NAM-CSIRT
NAMIBIA CYBER SECURITY INCIDENT RESPONSE TEAM

2026

NATIONAL CYBER SECURITY INCIDENT MANAGEMENT GUIDELINES

Powered by

CRAN
Communications Regulatory Authority of Namibia

TABLE OF CONTENTS

PREFACE

Namibia's economy has witnessed a significant improvement in the use and reliance on digital technology over the years, which was accelerated by the Covid-19 pandemic. Although this has been a significant advantage to development, the scale of digitalisation and connectivity has resulted in several cybersecurity breaches that threaten the public, private businesses, and the government. Cyber threats represent a principal and growing disruptive threat to Critical Infrastructure/Critical Information Infrastructure (CI/CII) and other essential services. It is necessary for the operators of Namibia's national and local infrastructure to understand and protect their critical assets, understand the cyber threats to their organisation, the risk to their infrastructure, manage the risk from their supply chain, and recognise staff as a potential access route.

As high-profile targets, operators of CI/CII and private and public entities face the challenge of maintaining robust security while ensuring reliable and efficient services for their customers. Cybercrime now poses a persistent and evolving threat, with attackers employing increasingly sophisticated tactics to exploit vulnerabilities. Recent statistics confirm that operators of CI/CII and their customers are among the most targeted globally. The surge in public sector attacks has raised concern and requires a response to ensure good cyber hygiene.

In response to the growing threat landscape, NAM-CSIRT created these National Cyber Security Incident Management Guidelines 2026. These Guidelines were formulated to provide a comprehensive framework for establishing effective cybersecurity protocols and procedures for operators of CI/CII and public and private entities to protect their critical infrastructure.

The Guidelines set out clear expectations for routine and emergency scenarios, inter- and intra-company communication, coordination with the Authority as the National CSIRT, incident reporting mechanisms, and the safeguarding of data and network integrity. By adhering to these Guidelines, operators of CI/CII, government OMAs, and public and private entities can strengthen their resilience against cyber threats, foster trust with stakeholders, and contribute to a secure and stable cybersecurity ecosystem in Namibia.

Additionally, the Guidelines stress that operators of CI/CII, government OMAs, and public and private entities must have adequately planned and prepared for the disruptions a potential cyberattack could have on their organisation and should test cyber threat incident response plans to ensure the effective response and recovery of the organisation, reducing disruption of services.

Namibia, like any other country, is exploiting the opportunities, and facing the security challenges, that come with constantly developing ICT infrastructure. Furthermore, the country's limited resources, technological dependence, high vulnerability, low cybersecurity awareness, few skilled cybersecurity experts, and underdeveloped research work, all pose additional cybersecurity risks.

To ensure security, a risk-based approach to planning, preparation, response, and recovery will help entities understand their vulnerability to cyberattacks and take appropriate measures. Key to taking a risk-based approach is understanding the nature of the cyber threat to the organisation.

Appetite for cyber hygiene as a collective effort requires deliberate action to ensure trust of citizens, customers, and service providers within the digital services, and guarantee sovereign state protection.

ACKNOWLEDGEMENTS

The *National Cyber Security Incident Management Guidelines* were authored by the 2024C CRAN team under the Swedish Programme for ICT in Developing Regions (SPIDER) in collaboration with the Namibia Cyber Security Incident Response Team (NAM-CSIRT).

The drafting team extends its sincere appreciation to SPIDER and the Communication Regulators' Association of Southern Africa (CRASA) for their invaluable technical and strategic support throughout the drafting process.

Special thanks are also due to the Executive Management and Board of the Communications Regulatory Authority of Namibia (CRAN) for availing both human capital and financial resources that made the development and finalisation of these guidelines possible.

Date of First Publication – April 2026

1.

KEY ACRONYMS AND DEFINITIONS

1.1 ACRONYMS

ACM	Access Control Matrix
AfricaCERT	African Forum of Computer Emergency Response Teams
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BYOD	Bring Your Own Device
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIRT	Cyber Incident Response Team
CIRTs	Cyber Incident Response Teams
CRAN	Communications Regulatory Authority of Namibia
CRASA	Communications Regulators' Association of Southern Africa
CSP	Cloud Service Provider
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
EDR	Endpoint Detection and Response
FIRST	Forum of Incident Response and Security Teams
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDR	Intrusion Detection and Response
INSA	Information Network Security Agency
IOC/IOCs	Indicator(s) of Compromise
IP	Internet Protocol
ISMS	Information Security Management System(s)
ISSC	Information Security Steering Committee
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MoU	Memorandum of Understanding
NAM-CSIRT	Namibia Cyber Security Incident Response Team
NIST	National Institute of Standards and Technology
OMAs	Offices, Ministries and Agencies
OSINT	Open-Source Intelligence
PCI-DSS	Payment Card Industry Data Security Standard
POS	Point of Sale
R&D	Research and Development
SADC	Southern African Development Community
SADC CIRT	Southern African Development Community Computer Incident Response Team
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Centre
TLP	Traffic Light Protocol
TTPs	Tactics, Techniques, and Procedures
UNODC	United Nations Office on Drugs and Crime
XDR	Extended Detection and Response

1.2 DEFINITIONS

The Authority refers to the Communication Regulatory Authority of Namibia (CRAN).

Business continuity means a state of continued and uninterrupted operation of business functions despite disruptive incidents.

Critical Infrastructure (CI) refers to systems and assets, networks, services, and installations that, if disrupted or destroyed, would have a significant impact on the country's security, economy, or public welfare.

Critical Information Infrastructure (CII) refers to interconnected information systems and networks which are essential for the maintenance of vital societal functions (health, safety, security, economic, or social well-being of people), the disruption of which would have serious impact on the economic well-being of customers or on the effective functioning of payment service providers and the economy.

Critical asset means facilities, systems, and equipment which, if destroyed, degraded, or rendered unavailable, would affect the reliability or operability of an institution.

Cyber means computers, electronic systems, the Internet, and any data, services, or activities that exist or operate within the virtual or digital environment.

Cyberattack means activities undertaken to bypass or exploit deficiencies in a digital system's security mechanisms to compromise confidentiality, integrity, or availability.

Cybersecurity means the collection of tools, policies, actions, systems, best practices, assurance, and processes used to protect the cyber environment and organisational assets, minimising vulnerabilities of critical network, systems, and information assets and resources.

Cyberspace means the virtual environment comprising interconnected information systems, infrastructures, and users who create, access, and utilise information.

Cyber threat means any potential occurrence that may compromise the security of a network, system, or digital asset.

Cybersecurity incident is an unwanted or unexpected cybersecurity event, or a series of such events, that has compromised business operations or has a significant probability of compromising business operations.

Cybersecurity Risk Register means a catalogue or database of cybersecurity threats which is kept and maintained by the operators of CI/CII, government ministries, offices and agencies (OMAs), and public and private entities.

Cyber Incident Reporting Platform means the reporting platform provided by NAM-CSIRT, accessible via the email address report@nam-csirt.na.

Cybersecurity information sharing is the structured exchange of threat, vulnerability, and mitigation information among stakeholders to foster collective cyber resilience.

Entity/Entities refers to operators of CI/CII, government OMAs, and public or private sector organisations in Namibia.

Incident Management refers to the process of detecting, analysing, and resolving unplanned service interruptions or disruptions to minimise business impact and restore services to normal operations.

Incident Response is the strategic action taken to detect, contain, eradicate, and recover from cybersecurity incidents, minimise damage, and prevent recurrence.

Point of Contact means the designated contact point established for incident response coordination with the CI/CII owners.

Vulnerability refers to weaknesses in an information system, security procedure, internal control, or configuration that could be exploited by a threat actor.

National CSIRT refers to the Namibia Incident Response Team (NAM-CSIRT).

2.

BACKGROUND AND PURPOSE OF GUIDELINES

2.1 INTRODUCTION

Cybersecurity profoundly affects national peace, development, and democracy. As government, businesses, and citizens increasingly depend on digital technologies for communication, financial transactions, health services, and governance, the integrity and resilience of Namibia's cyberspace have become essential to national sovereignty, public trust, and sustainable economic growth.

The pace of digitalisation across sectors has strengthened efficiency and inclusion but has simultaneously exposed critical systems and services to growing levels of cyber risk. The convergence of networks, devices, and data has amplified the potential impact of cyberattacks on CI/CII, including telecommunications, financial systems, energy, transport, health, and public administration.

