk-based Security Incident Management processes, procedures, and Sectoral CERT teams linked to SOMCIRT. c) Ensure compliance with the National Cybersecurity Compliance Framework. d) Maintain active points of contact with SOMCIRT. e) Maintain periodic reporting to SOMCIRT on cybersecurity incidents for information sharing and/or coordinated resolution. f) Participate in national cyber drills and/or organize sector-specific cyber exercises. g) Maintain regional and international cybersecurity collaboration mechanisms within the relevant sector.
Designated Critical Infrastructure (CI) Operator	a) Establish and maintain effective risk-based Security Incident Management processes, procedures, and institutional cybersecurity teams. b) Provide first-level analysis, detection, containment, and resolution of cybersecurity incidents. c) Maintain coordination and escalation channels with SOMCIRT and Sectoral CERTs for cyber incidents above Low severity level. d) Maintain periodic reporting to the Sectoral CERT on cybersecurity incidents for information sharing and/or coordinated resolution. e) Design, implement, maintain, and test Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP). f) Participate in national and sectoral cyber drills and exercises. g) Implement applicable CERT advisories, alerts, and mitigation measures.
Ministries and Government Agencies	a) Establish and maintain effective risk-based Security Incident Management processes, procedures, and institutional cybersecurity teams. b) Provide first-level analysis, detection, containment, and resolution of cybersecurity incidents. c) Maintain coordination and reporting mechanisms with SOMCIRT for reporting and/or escalation of cyber incidents above the Low severity level. d) Design, implement, maintain, and test Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP). e) Participate in national cyber drills and incident response exercises. f) Implement applicable CERT advisories, alerts, and recommended mitigation measures.

In addition to the above, the following cross- cutting operational requirements and

coordination mechanisms shall apply:

a) The SOMCIRT shall take the lead in organising periodic inter-agency cybersecurity education, training, simulation exercises, and capacity-building programmes to ensure that incident responders develop a clear understanding of the roles, responsibilities, operational procedures, and coordination mechanisms of partner institutions.
b) A Unified Command approach shall be adopted to improve unity of effort in multi-jurisdictional or multi-agency cyber incident management. The use of Unified Command enables institutions with legal authority, operational responsibility, or functional roles relating to the incident to jointly manage and coordinate incident response activities through the establishment of common incident objectives, response priorities, communication channels, and operational strategies. However, each participating institution shall retain authority, responsibility, and accountability for its personnel, systems, and resources, and each member of the Unified Command shall ensure timely information sharing and coordination with other participating entities.
c) All institutions and agencies shall develop and maintain an Information Exchange Policy to govern the secure sharing of information with third parties, Sectoral CERTs, and SOMCIRT. This Plan adopts the Information Exchange Policy Framework developed by the Forum of Incident Response and Security Teams (FIRST) as the guiding framework for cybersecurity information sharing and coordination.

3.3 Incident Communication

Incident communication planning provides an organised, coordinated, and harmonised approach to responding to cybersecurity incidents at both organisational and national levels. Each phase of the incident management lifecycle has unique communication requirements that must be addressed appropriately. Throughout the incident management process, effective communication is essential to ensure a timely, coordinated, and efficient response from the detection phase through containment, recovery, and post-incident review activities. Cyber incident response requires the active participation and coordination of multiple stakeholders to ensure the effective resolution of incidents and the restoration of affected systems, services, and information assets to normal operations. In addition to the technical teams responsible for incident handling and recovery, other stakeholders, including users, customers, citizens, partners, service providers, regulators, and the public, may also be affected by the incident. These stakeholders require timely, accurate, and consistent communication regarding the nature of the incident, the measures being implemented to address it, and any required remedial or protective actions. Where incidents involve cybercrime or violations of applicable laws, organisations shall cooperate with law enforcement agencies and relevant authorities to support investigations, evidence preservation, attribution activities, and legal enforcement processes. From a national perspective, effective incident communication provides the following benefits:

a) Enhancing cross-agency coordination, collaboration, and information sharing in cybersecurity incident management;
b) Strengthening public trust and confidence in digital services and Information Technology-enabled systems; and
c) Promoting a national culture of cybersecurity awareness, resilience, and preparedness.