Recognising the centrality of cybersecurity to national stability and economic advancement, Namibia affirms that protecting its digital ecosystem is a strategic regulatory and national-security imperative. The nation must therefore adopt a coordinated, proactive, and risk-based approach to safeguard its infrastructure, institutions, and citizens from malicious cyber activities.

These Guidelines provide a comprehensive framework for establishing effective cybersecurity protocols and procedures to strengthen resilience, enhance coordination, and build capacity across all sectors.

They are intended for application by:

- Operators of CI/CII
- Government OMAs
- Private sector entities

Specifically, the Guidelines seek to:

(i) Develop a strong cybersecurity culture across organisations and sectors.
(ii) Identify and manage risks associated with assets, systems, and services.
(iii) Implement effective controls to prevent and mitigate cyber threats.
(iv) Detect, analyse, and respond to cybersecurity incidents in a structured manner.
(v) Coordinate national response mechanisms through the Namibia Cyber Security Incident Response Team (NAM-CSIRT).
(vi) Foster collaboration and information sharing among stakeholders.
(vii) Enhance public trust and service reliability within Namibia's digital economy.

NAM-CSIRT was established in line with the Cabinet directive to be housed under the Communications Regulatory Authority of Namibia (CRAN). NAM-CSIRT serves as the national focal point for the prevention, detection, analysis, coordination, and response to cybersecurity incidents affecting Namibia's CI/CII, government entities, and the private sector.

CRAN, as the designated national regulatory authority, provides oversight and operational hosting of NAM-CSIRT, ensuring that incident management, threat response, and national coordination are implemented within a coherent regulatory and technical framework. This mandate aligns with the Electronic Transactions Act, 2019 (Act No. 4 of 2019) and the Communications Act, 2009 (Act No. 8 of 2009), which empower CRAN to prescribe and enforce security and technical standards essential for public safety, service reliability, and national security.

NAM-CSIRT's coordination mandate encompasses the following key functions:

ROLE	FUNCTION
National Focal Point for Cybersecurity	Serves as Namibia's single point of contact for cybersecurity incident reporting, coordination, and crisis communication.
Sectoral Collaboration and Constituency Support	Facilitates structured cooperation with sector-specific Cyber Incident Response Team (CIRTs), operators of CI/CII, and government OMAs through formal constituency frameworks.
Advisory and Early Warning Function	Issues national advisories, alerts, and vulnerability bulletins to enable timely defensive measures.
Incident Analysis and Technical Coordination	Conducts incident triage, root-cause analysis, threat attribution, and coordination of containment and recovery measures.
Capacity Building and Preparedness	Leads training, awareness programmes, and cyber-drills to enhance national readiness in line with International Telecommunication Union Standardization Sector (ITU-T) Recommendation X.1051 and National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0.
International and Regional Cooperation	Represents Namibia within the Southern African Development Community Cyber Incident Response Team (SADC CIRT), African Forum of Computer Emergency Response Teams (AfricaCERT), and the Forum of Incident Response and Security Teams (FIRST), promoting cross-border collaboration and harmonised response procedures.
Policy Advisory and Research	Provides technical input to national cybersecurity policies and supports research and innovation for continual improvement.

2.2 PURPOSE OF THE GUIDELINES

The purpose of these Guidelines is to establish a clear and harmonised national framework for cybersecurity incident handling and management in Namibia. These include a framework for detecting, reporting, analysing, managing, and resolving cybersecurity incidents affecting Namibia's CI/CII and other essential digital systems.

The Guidelines serve as a practical instrument to strengthen national cyber resilience by defining the minimum standards, roles, and procedures that must be observed when responding to cybersecurity incidents, considering increasing digitalisation, the evolving cyber threat landscape, and the need to enhance cyber resilience.

They provide operational direction for:

(i) Developing institutional incident response frameworks aligned to international standards.
(ii) Establishing clear incident reporting channels between operators and NAM-CSIRT.
(iii) Ensuring timely coordination and escalation during cybersecurity incidents of national significance.
(iv) Enhancing situational awareness, information sharing, and national threat intelligence.
(v) Supporting continuity of essential services and public trust in Namibia's digital ecosystem.

The Guidelines aim to:

(i) Strengthen Namibia's national cyber resilience by ensuring a coordinated, risk-based, and proactive approach to cyber incident management.
(ii) Promote the integrity, availability, and confidentiality of systems and data that underpin national economic and social stability.
(iii) Support operators of CI/CII, government OMAs, and private sector entities to anticipate, prevent, detect, and respond effectively to cybersecurity incidents.
(iv) Enhance public confidence in Namibia's digital environment by ensuring consistent standards for incident preparedness, reporting, and response.
(v) Facilitate national, regional, and international cooperation through structured engagement with the SADC CIRT, AfricaCERT, and FIRST communities.

The Guidelines are non-binding but highly instructive. They complement existing laws and regulations by providing a common operational baseline for all sectors, ensuring alignment with:

- the Electronic Transactions Act, 2019 (Act No. 4 of 2019)
- the Communications Act, 2009 (Act No. 8 of 2009)
- the National Cybersecurity Strategy and Awareness Raising Plan, 2022

and international best-practice standards such as:

- ISO/IEC 27001, ITU-T Recommendation X.1051
- the NIST Cybersecurity Framework (CSF) 2.0

3.

OBJECTIVE OF THE GUIDELINES

3.1 OVERARCHING OBJECTIVES

The general objectives of these Guidelines are to:

(i) Safeguard the confidentiality, integrity, and availability of Namibia's national digital infrastructure, systems, and data.

(ii) Enhance national preparedness and resilience against cybersecurity incidents and emerging digital threats.

(iii) Establish a coordinated national approach for incident prevention, detection, reporting, and response across both public and private sectors.

(iv) Promote trust and transparency through secure information sharing between NAM-CSIRT, sectoral CIRTs, and operators of CI/CII.

(v) Strengthen institutional accountability by setting minimum cybersecurity and reporting standards applicable to all critical sectors.

(vi) Ensure continuity of essential services during and after cybersecurity incidents.

(vii) Promote alignment with regional and international frameworks, including SADC CIRT, AfricaCERT, and FIRST, to enhance Namibia's participation in the global cybersecurity ecosystem.

(viii) Support CRAN's regulatory mandate to develop and enforce national cybersecurity standards consistent with international best practice.

3.2 SPECIFIC OBJECTIVES

To achieve the above, these Guidelines seek to:

(i) Define a national incident management framework that standardises incident identification, classification, and escalation procedures.

(ii) Establish minimum technical and procedural controls for cyber incident handling and response.

(iii) Strengthen communication, coordination, and reporting mechanisms between regulated entities and NAM-CSIRT.

(iv) Promote the development of internal Cybersecurity Incident Response Teams (CSIRTs) or focal points within organisations.

(v) Encourage the use of risk-based approaches to cybersecurity incident prevention, management, and recovery.

(vi) Ensure that incident reports and threat intelligence are collected and disseminated securely and efficiently to relevant stakeholders.

(vii) Enhance cybersecurity awareness, education, and training for staff and executives across public and private sectors.

(viii) Facilitate information exchange and trust-based cooperation between CRAN, industry operators, and other national and regional bodies.

(ix) Support post-incident evaluation and continuous improvement through lessons learned, technical reviews, and procedural updates.

(x) Establish mechanisms for early warning, cross-border cooperation, and rapid response in collaboration with SADC CIRT, AfricaCERT, and FIRST.

4.

GUIDING PRINCIPLES, USE OF GUIDELINES, AND APPLICABILITY

4.1 GUIDING PRINCIPLES

Implementation of these Guidelines shall be guided by the following principles:

PRINCIPLE	DESCRIPTION
1. National Sovereignty	Protection of Namibia's digital assets and infrastructure as a matter of national security and economic stability.
2. Collaboration and Trust	Promoting mutual confidence between the regulator, operators, and stakeholders through non-punitive reporting and transparent communication.
3. Accountability	Ensuring that all entities take responsibility for the security and resilience of their systems.
4. Proportionality	Adopting risk-based measures commensurate with the nature and sensitivity of the assets being protected.
5. Regional Cooperation	Aligning Namibia's cybersecurity posture with SADC and African Union frameworks for digital cooperation.
6. Continuous Improvement	Encouraging periodic review, learning, and adaptation of cybersecurity practices in response to evolving threats and technologies.