3.3.1 Communication Lifecycle

a) For incident communication to be effective, communication approaches and procedures must be aligned with the

incident management lifecycle and tailored to the severity, impact, and nature of the incident. Communication activities must also consider the operational, legal, regulatory, reputational, and business impacts arising from the incident. Furthermore, stakeholders involved in incident response have different information requirements depending on their roles, responsibilities, interests, and concerns. Accordingly, this Plan adopts the following incident communication lifecycle:

Communication Lifecycle description is as below:

Sn.	Lifecycle stage	Descriptive Notes
a)	Pre-Incident	• Establish communication procedures, roles and responsibilities. • Develop approved communication templates. • Define escalation and incident reporting contacts. • Conduct awareness and training activities
b)	Initial Response	• Detect and assess cybersecurity incidents. • Conduct incident analysis and classification. • Verify and acknowledge the incident. • Designate authorized spokespersons. • Provide clear, accurate, and timely communication. • Disseminate verified updates through approved communication channels. • Maintain stakeholder coordination and transparency.
c)	Incident Management	• Continuous coordination and information sharing • Provide operational and situational updates • Support containment and investigation activities • Coordinate stakeholder communication and response actions • Address misinformation and stakeholder concerns.
d)	Resolution & Recovery	• Communicate incident resolution and recovery status. • Implement and communicate corrective measures. • Highlight response activities and institutional capabilities. • Reinforce institutional credibility, public confidence, and corporate identity.
e)	Post-Incident Review	• Evaluate communication effectiveness and response performance. • Document and share lessons learned and improvement areas. • Identify corrective actions to address gaps and weaknesses. • Update communication procedures and response plans for continuous improvement.

3.4 Monitoring and Evaluation

Monitoring and Evaluation (M&E) is essential for measuring the effectiveness and progress of the implementation of this Plan. This shall be achieved through periodic performance reviews and incident response assessments, as outlined below:

a) Each Incident Response Team (IRT) will conduct monthly performance assessments based on incident management and response activities. The assessment reports shall be submitted quarterly to the respective Sector CERT. Sector CERTs shall analyze and consolidate the reports and submit semi-annual performance reports to the National SOMCIRT. Where a Sector CERT has not been established, Incident Response Teams shall submit monthly performance reports directly to the National SOMCIRT.

The following minimum Key Performance Indicators (KPIs) shall be included in the monthly reporting:

KPI	Descriptive Notes
Number of Incidents	Total number of registered cybersecurity incidents categorized by incident type.
Number of Escalations	Total number of incidents escalated due to failure to resolve within the defined resolution timeframe.
Average Initial Response Time	Average time between incident reporting and the initial response by the Incident Response Team.
Incident Resolution Time	Average time required to resolve incidents, categorized by incident type and severity.
Incident Resolution Effort	Average operational effort required to resolve incidents, categorized by incident type.
First Time Resolution Rate	Percentage of incidents resolved by the Incident Response Team without external support or escalation.

a) SOMCIRT will analyze performance reports submitted by Incident Response Teams and provide consolidated reports to the National Cybersecurity Committee.

b) SOMCIRT will organize bi-annual performance review meetings for all Incident Response Teams to evaluate performance, share lessons learned, and identify improvement actions.

APPENDIX 2

1.0 Implementation Roadmap

This roadmap establishes a phased national implementation approach to support Critical Infrastructure Operators (CIOs) in translating regulatory obligations into practical and measurable actions. The roadmap adopts a graduated compliance model based on three core principles: establishing foundational capabilities, strengthening institutionalized risk management, and advancing assurance, resilience, and continual improvement. This phased approach recognizes that many operators require time to identify critical assets, assign accountable leadership, implement baseline security controls, operationalize incident reporting procedures, and develop evidence-based compliance capabilities before achieving full regulatory assurance and resilience maturity. The roadmap is structured around three implementation horizons covering the short-term, medium-term, and long-term phases.

1.1 SHORT-TERM MILESTONES

Within the first **12 months**, each designated operator should determine its regulatory applicability, identify accountable personnel, classify critical assets and services, establish incident reporting procedures, and implement minimum cybersecurity policies, controls, and compliance records.

The following key milestones shall apply:

a) **Formal launch and regulatory activation**

The National Communications Authority (NCA) will finalize the national register of Critical Infrastructure Operators and will formally issue the two frameworks and this roadmap through an official launch and stakeholder engagement process with designated Critical Infrastructure Operators.

b) **Governance And Accountability Established at Operator Level**

Each designated operator shall appoint an accountable executive, designate a cybersecurity focal point, establish a cyber risk governance committee or equivalent management forum, and approve a board-level or executive-level implementation charter. Operators shall also define reporting lines between cybersecurity, IT, operations, legal, risk, compliance, and business continuity functions.

c) **Baseline Asset, Service and Risk Identification**

» Each designated operator shall complete an initial inventory of critical services, supporting business processes, information assets, key technologies, external dependencies, and high-risk suppliers.

» Operators shall conduct a baseline cyber risk assessment and identify highest-priority treatment actions. The National Cyber Risk Management Framework shall be operationalized through identification of critical services, mapping supporting assets and dependencies, assessment of threats and vulnerabilities, evaluation of business impacts, and documentation of treatment priorities.

d) **Minimum Control Baseline Implemented**

Each operator shall implement a minimum control baseline in accordance with the National Cybersecurity Compliance Framework controls. Where controls cannot yet be fully implemented, operators shall document compensating measures and remediation timelines.

e) **Incident Reporting and Coordination Operationalized**

» Each operator shall comply with incident severity thresholds and reporting timelines established by SOMCIRT. Accordingly, SOMCIRT will operationalize

incident intake, escalation, advisory, and feedback channels for designated operators.

» Each operator shall test internal procedures for detecting, escalating, and reporting notifiable incidents.

» The first-year objective is to ensure incident reporting becomes routine rather than exceptional. Operators shall understand when to report, what to report, how to preserve evidence, and how to coordinate with SOMCIRT during significant incidents.

» f)**Initial compliance submissions completed**

» By the end of the short-term phase, each operator shall submit an initial compliance package to the NCA. This shall include a self-assessment against the compliance framework, baseline risk register, prioritized remediation plan, governance evidence, incident reporting contact matrix, and executive attestation.

» The NCA will use the first cycle of submissions to identify sector-wide weaknesses, refine supervisory expectations, target technical assistance, and establish a national baseline view of cybersecurity readiness across critical infrastructure sectors.

1.2. MEDIUM-TERM MILESTONES

Between months 12 and 24, operators shall transition from baseline adoption to repeatable implementation, while the NCA will transition from awareness-led supervision to structured monitoring, validation, and targeted intervention. The primary objective of this phase is to ensure cybersecurity becomes embedded within business processes, procurement, service delivery, and resilience planning rather than remaining a policy-driven exercise.

a) **Sector-Specific Guidance and Supervisory Differentiation**

The NCA will establish differentiated supervisory cycles based on risk tiers, with higher-risk operators subject to enhanced reporting, monitoring and review requirements.

b) **Risk Treatment Programs Institutionalized**

» Operators shall convert first-year remediation plans into formal risk treatment programs with approved budgets, accountable owners, implementation milestones, and residual risk decisions. Cyber risk shall be integrated into enterprise risk management, business continuity, change management, and capital planning processes.

» Operators shall manage cybersecurity remediation as a structured risk management portfolio rather than isolated technical activities. This shall include linking remediation initiatives to risk statements, documenting treatment decisions, escalating overdue actions, and ensuring accepted risks are formally approved at the appropriate management level.

c) **Exercise and Resilience Testing Program Launched**

» Each operator shall conduct at least one tabletop exercise and one technical or operational resilience test relevant to its threat environment.