4.2 HOW TO USE THESE GUIDELINES

These Guidelines provide both policy direction and technical guidance that entities may adopt to enhance their cyber resilience and incident response capability.

They outline minimum expectations and recommend best practices that entities should implement in alignment with their size, operational complexity, and risk exposure. While certain provisions are instructive for compliance under existing legal instruments, others are advisory in nature, providing flexibility for adaptation within institutional contexts. Entities are therefore encouraged to:

(i) Integrate the Guidelines into their existing cybersecurity frameworks, risk management processes, and business continuity plans.

(ii) Establish internal policies and procedures that align with the principles, controls, and reporting mechanisms described in the Guidelines.

(iii) Scale implementation according to organisational capacity, ensuring that smaller entities meet minimum standards while larger or high-risk entities adopt advanced practices.

(iv) Maintain coordination and communication with NAM-CSIRT for incident reporting, threat intelligence sharing, and post-incident analysis.

(v) Conduct regular reviews and simulations to ensure operational readiness and continuous improvement in response and recovery capabilities.

(vi) Reference the annexes for technical and procedural details, including incident classification, reporting templates, and response cycle guidance.

The Guidelines should be read in conjunction with relevant legislation, regulatory instruments, and sector-specific policies. They are designed to complement, not replace, existing cybersecurity, ICT, or operational standards already in force.

By applying these Guidelines, entities contribute to a cohesive national cybersecurity posture that enhances Namibia's digital resilience, protects critical assets, and strengthens collective trust in the national cyber ecosystem.

4.3 APPLICABILITY

These Guidelines apply to:

(i) Government OMAs responsible for national and sectoral digital systems and e-services.

(ii) Operators of CI/CII that support essential services such as telecommunications, energy, education, transport, finance, health, and water.

(iii) Private-sector entities whose operations rely on digital platforms or data systems that may affect national stability or service delivery.

While the Guidelines are non-binding, all covered entities are strongly encouraged to align their internal incident management procedures to this framework. The Authority may revise or expand the Guidelines periodically to maintain consistency with emerging threats, technologies, and regional developments.

5.

SOURCES OF CYBER RISK

5. SOURCES OF CYBER RISK

Cyberattacks against organisations' information systems have placed the abuse of cyberspace high on domestic and international agendas. Some examples of internal and external cyber threat risks, including those caused by cybercrime activities, include but are not limited to:

(i) Human threats, including inadequately trained personnel that might poorly perform tasks or misconfigure systems and networks, leading to high-risk cyber errors both unintentional and intentional (e.g., data theft by an insider).

(ii) Lack of, or inadequate, personnel or staff awareness on cyber hygiene, internal policies, and ethical conduct of digital assets.

(iii) Third-party cyber risks which, due to the interconnectedness of institutions, could compromise the institutions' entry points (e.g., through service providers).

(iv) Cyber criminals acting toward the corruption of data, limiting access to systems, and disrupting businesses.

(v) Espionage of advanced persistent threats from attack groups motivated to exploit systems and networks (e.g., ransomware groups).

(vi) Lack of security controls, and procedures that lead to software errors, technical failures, hardware flaws, unauthorised access, and possibly compromised digital assets.

(vii) Manipulating and tricking people to reveal information (e.g., password or financial information) that can be used to attack systems or networks through social engineering.

6.

POLICY AND LEGAL FRAMEWORK

6. POLICY AND LEGAL FRAMEWORK

The Authority's mandate for cybersecurity governance and coordination is derived from several key legal instruments that collectively empower CRAN to oversee, prescribe, and enforce cybersecurity standards across the national digital ecosystem.

Foremost among these is the Electronic Transactions Act which, under Section 45, mandates CRAN to prescribe and enforce security standards for accredited service providers and digital platforms. This provision ensures the protection of data integrity, confidentiality, and authentication mechanisms within electronic communication and transaction environments. Complementing this, the Communications Act, under Section 37, authorises the Authority to establish technical and operational standards for telecommunications and broadcasting networks, thereby safeguarding public safety, ensuring service reliability, and reinforcing national security.

Further, the Cabinet Directive on Cybersecurity and CI Protection mandates CRAN to serve as the national coordinator for cybersecurity incident response and prevention across both public and private sectors, strengthening institutional coordination in the protection of national information assets. Additionally, the data protection and cybercrime provisions embedded within relevant national legislation and subsidiary instruments reinforce institutional accountability for safeguarding critical digital infrastructure and maintaining public trust in digital systems.

Together, these instruments form the legal foundation for CRAN's authority to issue guidelines, directives, and procedures governing cybersecurity standards, incident management, reporting obligations, and sectoral coordination across Namibia's critical information and communications ecosystem.

6.1 INTERNATIONAL STANDARDS AND BEST PRACTICES

Operators are encouraged to align with the following international standards:

ISO/IEC 27001 Information Security, Cybersecurity, and Privacy Protection

The ISO/IEC 27001 is the international standard for information security management systems (ISMS) set by the International Organisation for Standardisation (ISO) and defines the requirements that ISMSs must meet. The standard provides companies of any size and from all sectors with guidance for establishing, implementing, maintaining, and continually improving information security management systems. An organisation or business that conforms with ISO/IEC 27001 has implemented a system to manage risks related to the security of data owned or handled by the company and ensures that this system respects all the best practices and principles enshrined in the standard. While ISO/IEC 27001 outlines the requirements for an ISMS, ISO/IEC 27002 offers control objectives related to cybersecurity aspects of an ISMS.

The NIST Cybersecurity Framework (CSF) 2.0

The United States' National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) is a guide for identifying and describing an organisation's current and target cybersecurity posture, based on a detailed taxonomy of high-level cybersecurity outcomes (NIST, 2024). These outcomes can be understood by a broad audience, regardless of their cybersecurity expertise. The NIST CSF aids in identifying the outcomes for addressing the unique cybersecurity risks of a specific organisation. It does not describe how these outcomes can be achieved but provides links to online resources accessible through the NIST CSF website.

MITRE ATT&CK Framework

The Adversarial Tactics, Techniques, and Common Knowledge or MITRE ATT&CK is a guideline for classifying and describing cyberattacks and intrusions. The framework enhances the understanding of how cyber attackers think and work. The MITRE framework is a globally accessible, continuously updated knowledge base of adversarial tactics, techniques, and procedures (TTPs) based on real-world cybersecurity incidents and observations. It serves as a common language for cybersecurity professionals to understand and model attacker behaviours across enterprise, mobile, cloud, and industrial control systems, enabling better threat detection, assessment of security readiness, and the development of more effective defence strategies.

Payment Card Industry Data Security Standard (PCI-DSS)

The Payment Card Industry Data Security Standard (PCI-DSS) 4.0 is a set of rules and guidelines designed to help organisations that handle credit card information keep that information safe and secure. PCI-DSS guidelines are essential to protect against data breaches, credit card fraud, and protect cardholder data. They consist of a set of technical and operational requirements designed to reduce credit card fraud for organisations that store, process, or transmit credit and debit card information. Administered by the Payment Card Industry Security Standards Council, PCI-DSS is a global standard that all financial businesses, regardless of size, must follow to accept payment cards. Compliance helps prevent data breaches, maintain customer trust, and avoid significant fines for non-compliance.

Centre for Internet Security (CIS) Benchmarks

The Centre for Internet Security (CIS) Benchmarks are a set of globally recognised and consensus-driven best practices to help security practitioners implement and manage their cybersecurity defences. These consensus-driven guidelines, known as CIS Benchmarks, provide actionable rules for various technologies, helping organisations harden systems, reduce cyber risks, and meet industry security standards.

6.2 REGIONAL AND INTERNATIONAL COOPERATION

Cyber threats are transnational and require coordinated regional and global responses. Namibia's participation in regional cybersecurity frameworks is therefore essential to ensure early warning, information sharing, and collective incident response capabilities.

NAM-CSIRT pursues regional integration and international collaboration through the following mechanisms:

(a) AfricaCERT:

NAM-CSIRT participates in AfricaCERT, the continental coordination hub for cybersecurity response teams. Through this platform, Namibia accesses shared threat intelligence, capacity-building programmes, and joint cyber-drill exercises with peer African CERTs.

(b) SADC CIRT: Regional Computer Incident Response Team:

NAM-CSIRT participates in SADC CIRT, the regional coordination hub for cybersecurity response teams within SADC. Through this platform, Namibia accesses shared capacity-building programmes, high-level impact incident response support, and joint cyber-drill exercises with SADC member states.