» SOMCIRT will coordinate selected cross-sector exercises involving incident reporting, communication, escalation, and recovery coordination. Testing shall cover ransomware, service disruption, data compromise, insider misuse, and third-party failure scenarios. After-action reports shall be used to update response plans, awareness programs, training activities, and technical controls.

d) Workforce and capability development scaled

The NCA will implement a national capacity-building program for regulated operators, including executive briefings, practitioner training, and communities of practice for cybersecurity focal points across critical sectors. Operators shall establish role-based awareness and specialist development programs. Sustainable compliance depends on people, governance, and operational capability, not solely on technical controls. The NCA's cybersecurity mandate on capacity building and awareness will be expanded into a structured operator support program covering governance, risk assessment, incident handling, evidence retention, secure configuration, and supervisory engagement. The objective is to reduce dependency on limited personnel and improve implementation consistency across critical sectors.

1.3 LONG-TERM MILESTONES

Between months 24 and 36 and beyond, the cybersecurity ecosystem shall transition into a stable and sustainable national cybersecurity framework in which operators demonstrate continuous compliance, operational resilience, and ongoing improvement. National resilience shall be strengthened through recurring assurance activities, information sharing, and adaptation to evolving cyber threats.

a) **Full Compliance Cycle and Formal Assurance**

The NCA will require full-cycle compliance submissions covering governance, risk management, security controls, incident management, resilience testing, third-party oversight, and improvement actions. For higher-risk operators, this shall be complemented by independent assurance, thematic reviews, and on-site validation activities, where legally and operationally appropriate. The long-term objective is to ensure not only the existence of policies, but also confidence that controls are operating effectively and consistently. Formal assurance shall include internal audit reviews, SOMCIRT-led independent assessments, evidence-based supervisory inspections, and thematic reviews focused on persistent high-risk areas. Compliance shall become demonstrable, measurable, and evidence-based, rather than self-declared.

b) **Enforcement fully operational**

After the transitional implementation periods have elapsed, the NCA will implement a graduated, risk-based enforcement model that may include remedial directives, mandatory corrective action plans, enhanced reporting obligations, and sanctions for persistent or material non-compliance, subject to the Cybersecurity Act and related regulations. Enforcement actions shall be predictable, proportionate, and risk-based, taking into account good-faith implementation gaps, systemic negligence, failure to report significant incidents, and non-compliance with corrective directives.

c) **National Cyber Risk Picture and Sector Benchmarking Established**

SOMCIRT will produce periodic national and sectoral cyber risk outlooks based on compliance submissions, incident trends, systemic weaknesses, and resilience indicators. Operators shall receive anonymized benchmarking reports comparing their cybersecurity maturity and performance against sector peers. The NCA will transition from entity-level supervision to ecosystem-wide cyber risk intelligence and coordination. Benchmarking shall support continuous improvement by enabling operators to identify capability gaps and maturity weaknesses, while national-level analysis shall support policy development, international cooperation, and strategic investment in protecting Somalia's critical digital infrastructure.

d) Continuous improvement and frameworks refresh

The NCA will periodically review and update the cybersecurity frameworks and this roadmap based on operator feedback, incident trends, exercise outcomes, technological developments, and lessons learned from supervisory activities. Operators shall maintain annual review cycles for cybersecurity risk assessments, policies, control effectiveness, incident response procedures, and awareness and training programs to ensure continuous improvement and long-term resilience.

2.0 Implementation Governance

SOMCIRT will establish a coordination and engagement forum comprising sector focal points and operator representatives from priority critical infrastructure sectors. The forum shall facilitate information sharing, discuss common implementation challenges, promote coordination, and clarify regulatory and supervisory expectations.

2.1 Key risks and mitigation

The roadmap shall explicitly identify potential implementation risks and define corresponding mitigation measures to support effective, consistent, and sustainable implementation across critical infrastructure sectors.

Risk	Likely effect	Mitigation
Unclear scope of covered operators	Delayed compliance implementation and disputes over applicability.	Identify, designate, and gazette Critical Infrastructure (CI) Operators.
Limited operator capability	Inconsistent implementation and weak operational resilience.	Conduct capacity-building programs, technical training, and sector-based awareness initiatives.
Supplier dependence	Hidden systemic risk through outsourced services	Require supplier classification, contractual security clauses, and incident notification obligations.
Fragmented inter-agency coordination	Slow response during national cyber incidents	Establish standing coordination protocols and conduct regular exercises

3.0 Supporting implementation

To support effective implementation, SOMCIRT will establish the following capabilities in the medium term:

a) Establishment of an information exchange and information sharing platform to enable timely, trusted, and structured sharing of cyber threat, incident, and vulnerability information between SOMCIRT, Sector CERTs, Critical Infrastructure Operators, and relevant government stakeholders, thereby improving collective situational awareness and coordinated response.

b) Development of a national cybersecurity training and certification program to build a sustainable pipeline of qualified

cybersecurity professionals, harmonize minimum competence standards across sectors, and strengthen implementation capacity within government institutions and Critical Infrastructure Operators.

c) Development and implementation of a cyber threat intelligence platform integrated with Sector CERTs, where applicable, and operator Security Operations Centers (SOCs). This will support automated collection, analysis, and dissemination of actionable threat intelligence, early detection of cyber campaigns targeting national infrastructure, and coordinated defensive measures across sectors.

d) Development of directives and guidelines for emerging technologies to support secure adoption and usage of emerging technologies within government institutions and designated Critical Infrastructure Operators, while strengthening cybersecurity governance, risk management, regulatory compliance, and secure technology adoption.

In addition to the above, and to facilitate effective implementation of the National Cyber Risk Management Framework and the National Cybersecurity Compliance Framework by designated Critical Infrastructure (CI) Operators, the National Communications Authority (NCA) will prioritize, develop, and operationalize the following regulatory instruments:

a) **National Registration and Certification of Cybersecurity Professionals**

The National Communications Authority (NCA) will establish and operationalize a national system for the registration and certification of cybersecurity professionals providing services in Somalia, with particular emphasis on professionals supporting designated Critical Infrastructure (CI) Operators. The system shall define minimum competency standards, ethical obligations, and continuous professional development requirements, and shall be supported by a publicly accessible register of certified professionals. This will enhance assurance and trust for Critical Infrastructure Operators when procuring cybersecurity advisory, implementation, assessment, and managed security services.

b) **Implementing regulation on professional registration and certification**

The National Communications Authority (NCA) will fast-track the development and issuance of implementing regulations establishing the procedures, eligibility criteria, and oversight mechanisms for the registration and certification of cybersecurity professionals. The regulations shall clearly define eligibility requirements, application and vetting procedures, assessment mechanisms, recognition of foreign qualifications, renewal and suspension conditions, and appeal procedures to ensure a predictable, transparent, and accountable regulatory framework for cybersecurity professionals and designated Critical Infrastructure (CI) Operators.

c) **National Certification Regime for Cybersecurity Tools, Services, and Protection Techniques**

The National Communications Authority (NCA) will establish, as a matter of priority, a national certification framework for cybersecurity tools, services, and protection technologies deployed within Somalia, with particular focus on solutions used by designated Critical Infrastructure (CI) Operators. The certification framework shall verify that cybersecurity tools and services meet

minimum security, interoperability, reliability, and quality requirements, thereby reducing the risk of insecure, untested, or ineffective technologies being deployed within systems supporting essential national services.

d) **Implementing regulation on certification of tools, services, and techniques**

The National Communications Authority (NCA) will concurrently develop and issue implementing regulations defining the procedures, evaluation criteria, and assurance requirements applicable to the certification of cybersecurity tools, services, and protection technologies. The regulations shall clearly define categories of products and services subject to mandatory or recommended certification, establish testing and evaluation methodologies, including the use of accredited laboratories and recognized international certification schemes, and specify applicable labelling or trust-mark requirements. The regulations shall further establish procedures for certification renewal, suspension, and revocation where certified products or services no longer comply with established security, interoperability, or quality requirements.

APPENDIX 3

3.0 SOMCIRT Cybersecurity Information Exchange Policy

1. PURPOSE

This Information Exchange Policy establishes mandatory requirements for the classification, handling, protection, and sharing of cybersecurity incident information between the National SOMCIRT and Critical Infrastructure (CI) Operators using the Traffic Light Protocol (TLP). The objective of this Policy is to enable timely, secure, and effective incident reporting, information sharing, and operational coordination while protecting sensitive technical, operational, and personal information from unauthorized disclosure, misuse, or dissemination.