(c) Forum of Incident Response and Security Teams (FIRST):

NAM-CSIRT aligns with FIRST principles and participates in the global community of incident response teams for knowledge exchange, peer collaboration, and adherence to international best practices.

(d) Bilateral and Multilateral Partnerships:

NAM-CSIRT maintains bilateral cooperation agreements with peer institutions, international organisations such as the International Telecommunication Union (ITU), the United Nations Office on Drugs and Crime (UNODC), and the International Criminal Police Organization INTERPOL, as well as development partners, to support technical exchange, training, and infrastructure development.

7.

MANDATE OF NAM-CSIRT

7. MANDATE OF NAM-CSIRT

(i) NAM-CSIRT shall provide support and guidance to a CI/CII either through constituent collaboration and partnership agreements or directly to the designated CI/CII owner pursuant to the implementation of these guidelines.

(ii) NAM-CSIRT has the overall oversight responsibility to ensure the implementation of the Guidelines through collaboration with the constituents, international institutions, or directly with the designated CI/CII owners.

(iii) NAM-CSIRT is responsible for coordinating with relevant sectoral stakeholders to produce coherent guidelines, directives, reports, and engagement with CI/CII owners.

8.

CYBERSECURITY INCIDENT MANAGEMENT

8.1 INCIDENT MANAGEMENT HANDLING LIFE CYCLE

An incident handling process is a structured life cycle of cybersecurity incident management, typically involving the following phases: preparation, identification, containment, eradication, recovery, and other post-incident activity. Incident handling consists of all tasks required to handle an incident, which include the below:

(i) Detection and Reporting: receiving, tracking, and reviewing event information, alerts, and reports.
(ii) Triage Phase: prioritising, categorising, and assigning the event to respective personnel and support team.
(iii) Analysis Phase: determining the type of threat, root cause, impact and damage caused, recovery, remediation, and mitigation to be affected.
(iv) Incident Response Phase: coordinating and disseminating information, resolving or mitigating the incident, and taking record of lessons learned.

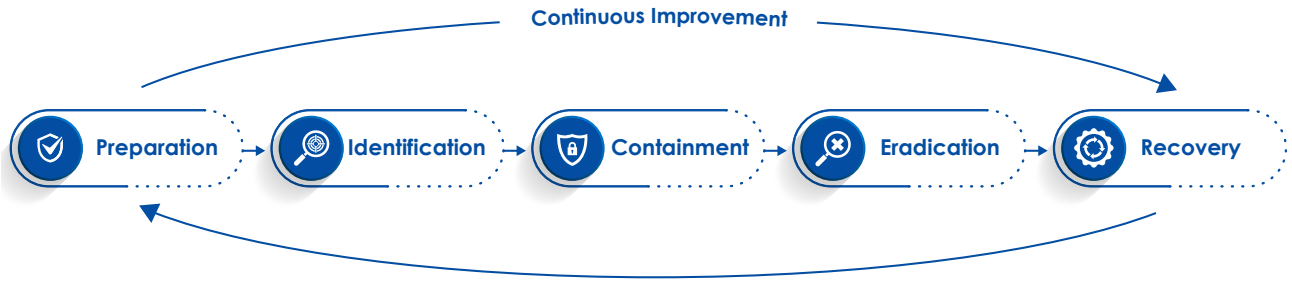

Figure 1: Incident Management Handling Life Cycle

Further guidance of the incident response phase is provided in Appendix 2.

8.2 INCIDENT MANAGEMENT PREPAREDNESS

An incident management plan forms a key component in an organisation's broader risk-management framework. It focuses on planning, preparedness, and the timely identification of events that fall outside normal operations. Its primary objective is to reduce the impact of such incidents and support a swift return to standard business activities.

Organisations must minimise the time required to identify, analyse, respond to, and recover from incidents. Reducing these timelines directly decreases the operational and financial impact associated with disruptions. It is therefore essential that leadership ensures the existence of well-designed and properly maintained incident response plans and procedures.

Effective incident response also requires adequate resources, including:

- trained personnel
- adherence to compliance obligations
- consideration of the organisation's operational nature and geographic location
- an appropriate level of cybersecurity maturity

Typically, organisations with higher regulatory demands, greater size, and mature cybersecurity capabilities are better positioned to dedicate infrastructure, personnel, and processes toward effective incident management.

There is no single, universally applicable structure for incident management. In addition to these Guidelines, each entity must develop and implement an incident management programme and response plan tailored to its operational context, industry requirements, and risk environment.

Operators of CI/CII and other entities must be prepared to respond to and manage incidents in a manner that enables timely recovery and continuity of essential services. The evolving and unpredictable nature of cyber threats further requires leadership to ensure that incident management practices and response capabilities are aligned with organisational strategy and adequately protect stakeholders.

Effective incident management and response capabilities must integrate baseline security controls, business continuity arrangements, and disaster recovery processes. A robust incident management capability is essential for meeting recovery time and recovery point objectives and plays a critical role in enhancing overall cyber resilience.

8.2.1 Control: Incident Response Capability and Preparation

(a) Operators of CI/CII and private entities must be prepared and able to respond to detected cyberattacks through appropriate incident response procedures to limit the adverse effects of, and enable recovery from, a network compromise. This incident response capability must cover all phases of incident response, namely preparation, identification, containment, eradication, and recovery, and should:

(i) Maintain an up-to-date incident response plan approved by management and annually reviewed.
(ii) Assign roles and responsibilities for incident response within the organisation.
(iii) Ensure availability of incident detection tools for incident handling.
(iv) Maintain contact list with NAM-CSIRT, sector CERTS (if applicable), relevant regulators, and law enforcement.
(v) Conduct regular simulation exercises for incident response teams.
(vi) Implement continuous monitoring to identify potential abnormalities and indicators of compromise.
(vii) Classify incidents based on their impact, urgency, and response needed.
(viii) Highlight all incident response phases (i.e., preparation, identification, containment, eradication and recovery) and lessons learned.
(ix) Able to suspend or disable network access to compromised end users or devices.
(x) Maintain copies of critical configuration or user information which can be used to restore service connectivity and information access.
(xi) Limit, throttle, filter, or block certain traffic flows to mitigate any service degradation that may occur.
(xii) Identify and notify any impacted customers about the event and the estimated timeframe for resolution, confirming when the matter has been resolved.

(b) Operators of CI/CII and private entities must have the capacity to respond to incidents, both internal and external to their networks, and are required to have well-defined, repeatable processes for responding to these events as part of their cybersecurity plans. Operators of CI/CII and private entities must be able to respond to security incidents during working and off hours, as part of the network security plans.
(c) Learning and evolving operators of CI/CII and private entities must:

Ensure that cybersecurity and cyber resilience frameworks are adaptive and evolve with the dynamic nature of cyber risk to identify, assess, and manage security threats.

(i) Ensure continuous learning from previous cyber incidents and events to ensure that their security systems are improved to increase resilience.
(ii) Keep abreast with new cyber risk management processes and continually monitor technological developments that effectively counter existing and emerging forms of cyberattacks.
(iii) Ensure there are reasonable measures to include predictive and anticipatory capabilities that extend beyond reactive controls and include proactive protection against future cyber events in the risk management practices.

8.3 INCIDENT DETECTION

The purpose of this subdomain is to ensure necessary controls are in place to activate, protect, and maintain the cybersecurity event logs within networks, systems, and applications. In addition, this subdomain ensures that monitoring is conducted to required events within the networks, systems, and applications to identify any suspicious behaviour which may lead to cybersecurity incidents.

8.3.1 Control: Detecting Cybersecurity Incidents

(a) One of the core elements of detecting and investigating cybersecurity incidents is the availability of appropriate data sources and implementation of technologies such as an intrusion prevention system, Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), firewall policy logs, and event logs. It is important to identify event logs that can be used by an organisation to assist with detecting and investigating cybersecurity incidents, such as:

- Cross Domain Solutions
- Domain Name System Services
- Email Servers
- Gateways
- Multifunction Devices
- Operating Systems
- Remote Access Services
- Security Products
- Server Applications
- System Access
- User Applications
- Web Applications
- Web Proxies

(b) Operators of CI/CII and private entities shall establish capability for ongoing (24/7) monitoring of their IT systems, infrastructure, applications, services, and other relevant components to promptly detect anomalies or cyber incidents. This capability can be outsourced to a third-party provider or managed internally. Regardless of the chosen approach, the entity management shall ensure the monitoring is adequate to detect cyber threats.

8.3.2 Control: Know Your Environment

An entity should proactively familiarise itself with its business environment and identify its critical assets. To ensure effective security measures, operators of CI/CII and private entities shall establish mechanisms for maintaining up-to-date inventory of authorised software, hardware, and internal and external network connections. Additionally, an entity shall identify and document its data, assets, and capabilities, and potential threats and vulnerabilities associated with its assets should be monitored. Employees and contractors providing information technology and cybersecurity services shall also be identified and documented. Details on specific controls are contained in Appendix 1.

8.4 MANAGING CYBERSECURITY INCIDENTS

Operators of CI/CII and private entities' networks and facilities carry different forms of network traffic, confidential and/or personal data storage, and information infrastructure that support the services they provide. They therefore should be able to manage their critical assets to detect malicious behaviour and activity to protect them from external and internal threats.

This subdomain sets out appropriate controls for ensuring that operators of CI/CII and private entities maintain a robust organisational capacity to respond to a cybersecurity incident quickly and effectively. This response capability must not only be able to effectively address the immediate cyber threat under a wide variety of adverse circumstances but must also anticipate a wide variety of post incident measures that are likely to be necessary.

8.4.1 Control: Development and Maintenance of Cybersecurity Strategic Plans and Cyber Incident Response Plan

(i) As part of the preparation to secure their networks and respond to incidents, operators of CI/CII and private entities will be required to develop strategic cybersecurity plans which includes a cyber incident response plan that must be endorsed by senior leadership and their Board of Directors.

(ii) The cyber incident response plan must identify a cyber incident response team that is responsible for assessing and responding to cyber incidents. If the entity is large or complex, where this function may be fulfilled by multiple teams, the division of responsibilities must be made clear.

(iii) The cyber incident response plan shall detail the specific measures that operators of CI/CII and private entities will implement to ensure that their networks and corresponding elements are secure, detailing: access is restricted to those who are not authorised; critical network infrastructure is hardened and protected as far as reasonably possible; how the security of the network and threats, attacks, and compromises will be monitored and logged; how operators of CI/CII and private entities will respond to incidents, whether purely at threat stage or if an actual cyberattack has occurred; and how the security of the network will be continually tested and updated.

(iv) Operators of CI/CII and private entities must document the cyber incident response plan and procedures relating to the securing of their networks from cyber threats and attacks, either as part of existing network development and quality of service plans, or as a separate and dedicated plan addressing how the network will be developed and maintained, and quality of service assured in relation to cybersecurity.

(v) The cyber incident response plan must set out clear cybersecurity procedures and include those related to the response to cyberattacks and the reporting of the cyberattacks.

(vi) The cybersecurity strategic plans and cyber incident response plan shall be developed within one year of these Guidelines being effective, or when operators of CI/CII and private entities are directed to do so by the Authority. Plans should also be reviewed at least annually, or when a major threat is identified, to ensure they are relevant to the threat assessment conducted or published by NAM-CSIRT and other recognised cybersecurity authorities and resources. In addition to the plans being reviewed, the independent testing of the networks and systems under the plans is also to be conducted.

(vii) Under the cyber incident response plan, operators of CI/CII and private entities should conduct annual independent ICT security assessments of their networks and related systems under such a plan, which can include simulations, vulnerability assessments, security penetration testing, governance and access control reviews, and security monitoring and detection audits.

8.4.2 Control: Cybersecurity Incident Management Policy

Establishing a cybersecurity incident management policy can increase the likelihood of successfully planning for, detecting, and responding to malicious activity on networks and hosts, such as cybersecurity events and incidents. A cybersecurity incident management policy should cover the following:

(i) Responsibilities for planning for, detecting, and responding to cybersecurity incidents.

(ii) Resources assigned to cybersecurity incident planning, detection, and response activities.

(iii) Guidelines for triaging and responding to cybersecurity events and incidents.

Furthermore, as part of maintaining the cybersecurity incident management policy, it is important that it is, along with its associated cybersecurity incident response plan, exercised at least annually to ensure it remains fit for purpose.

8.4.3 Control: Cybersecurity Incident Register

Developing, implementing, and maintaining a cybersecurity incident register can assist with ensuring that appropriate remediation activities are taken in response to cybersecurity incidents. In addition, the types and frequency of cybersecurity incidents, along with the costs of any remediation activities, can be used as an input to future risk assessment activities.

A cybersecurity incident register contains the following for each cybersecurity incident:

Date and time of incident	The date the cybersecurity incident was discovered.
Description of incident	A description of the cybersecurity incident.
Contact person	A central contact person to whom the cybersecurity incident was reported.
Existing controls and remedial action	A list of existing measures and any actions taken in response to the cybersecurity incident.
Notifications	A summary of notifications that have been made and to whom (data protection authority, affected individual, third parties).
External parties involved	Information about the nature and role of the organisation and the external parties that may be affected and therefore need to be informed.

8.4.4 Control: Insider Threat Mitigation Programme

As an insider's authorised access to systems and their resources may make them harder to detect when intentionally performing malicious activities, establishing and maintaining an insider threat mitigation programme can assist an organisation to detect and respond to insider threats before they occur, or limit damage if they do occur. In doing so, an organisation will obtain the most benefit by logging and analysing the following user activities:

(i) Excessive copying or modification of data.
(ii) Unauthorised or excessive use of removable media.
(iii) Connecting devices capable of data storage to systems.
(iv) Unusual system usage outside of normal business hours.
(v) Excessive data access or printing compared to their peers.
(vi) Data transfers to unauthorised cloud services or webmail.
(vii) Use of unauthorised Virtual Private Networks, file transfer applications, or anonymity networks.

8.5 INCIDENT MANAGEMENT COORDINATION AND GOVERNANCE

It is incumbent on all operators of CI/CII, government OMAs, private entities, and other stakeholders concerned to implement an incident management governance structure.

It is important that the roles and responsibilities in case of a cybersecurity incident are documented in the cybersecurity incident response plan. When drafting the description of these roles and responsibilities, the following questions should be asked:

(i) Who is the internal contact point for cybersecurity incidents? How can he/she be contacted?

(ii) What are the different incident response tasks? Who is responsible for doing what?

(iii) Who is managing the incident from the business/technical side? This should be someone within the entity with decision-making authority and can follow the incident from start to finish.

(iv) Who will liaise with senior management?

(v) Who can engage the external incident response partner?

(vi) Who can file a complaint with law enforcement/inform the regulatory bodies?

(vii) Who is entitled to communicate with the press and external parties?

To adequately address a cybersecurity incident, different skills are needed to take on different responsibilities and necessary roles in an efficient incident response.

The following governance structure is vital for managing cybersecurity incidents:

ROLE	RESPONSIBILITIES
Management	► Assessing the business impact and acting upon it. ► Engaging the right resources. ► Taking decisions on how to proceed, for example: – deciding if the internet connection of a compromised system can be shut down and when is the most appropriate time – deciding when to start clean-up activities – deciding whether to file a complaint.
Communications or Public Relations Department	► Communicating appropriately to all relevant stakeholder groups. ► Answering customers, shareholders, press questions immediately.
ICT Technical Support Staff	► Analysing and managing compromised workstations and servers. ► Analysing, blocking, or restricting the data flow in and out of the network. ► Continuing IT operations, information security, and business continuity.
Cybersecurity Incident Response Manager	► Managing the cybersecurity incident from its detection until its closure.
Legal Department	► Assessing the contractual and judicial impact of an incident. ► Guaranteeing that incident response activities stay within legal, regulatory, and the organisational policy boundaries. ► Filling a complaint.

The size and nature of an organisation will determine if more roles are necessary. Smaller organisations often have the flexibility to quickly engage corporate management to manage the incident. This is not the case for larger organisations that might have to handle several incidents in a more autonomous mode, in which case corporate executives will only be engaged in incident response actions when a serious incident occurs.

Larger organisations have a more differentiated composition of an incident response team. They are ideally expected to have a crisis management team composed of corporate management representatives, in addition to the incident response team. This team might be set up to take over the responsibility for strategic and business-related decisions and communications when confronted with serious incidents. This will enable the incident response manager to focus more on the technical issues of the incident.

9.