2. SCOPE AND DEFINITIONS

This Policy applies to all cybersecurity incident-related information exchanged between SOMCIRT and CI operators, including:

a) Initial and follow-up incident reports.

b) Technical artifacts, including logs, Indicators of Compromise (IOCs), malware samples, and forensic images.

c) Situational updates, advisories, alerts, and cyber threat intelligence.

d) Post-incident findings, assessments, and lessons learned.

2.1 TRAFFIC LIGHT PROTOCOL (TLP)

The Traffic Light Protocol (TLP) is a standardized information classification and sharing framework used within the global Computer Incident Response Team (CIRT) community to indicate how information may be shared and distributed.The TLP consists of the classifications, as defined under the Forum of Incident Response and Security Teams (FIRST) TLP Version 2.0.

a) TLP : CLEAR

b) TLP : GREEN

c) TLP : AMBER

d) TLP : AMBER+STRICT, and

e) TLP : RED

For the purpose of this Policy:

» **“Source”** refers to the party originating or providing the information.

» **“Recipient”** refers to any party receiving, accessing, or handling the information.

3. GENERAL PRINCIPLES FOR TLP USE

3.1 All cybersecurity incident-related information exchanged between SOMCIRT and designated Critical Infrastructure (CI) Operators shall be clearly and explicitly labeled with the appropriate Traffic Light Protocol (TLP) classification at the time of dissemination (e.g., TLP:AMBER+STRICT).

3.2 The Source shall be responsible for assigning the appropriate TLP classification based on the sensitivity, potential impact, and intended distribution scope of the information, as well as the minimum audience required to receive and act upon it.

3.3 Recipients shall comply with the restrictions associated with the assigned TLP classification and shall not disclose, redistribute, or share the information beyond the authorized sharing boundaries defined by the applicable TLP designation, unless prior written authorization is obtained from the Source.

3.4 Where information is exchanged without an assigned TLP classification, Recipients shall treat such information as TLP: AMBER by default until the appropriate classification is confirmed by the Source.

3.5 The Traffic Light Protocol (TLP) governs the permitted scope of information sharing and dissemination and does not supersede applicable laws, regulatory obligations, national classification requirements, contractual confidentiality obligations, or data protection and privacy requirements.

4. TLP DESIGNATIONS AND HANDLING RULES

a) TLP: CLEAR

Information classified as TLP:CLEAR may be shared without restriction and is suitable for public disclosure, including public advisories, awareness materials, and high-level cybersecurity guidance.

Sharing and Handling Requirements

» Recipients may share TLP:CLEAR information with any party, including through publicly accessible channels such as websites, publications, and social media platforms.

» Critical Infrastructure (CI) Operators shall ensure that TLP:CLEAR information does not contain sensitive operational, personal, classified, or commercially confidential information prior to disclosure.

b) TLP: GREEN

Information classified as TLP:GREEN may be shared within the broader community or sector but shall not be publicly disclosed. The information is intended to support organizations with similar operational risks, responsibilities, or cybersecurity interests.

Sharing and Handling Requirements:

» Recipients may share TLP: GREEN information within their organization and with trusted partner organizations, sector members, or industry groups that are subject to equivalent confidentiality obligations.

» **TLP : GREEN** information shall not be disclosed through publicly accessible channels, including public websites, media outlets, or social media platforms.

c) TLP: AMBER

Information classified as TLP:AMBER

may only be shared within the Recipient's organization and with relevant clients or stakeholders on a strict need-to-know basis for the purpose of protecting systems, managing risk, or supporting incident response activities.

Sharing and Handling Requirements

» Recipients may share TLP: AMBER information only with individuals within their organization or directly affected entities who require access to the information to manage risk, support operational response, or mitigate the incident.

» TLP: AMBER information shall not be disclosed to the general public, media organizations, or through publicly accessible platforms.

Use in SOMCIRT and CI Operator Information Exchanges

» SOMCIRT will typically classify incident coordination updates, operator-specific technical advisories, and sensitive operational information as **TLP:AMBER**.