INCIDENT REPORTING AND AWARENESS TRAINING

9.1 REPORTING CYBERSECURITY INCIDENTS

NAM-CSIRT recognises that cyber risk will continue morphing due to the evolution of cyber threats in Namibia and across the globe. A prompt and effective response to cybersecurity incidents is crucial in minimising their impact. This section outlines the procedures of reporting incidents to relevant authorities and communicating with affected clients.

The operators of CI/CII and private entities should therefore notify the Authority of any cybersecurity incident that could have a significant and adverse impact on their ability to provide adequate services to customers, their reputation, or financial condition.

a) Mandatory Reporting of High Impact Incidents

Mandatory reporting requirements vary depending on the industry in which an organisation operates and the specific regulatory obligations applicable to that sector. Notwithstanding these differences, best practice dictates that all institutions report high-impact incidents to the relevant authorities. Such reporting ensures alignment with existing internal processes and policies, while also supporting compliance with external regulatory frameworks.

b) Non-mandatory Reporting to NAM-CSIRT

It is important that all high impact incidents are reported to NAM-CSIRT. Although not all public and private sector organisations are part of its constituents, these high impact incidents should be reported for purposes of national record.

In addition, organisations should consider voluntary reporting of cybersecurity incidents to NAM-CSIRT to prevent attacks on other similar or connected computer systems, and for NAM-CSIRT to create national or sector specific awareness on the Indicators of Compromise (IOCs), possible TTPs, and guides on taking effective countermeasures. IOCs and TTPs are artefacts observed on a system or network infrastructure indicating the high likelihood of an intrusion and compromise.

Reporting to NAM-CSIRT will further assist with research and analysis of whether the incident is isolated and makes it possible to keep track of related threat trends, contributing to preventing attacks on other information infrastructure.

Cyber incidents are categorised according to the four criticality levels of the Cyber Incident Classification Matrix. Each level entails specific handling procedures. The criticality of a cyber incident is defined across four impact scenarios as the qualitative measure of its severity, as below:

IMPACT SCENARIO	LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3
PEOPLE Impact on the health and safety of citizens	Negligible impacts	Limited impacts to a single constituent	Impacts involving more than one constituent or relevant impact on a single constituent	Impacts involving more than one constituent causing tangible hazards to citizens
ECONOMY Impact involving direct economic losses	Negligible impacts	Limited impacts to a single constituent	Impacts involving more than one constituent or relevant impact on a single constituent	Relevant economic impact for the entire constituency or Namibia as a whole
OPERATIONAL Impact on the services delivered to citizens	Negligible impacts	Limited impacts to a single constituent	Impacts involving more than one constituent or relevant impact on a single constituent	Serious impacts on the entire constituency or Namibia as a whole
REPUTATIONAL Damage to the image of the constituency and/or Namibia as a whole	Negligible impacts	Limited impacts to a single constituent	Impacts involving more than one constituent or relevant impact on a single constituent	Reputational damage with national impact

9.1.1 Control: Criteria for Reporting

The extent, breadth, and complexity of contemporary threats require cooperation among operators of CI/CII and private entities to protect critical networks and information infrastructure. The Authority understands that, during an event, an operator's attention may be fully consumed with the mitigation of the cyber threat and the restoration of its services. However, operators of CI/CII and private entities are required to promptly notify the Authority of any cybersecurity incident that meets the following criteria:

(i) Potential compromise to other CI/CII or entity.

(ii) Impact on the operators of CI/CII and private entities affecting critical services.

(iii) Impact to the infrastructure, data and/or systems, including but not limited to the confidentiality, integrity, or availability of customer information.

(iv) Disruptions to business systems or operations, including but not limited to utility or data centre outages, or loss or degradation of connectivity.

(v) Operational impact to key/critical systems, infrastructure, or data.

(vi) Disaster recovery teams or plans have been activated, or a disaster declaration has been made by a third-party vendor that impacts the system of the operators of CI/CII and private entities.

(vii) Operational impact to internal users or that poses an impact to external customers or business operations.

Further information on the type of activities to be reported to the Authority is contained in Appendix 3.

9.1.2 Control: Notification of Incidents to the Authority

(i) Operators of CI/CII and private entities should inform NAM-CSIRT within five (5) hours after an incident is classified, noting that an incident should be classified within the first twenty-four (24) hours of its detection. An incident is classified as major if it satisfies the requisite criteria in 9.1.1.

(ii) Cybersecurity events that have a reasonable likelihood of materially harming any part of the normal operation(s) of operators of CI/CII and private entities should also be reported via the Cyber Incident Reporting Platform to the Authority.

(iii) Operators of CI/CII and private entities should have a focal point-of-contact for reporting cybersecurity incidents.

9.1.3 Control: Notification To and From Customers

(i) CI/CII and private entities should keep customers informed of any major incident or data breach where their data has potentially been compromised. They should also assess the effectiveness of the mode of communication, and inform the public where necessary.

(ii) CI/CII and private entities must establish clear protocols for notifying clients affected by a cybersecurity incident. This communication should be timely and transparent and include information about the steps taken to address the incident.

(iii) CI/CII and private entities must educate users on what, how, and where to report information security incidents.

(iv) CI/CII and private entities must encourage anonymous reporting to promote responsible disclosure.

9.1.4 Control: Communication Plans

Operators of CI/CII and entities must have a communication plan in place, and they must constantly update the reporting and communication plans, based on changes or past incidents.

Such plans must, at a minimum, address relevant legal and ethical considerations to ensure regulatory compliance and maintain public and stakeholder trust. Communication plans must set out clear external communication protocols that govern how the organisation engages with third parties, including affected customers, the media, law-enforcement agencies, and regulatory authorities. The plans must clearly define roles and responsibilities for incident-related communications, including spokesperson designation, escalation paths, and approval authorities. They should also establish predefined communication workflows to ensure a structured and consistent approach to incident handling, reducing ambiguity and minimising response delays. Communication plans must provide for internal notifications, stakeholder updates, and formal external reporting mechanisms to promote transparency, accountability, and consistency throughout the entire incident response life cycle.

9.2 CYBERSECURITY AWARENESS AND TRAINING

The human element plays a critical role in cybersecurity. This domain ensures that the workforce of an entity (including contractors and part time employees) is provided with the awareness, knowledge, and skills to carry out their organisational responsibilities safely and utilise organisational systems and infrastructure in compliance with the entity's cybersecurity policies. Moreover, through awareness campaigns highlighting the dangers of cyberattacks, consumers should be made aware of what they should and should not do in relation to submitting personal information online. This section stresses the need for continuous awareness and engagement to foster a culture of cybersecurity awareness.

9.2.1 Control: Training of Staff, Training Focus Areas, and Learning Approaches

Operators of CI/CII and entities are encouraged to ensure the following controls:

(i) Conduct regular appropriate cybersecurity training and awareness programmes for all staff members (permanent employees, temporary, or contractors).

(ii) Conduct a skills-gap analysis before training is undertaken to identify skills which are lacking and fortify skills already existing within their teams. Once the skills-gap analysis is concluded, an entity is to identify and provide training offered by accredited and specialised cybersecurity experts with practical knowledge in the field.

(iii) Training should be followed up with quarterly reviews to test staff knowledge and ensure they are kept abreast with current cyber trends. Practical ways to test knowledge is by conducting cyber drill exercises. Cyber drills offer hands-on experience as they simulate cyberattacks and are effective to assess an organisation's preparedness, capabilities, and defences in responding to incidents. An entity should expose staff to international programmes which may be available to organisations in the cyber sector.

(iv) Enter Memorandums of Understanding with training institutions and academia to periodically send staff for skills upgrades. This is necessitated as technological programmes are ever changing and hackers have become more sophisticated in their attacks on organisations' security networks.

(v) Conduct pre- and post-training assessments at the beginning and end of the training programmes. Internal surveys may be conducted to assess the effectiveness of the training programmes on staff productivity and acquired knowledge.

(vi) Cybersecurity training programmes should be routinely evaluated to ensure they are kept up to date and effective and to meet the demands of the dynamic cyberspace, which is ever evolving.

(vii) CI/CII and private entities are encouraged to:

  (a) Invest in Research and Development (R&D) departments with units specifically focused on cybersecurity. This will ensure that training programmes are evaluated and kept up to date with current trends and information on cyberspace.
  (b) Incorporate R&D within their institution's cybersecurity strategies and annual budgets for programme continuity. This indicates the operators of CI/CII and private entities commitment to ensuring a safe cyberspace both for its staff and customers.

9.2.2 Control: Consumer Cybersecurity Awareness

Operators of CI/CII and private entities, in collaboration with the Authority, will ensure the following controls:

(i) Create cybersecurity awareness campaigns with its customers through various platforms such as observing a cybersecurity awareness month. The primary purpose would be to sensitise customers on cyber safety and preventative measures.

(ii) Conduct regular awareness workshops with the Authority and external customers, which may be conducted physically or online. The workshops should be tailored to assist customers in identifying methods used in cyberattacks.

(iii) Develop material or videos on their websites or social media platforms to enable customers to refer to educational material when necessary.

(iv) Educate their customers by developing campaign material in local languages which can easily be understood by the communities that utilise their services. This information can be disseminated via radio as it is widely used communication medium in Namibia.

(v) Conduct customer location and journey mapping which would provide a holistic database of their customers' locations, experience, and service reach.

(vi) Issue regular newsletters, in collaboration with the Authority, providing cyber tips and best practices to their customers.

9.3 RELATIONSHIP BUILDING

Cybersecurity is not solely about technical controls; it is fundamentally about trust and collaboration. A strong relationship between the Authority and operators of CI/CII and private entities is essential to foster a secure and resilient cyber environment. This pillar emphasises building a trust-based relationship that encourages voluntary, timely, and transparent reporting of cybersecurity incidents without fear of punitive action. Such openness cultivates a sense of ownership among operators of CI/CII and private entities, strengthens accountability, and ensures the confidentiality of sensitive information shared with the Authority.

To institutionalise this collaboration, various cybersecurity working groups will be established depending on the domain of the operators of CI/CII and private entities known as Constituencies. These Constituencies will facilitate continuous information exchange, support the NAM-CSIRT framework, and serve as a platform for joint initiatives and best practice sharing.

To further incentivise active engagement, the Authority may introduce recognition mechanisms for operators of CI/CII and private entities demonstrating strong cybersecurity practices. Potential incentives include reduced regulatory scrutiny, access to specialised cybersecurity resources, and participation in government-led programmes. Recognising cybersecurity as a strategic advantage rather than a compliance burden motivates industry-wide adoption of robust security standards. Moreover, aligning with international best practices and leveraging global partnerships will provide valuable insights to strengthen Namibia's cybersecurity posture. Benchmarking against established frameworks ensures the sector remains adaptive and resilient against emerging threats.

Technology will play a key role in reinforcing this relationship. A centralised, secure platform for real-time incident reporting, threat intelligence sharing, and regulatory updates will enhance transparency and improve communication efficiency. Such a platform can include automated alerts, compliance monitoring, and training resources to support the readiness of operators of CI/CII and private entities.

Finally, sustaining this relationship requires continuous engagement through industry roundtables, cybersecurity summits, and capacity-building workshops. These forums will encourage open dialogue, collective problem-solving, and innovation, ensuring that cybersecurity efforts evolve alongside technological and threat landscapes.

Through proactive relationship building, the Authority and industry can jointly create a cybersecurity culture rooted in trust, cooperation, and shared responsibility.

Key Elements of Relationship Building in Cybersecurity

KEY ELEMENT	DESCRIPTION	IMPACT ON CI/CII AND PRIVATE ENTITIES
Trust and Transparency	Open communication and clear expectations to encourage cooperation.	Encourages voluntary compliance and proactive security measures.
Confidential Information Handling	Ensuring that sensitive data shared by CI/CII and private entities is protected and used constructively.	Reduces fear of reputational damage or regulatory penalties.
Non-Punitive Incident Reporting	Creating a safe space for CI/CII and entities to disclose security incidents without automatic penalties.	Encourages honest reporting and faster response to threats.
Collaborative Cybersecurity Working Group	Establishing a platform for ongoing engagement between CRAN and industry stakeholders.	Provides an opportunity to shape cybersecurity policies and influence best practices.
Technology and Digital Platforms	Developing secure portals for real-time incident reporting and information exchange.	Simplifies compliance processes and access to regulatory support.
International Benchmarking and Best Practices	Learning from global cybersecurity frameworks to refine national strategies.	Aligns CI/CII and entities with international cybersecurity standards and practices.
Continuous Engagement and Training	Organising roundtables, workshops, and cybersecurity awareness programmes.	Helps CI/CII and entities build internal cybersecurity capabilities and resilience.

10.

MONITORING, REVIEW OF THE GUIDELINES, AND CONFIDENTIALITY CLAUSE

Effective implementation of these Guidelines depends on systematic monitoring and evaluation to measure progress, identify gaps, and ensure continuous improvement. Monitoring enables CRAN and NAM-CSIRT to assess the extent of compliance by operators of CI/CII, government OMAs, and private entities, while evaluation ensures that interventions remain relevant, efficient, and aligned with emerging cyber risks.

10.1 MONITORING MECHANISM

The Authority, through NAM-CSIRT, shall develop and maintain a monitoring framework to assess implementation across all stakeholder categories. This will include:

(i) Annual compliance self-assessments by CI/CII using standard reporting templates issued by the Authority.

(ii) Periodic reviews of incident reports, sectoral exercises, and response capabilities.

(iii) Tracking of key performance indicators related to incident response times, reporting compliance, training frequency, and awareness reach.

(iv) Documentation of lessons learned and dissemination of good practices across sectors.

10.2 REVIEW OF THE GUIDELINES

The Guidelines shall be formally reviewed every three (3) years, or earlier if deemed necessary by the Authority due to significant changes in the cybersecurity landscape, technology, or legislation.

10.3 CONFIDENTIALITY CLAUSE

To promote responsible information handling and safeguard sensitive cybersecurity data, all parties engaged in information exchange under this guideline must adhere to the Traffic Light Protocol (TLP). The TLP was developed to enhance the sharing of sensitive information and foster effective collaboration among trusted entities by providing a structured method for classifying and communicating how widely information may be disseminated. It uses four color-coded labels that define the sharing boundaries recipients must respect.

(a) **TLP: RED** – This level is strictly confidential and intended only for the individual recipients. It must not be shared beyond the people directly receiving it. TLP: RED is used when further dissemination would create serious risks to privacy, reputation, or operations. In a meeting context, this classification applies only to those physically present.

(b) **TLP: AMBER** – Allows limited sharing within an organisation and, where necessary, with its clients on a need-to-know basis. The TLP: AMBER+STRICT variant confines sharing strictly to the organisation. This classification is appropriate when controlled dissemination is required to act effectively but could still pose risks if shared too widely.

(c) **TLP: GREEN** – Information marked TLP: GREEN can be shared more broadly, but only within a defined community, such as the national or sectoral cybersecurity community. It aims to raise awareness among trusted peers but may not be released to the public or shared through open channels.

(f) **TLP: CLEAR** – This classification allows unrestricted public disclosure. TLP: CLEAR is used when information poses minimal or no foreseeable risk if shared openly, provided that applicable copyright and publication rules are observed.

10.4 ENTRY INTO FORCE

These guidelines will come into effect on the date of publication.

11.

APPENDICES

APPENDIX 1: KNOW YOUR ENVIRONMENT

11.1 KNOW YOUR IT ASSETS

(i) Maintain an up-to-date inventory of all authorised IT assets on-premises and in third-party cloud infrastructure used to process, store or transmit data/information such as workstations, laptops, ATMs, POS, network switches, routers, firewall, printers, scanners, photocopiers, IP Phones, mobile devices, surveillance cameras, applications, databases, services, protocols, etc.

(ii) Establish asset ownership and assign responsibility for managing each asset to a specific individual or team.

(iii) Ensure that all identified devices are categorised by the criticality and sensitivity of the data/information they store, process, or transmit.

(iv) Identify and document account profiles (systems administrators and privileged users), third-party vendors accounts, etc.

(v) Regularly review the account profile of staff (systems administrators and privileged users) and third parties who have access to devices identified.

(vi) Maintain an inventory of all data assets, including locations, owners, and access controls.

(vii) Implement a data classification framework that categorises data based on its sensitivity and criticality.

(viii) Document data handling procedures, retention policies, and secure data disposal processes.

(ix) Maintain an approved up-to-date network topology diagram of wired and wireless networks irrespective of location.

11.2 KNOW YOUR VULNERABILITIES

Operators of CI/CII and private entities shall:

(i) Implement a vulnerability management policy approved by their Board.

(ii) Conduct a vulnerability assessment of all IT assets and present the report of the assessment to the Information Security Steering Committee (ISSC) and senior management at least once every quarter.