» Critical Infrastructure (CI) Operators should classify incident reports, technical indicators, logs, forensic artifacts, and operationally sensitive cybersecurity information as **TLP:AMBER** where controlled sharing is required between SOMCIRT, competent authorities, and authorized internal stakeholders.

d) **TLP: AMBER+STRICT**

Information classified as **TLP:AMBER+STRICT** may only be shared within the Recipient organization on a strict need-to-know basis. This classification is used where the Source requires enhanced control over dissemination due to the sensitivity of the information.

Sharing and Handling Requirements

» Recipients may share TLP:AMBER+STRICT information only with authorized personnel within their own organization who require access to the information for operational, security, or incident response purposes.

» TLP:AMBER+STRICT information shall not be shared with clients, third parties, external partners, service providers, or the public unless prior written authorization is obtained from the Source.

Use in SOMCIRT and CI Operator Information Exchanges

» Due to the sensitivity of cybersecurity incident information, SOMCIRT strongly recommends that Critical Infrastructure (CI) Operators classify detailed incident reports, forensic artifacts, technical indicators, and sensitive operational information submitted to SOMCIRT as TLP:AMBER+STRICT by default, unless otherwise agreed.

» SOMCIRT will classify operator-specific technical feedback, investigation findings, incident coordination details, and sensitive operational advisories as TLP:AMBER+STRICT, except where broader distribution is operationally necessary and explicitly authorized.

e) **TLP: RED**

Information classified as TLP:RED is highly sensitive and may only be shared with specifically designated individuals during a defined meeting, communication, or operational exchange.

Sharing and Handling Requirements

» Recipients shall not disclose, forward, copy, or redistribute TLP:RED information beyond the explicitly authorized individuals identified by the Source.

» Any further sharing of TLP:RED information shall require prior explicit authorization from the Source.

» TLP:RED shall be used only in exceptional circumstances where unauthorized disclosure could significantly increase risks to critical infrastructure, national security, public safety, ongoing investigations, or incident response operations.

Use in SOMCIRT and CI Operator Information Exchanges

» SOMCIRT may classify highly sensitive operational information, law-enforcement-related investigations, or incident details that could materially increase national cybersecurity risk if disclosed as TLP:RED.

» Critical Infrastructure (CI) Operators may request TLP:RED handling for exceptionally sensitive incidents, including active compromises affecting nationally significant systems, during secure briefings, coordination meetings, or protected communication channels.

5. ASSIGNMENT AND REVIEW OF TLP LABELS

» Critical Infrastructure (CI) Operators shall assign an appropriate Traffic Light Protocol (TLP) classification to all incident reports, technical artifacts, and supporting attachments submitted to SOMCIRT, based on the highest sensitivity level of the included information.

» SOMCIRT may review and adjust the assigned TLP classification where necessary to support effective coordination, incident response, or sector-wide awareness activities. This may include downgrading classifications for anonymized or aggregated information sharing purposes; however, SOMCIRT shall not broaden the permitted sharing scope without prior consultation with the originating CI Operator.

» Where incident information has been sufficiently de-identified, sanitized, or aggregated, SOMCIRT may reclassify the resulting information, including sectoral trends, alerts, or advisories, as TLP: GREEN or TLP:CLEAR to facilitate broader cybersecurity awareness, information sharing, and national coordination activities.

6. PROTECTION OF SENSITIVE INCIDENT DATA

» All TLP-classified incident information shall be transmitted using secure communication channels approved or designated by SOMCIRT, including encrypted email, secure portals, VPN-protected interfaces, or other protected communication mechanisms.

» Critical Infrastructure (CI) Operators and SOMCIRT shall implement appropriate technical, administrative, and organizational safeguards to prevent unauthorized access, disclosure, alteration, destruction, or loss of cybersecurity incident information, in accordance with applicable cybersecurity, confidentiality, and data protection requirements.

» Storage of TLP: AMBER, TLP: AMBER+STRICT, and TLP:RED information shall be restricted to secure systems implementing appropriate access controls, authentication mechanisms, logging, monitoring, and retention controls aligned with legal, regulatory, operational, and evidentiary requirements.