(iii) Conduct vulnerability assessment when there is a notable change to the institution's information processing infrastructure (such as installation of new systems, devices, applications, etc.) or when there is knowledge of new vulnerabilities.

(iv) Where possible, implement automated vulnerability scanning tools for continuous identification of vulnerabilities.

(v) Conduct external Penetration Test (PT) on IT Assets at least annually. PTs may be conducted more-frequently on internet-facing financial systems/applications.

(vi) Conduct regular audits of IT assets and associated services, on premises and in cloud infrastructure to identify any potential weaknesses. This may include third-party audits, security reviews, or compliance assessments.

(vii) Continually identify inherent risks and vulnerabilities associated with IT platform/protocols used for business services (e.g., USSD, Mobile Banking).

(viii) Establish efficient mechanisms and processes to identify patch compliance status of IT assets.

11.3 KNOW YOUR THREATS

Operators of CI/CII and private entities must:

(i) Establish a Cyber Threat Intelligence (CTI) programme approved by their Board which should include policies to aid proactive identification of emerging cyber threats, trends, patterns, risks, and possible impacts.

(ii) Identify and document various internal and external CTI Sources. Internal sources are the IT infrastructures that generate logs. External sources are reputable commercial threat intelligence sources. These feeds should be integrated with security controls to enhance threat detection and response capabilities.

(iii) Leverage "Open-Source Intelligence" (OSINT) by monitoring publicly available sources, such as search engines, online forums, social media platforms, and security blogs.

(iv) Where possible, monitor the dark web for mentions of the institution, critical assets, or sensitive information such as customers' data or staff's access credentials.

(v) Make informed decisions based on the CTI programme as it provides valuable information on areas susceptible to cyberattacks, latest threats, attack vectors, etc. Decisions may include reviewing the Bring-Your-Own Device (BYOD) policy, conducting emergency staff or customers awareness/training, vulnerability assessment, penetration testing, review of vendor source codes, cyber incident response plan, business continuity/disaster recovery plans, vendor service level agreements, among others.

(vi) Engage in information sharing and collaboration with trusted industry peers, sector-specific information sharing establishments.

(vii) Promptly report all cyber threats to their information assets to the Authority.

11.4 KNOW YOUR THIRD-PARTY SERVICE PROVIDERS AND CONNECTIONS

Operators of CI/CII and private entities shall:

(i) Maintain a record of all third-party service providers, including Cloud Service Providers (CSP).

(ii) Periodically review their records to ensure discontinued third parties' access credentials have been revoked and network connections terminated.

(iii) Identify and document all connections to third parties (e.g., wholesale customers, vendors, and switches that provide Value-Added-Service). The objective of each connection shall be documented and reviewed regularly.

(iv) Evaluate the security controls and processes of the CSP before adopting a cloud service. Where applicable the data centre and network infrastructure facilities of third parties should be visited and their cybersecurity policies reviewed to ensure all cybersecurity concerns are addressed.

11.5 KNOW YOUR PRIVILEGED USERS:

Operators of CI/CII and private entities shall:

(i) Identify and document all employees and system/service accounts with privileged access on systems, applications, and databases in an Access Control Matrix (ACM).

(ii) Regularly review the ACM to ensure privileges are withdrawn once staff role changes.

(iii) Ensure that risks associated with this category of persons are regularly assessed as part of the enterprise risk assessment framework.

APPENDIX 2: INCIDENT MANAGEMENT LIFE CYCLE PHASES

Phase	DESCRIPTION	IMPACT ON CI/CII AND PRIVATE ENTITIES
1. Preparation	► Maintain policies, playbooks ► Conduct awareness training	CSIRT team, IT administrators
2. Identification	► Detect, collect, and validate alerts ► Classify and prioritise incident accordingly to severity and impact	CSIRT team, Security Operations Centre (SOC) team, IT administrators
3. Containment	► Isolate affected systems, block IPs, and disable accounts ► Implement segmentation	CSIRT team, IT/Network administrator, SOC team
4. Remediation	► Remove malware, exploits ► Patch vulnerabilities ► Harden affected systems	CSIRT team, IT/Network administrator, SOC team
5. Recovery	► Validate that systems are clean and stable ► Restore system to production ► Monitor for recurrence	CSIRT team, IT/Network administrator, SOC team and business owner

APPENDIX 2: INCIDENT MANAGEMENT LIFE CYCLE PHASES (CONTINUED)

Phase	DESCRIPTION	IMPACT ON CI/CII AND PRIVATE ENTITIES
6. Lessons Learned	► Conduct post-incident reviews ► Document root cause and response effectiveness ► Update playbooks, control, and training	CSIRT team, IT/Network administrator, SOC team and management

APPENDIX 3: TYPES OF CYBERSECURITY INCIDENTS

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Abusive Content	Spam	Aka "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content.
	Harmful Speech	Discreditation or discrimination of somebody (e.g., cyber stalking, racism and threats against one or more individuals).
	Child/Sexual/Violence	Child pornography, glorification of violence.
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
	Ransomware	A type of malicious software from crypto virology that blocks access to the victim's data or threatens to publish it until a ransom is paid.
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services, and accounts. Examples: fingerd, Domain Name System (DNS) querying, Internet Control Message Protocol (ICMP), Simple Mail Transfer Protocol (SMTP) (EXPN, RCPT), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g., lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as Common Vulnerabilities and Exposures (CVE) name (e.g., buffer overflow, backdoor, cross site scripting, etc.).

APPENDIX 3: TYPES OF CYBERSECURITY INCIDENTS (CONTINUED)

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Intrusion Attempts	Login attempts	Multiple login attempts (Guessing/cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can be caused remotely by a known or new vulnerability, but also by an unauthorised local access. Also includes being part of a botnet.
	Unprivileged account compromise	
	Application compromise	
	Bot	
Availability	DoS	The incident involving a temporary disruption of a computer-based element or network service.
	DDoS	
	Sabotage Outage (no malice)	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks, and mailbombing. Distributed Denial of Service (DDoS) often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (e.g., destruction, disruption of power supply) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
Information Content Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/ software error can also be the cause.
	Unauthorised modification of information	
Fraud	Unauthorised use of resources	Using resources for unauthorised purposes including profit-making ventures (e.g., the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another to benefit from it.
	Phishing	Masquerading as another entity to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open resolvers, world readable printers, vulnerability apparent from Nessus scans, virus signatures not up to date, etc.

APPENDIX 3: TYPES OF CYBERSECURITY INCIDENTS (CONTINUED)

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

Source: CIRCL Taxonomy – Schemes of Classification in Incident Response and Detection (ecsirt.net).

APPENDIX 4: CHANGE LOG TABLE

Version	Date	Description of Change	Section/Annex amended	Approved by
1.0	April 2026	Initial release of the National Cybersecurity Incident Handling & Management Guidelines	Full Document	CRAN Executive Management

12.

REFERENCES

REFERENCES

ACSA, 2024. *Guidelines for Cyber Security Incidents-Australian Signals Directorate*, Information Security Manual. Available at cyber.gov.au.

ENISA, 2018. *Incident Classification Taxonomy*. Technical Guidance, Europe: ENISA. Available at: ecsirt.net.

ENISA, 2021. *Guidelines on Security Measures under the EECC*. Technical Guidance, Europe: ENISA.

ISO/IEC. 2022. *ISO/IEC 27001 - Information Security, Cybersecurity and privacy protection Requirements.* Standard, Geneva, Switzerland: ISO/IEC.

ITU, 2009. *Cybersecurity: The Role and Responsibilities of an Effective Regulator*. Switzerland: International Telecommunication Union.

IT, 2015. *Security in Telecommunications and Information Technology*. Report, Switzerland: International Telecommunication Union.

ITU, 2023. *ITU-T Recommendation X.1051 - Information Security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organisations.* Recommendation, Geneva: International Telecommunication Union.

NIST, 2024. *The NIST Cybersecurity Framework (CSF) 2.0.* Gaithersburg: National Institute of Standards and Technology.

TATT, 2024. *Consultative Document on the Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities* (October 2024). Barataria, Trinidad and Tobago.

NOTES

NOTES

NAM-CSIRT

NAMIBIA CYBER SECURITY INCIDENT RESPONSE TEAM

Powered by

CRAN

Communications Regulatory Authority of Namibia

www.nam-csirt.na +264 61 222 666 info@nam-csirt.na