» When sharing technical artifacts, including logs, packet captures, malware samples, or forensic data, Critical Infrastructure (CI) Operators shall minimize unnecessary personal information and non-essential commercially sensitive information while preserving the operational, investigative, and forensic integrity of the data.

7. PERMITTED SHARING BY SOMCIRT

7.1 SOMCIRT may share information provided by Critical Infrastructure (CI) Operators, in accordance with the assigned Traffic Light Protocol (TLP) classification, with:

» Relevant national authorities, regulators, and competent government institutions, where required by law, regulatory mandate, or formally established governance arrangements.

» Other Critical Infrastructure (CI) Operators, Sector CERTs, or trusted partners, only where the applicable TLP classification permits such sharing and where the information has been appropriately anonymized, sanitized, or aggregated.

7.2 For information classified as TLP: AMBER or TLP: AMBER+STRICT, SOMCIRT shall:

- Restrict access and sharing to authorized personnel and entities with a defined operational or regulatory need-to-know.
- Apply anonymization, sanitization, or generalization measures prior to any broader dissemination.
- Consult the originating Source before any exceptional disclosure or sharing beyond the permitted TLP boundaries, unless disclosure is required by applicable law or lawful authority.

7.3 For information classified as TLP: RED, SOMCIRT shall not disclose or redistribute the information beyond the specifically authorized individuals directly involved in the incident response, unless disclosure is required by law. Where legally and operationally feasible, SOMCIRT shall inform the originating Source prior to such disclosure.

8. PERMITTED SHARING BY CI OPERATORS

8.1 Critical Infrastructure (CI) Operators shall not disclose, redistribute, or share information originating from SOMCIRT beyond the sharing permissions and restrictions defined by the applicable Traffic Light Protocol (TLP) classification.

8.2 Critical Infrastructure (CI) Operators may internally reclassify SOMCIRT information to a more restrictive TLP designation, including reclassifying information from TLP: AMBER to TLP: AMBER+STRICT or TLP: RED, for internal handling and access control purposes. However, Operators shall not broaden or expand the permitted sharing scope beyond the original TLP classification assigned by SOMCIRT.

8.3 Where Critical Infrastructure (CI) Operators share SOMCIRT information with regulators, supervisory authorities, or other competent government entities, such sharing shall be conducted in accordance with the applicable TLP classification, legal obligations, and confidentiality requirements. Operators shall take reasonable measures to prevent unauthorized onward disclosure or redistribution beyond the authorized recipients, unless required by law or lawful authority.

9. MISLABELING, BREACHES, AND CORRECTIVE ACTIONS

9.1 If a Critical Infrastructure (CI) Operator or SOMCIRT becomes aware that information has been incorrectly classified or mislabeled under the applicable Traffic Light Protocol (TLP) designation, the affected parties shall promptly notify one another and agree on the appropriate corrected TLP classification.

9.2 If any suspected or confirmed unauthorized disclosure, access, redistribution, or compromise of TLP-classified information occurs, it shall be treated as a cybersecurity or information security incident and shall be subject to appropriate containment, investigation, remediation, and notification procedures, including reporting to affected parties and competent regulatory authorities where required.

9.3 If recurring violations, systemic weaknesses, or non-compliance with this Policy are identified, SOMCIRT may issue additional guidance, directives, or binding instructions to address such deficiencies and strengthen compliance with applicable information handling requirements.

10. EFFECTIVE DATE AND REVIEW

10.1 This Policy shall take effect from the date of issuance and shall apply to all subsequent cybersecurity incident-related information exchanges between SOMCIRT and Critical Infrastructure (CI) Operators.

10.2 SOMCIRT will periodically review and update this Policy, including where revisions to the FIRST Traffic Light Protocol (TLP) standard, legal requirements, regulatory obligations, or operational considerations necessitate amendments or improvements.

Hay'adda Isgaarsiinta Qaranka
الـهيئـة الوطنيـة للإتـصالات
National Communications Authority

NATIONAL CYBERSECURITY RISK MANAGEMENT FRAMEWORK