GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$8.00 WINDHOEK - 3 July 2026 No. 8968

CONTENTS

Page

General Notice

BANK OF NAMIBIA

No. 501 2026

DETERMINATION UNDER PAYMENT SYSTEM MANAGEMENT ACT, 2023: OPERATIONAL AND CYBERSECURITY STANDARDS WITHIN NATIONAL PAYMENT SYSTEM (PSD-12)

In my capacity as Governor of the Bank of Namibia (the Bank), and under the powers vested in the Bank by virtue of section 45 of the Payment System Management Act, 2023 (Act No. 14 of 2023), I hereby issue the Determination on the Operational and Cybersecurity Standards within the National Payment System (PSD-12), which Determination shall become effective on the date of publication in the *Gazette*.

EBSON UANGUTA
GOVERNOR
BANK OF NAMIBIA Windhoek, 9 June 2026

Payments System Determination (PSD-12)

DETERMINATION ON THE OPERATIONAL AND CYBERSECURITY STANDARDS WITHIN THE NATIONAL PAYMENT SYSTEM

Arrangement of Paragraphs

PART I
PRELIMINARY

1. **Short Title** – Determination on the Operational and Cybersecurity Standards within the National Payment System (PSD-12).

2. **Application** – This Determination applies to all payment service providers and payment system operators within the National Payment System.

3. **Definitions** – In this Determination, unless the context otherwise indicates, the words and expressions used herein have the same meaning assigned in the Payment System Management Act, 2023 (Act No. 14 of 2023), and cognate expressions have corresponding meanings:

"Act" means the Payment System Management Act, 2023 (Act No. 14 of 2023).

"Availability" means the status of being accessible and usable as expected upon demand.

"Availability loss" means the cumulative duration, expressed in minutes, of any unscheduled interruption to planned production processes. An interruption begins at the moment a planned production activity is halted and ends when affected production is restored.

"Banking institution" means a banking institution as defined in section 1 of the Banking Institutions Act, 2023 (Act No. 13 of 2023).

"Critical operations" means activity, function, process, or service, the loss of which, would affect the continued operation of the National Payment System, its users and/or the broader financial system.

"Critical systems" means all systems required for the efficient and effective operation of the National Payment System in terms of the following:

(a) Systems used for the provision of payment services as specified under the Schedule of the Act;
(b) Payment-related modules of core banking systems that are essential for initiating, processing, or settling payment transactions;
(c) Financial Market Infrastructures (FMIs); or
(d) Interoperable Retail Payment Systems such as Payment Card, Electronic Fund Transfers (EFT), Electronic-Money (E-money), Instant Payment System, and any payment activity as may be authorised or designated by the Bank.

"Cyber" means the interconnected information infrastructure of interactions among persons, processes, data, and information and communication technologies, along with the environment and conditions that influence those interactions.

"Cyberattack" means the use of an exploit by an adversary to take advantage of weakness(es) with the intent of achieving an adverse effect on an information communication technology environment, which results in harmful consequences including operational, reputational, financial, security or data loss.

"Cybersecurity" means the preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

"Cyber event" means an observable occurrence in an information system that may indicate a security incident is occurring.

"Cyber incident" means any event that jeopardises the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

"Cyber resilience" means the ability to safeguard the security of systems, prevent, anticipate, withstand, and rapidly recover from a cyber incident, so as to uphold its confidentiality, integrity, and availability.

"Cyber risk" means the combination of the probability of an event occurring within the realm of an applicable entity's information assets, computer and communication resources and the consequences of that event for the entity.

"Cyber threat" means a circumstance or event with the potential to exploit one or more vulnerabilities in the entity's systems, resulting in a loss of security, confidentiality, integrity or availability.

"Data at rest" means data that has reached a destination, being stored and is not being accessed or used.

"Data in motion" means data that is actively moving across devices and networks.

"Data in use" means data actively being used across the network or temporarily residing in memory, or any data not "inactive".

"Encryption" means the process of converting information or data into a code which is only accessible with a defined digital key, to prevent unauthorised access.

"Entity" means a payment service provider or payment system operator or both.

"Framework" means the policies, procedures and controls established to identify, protect, detect, respond to and recover from the plausible sources of cyber, fraud and operational risks in terms of this Determination.

"Fraud" means any act intended to unlawfully gain a benefit or cause financial loss to another party. This may result from exploiting technical flaws, manipulating documents, misusing relationships, authority, or intentionally taking advantage of weaknesses in systems or standards performed either directly or indirectly.

"Information asset" means any piece of data, device or other components of the environment that supports information-related activities.

"Information security" means the practice of protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to ensure the security, confidentiality, integrity, and availability of data.

"Information Technology (IT) system" means all hardware, software, networks, and related infrastructure used for processing, storing, or transmitting electronic information and its integration within the IT environment.

"Integrity" means the completeness, accuracy, and freedom from unauthorised modification, destruction, or use of data, information systems, or its components, ensuring that it remain reliable and unaltered.

"Masking" means the obfuscation or hiding of information and data using modified content like characters or numbers, with the objective of creating an alternate version of information or data that cannot be easily identifiable or reverse-engineered, protecting data classified as sensitive.

"**Multi-factor Authentication (MFA)**" means the use of a minimum of two authentication factors to verify the identity of a user.

"National Payment System" means the entire national payments ecosystem and includes all the payment systems, clearing systems, settlement systems and the rules, standards, arrangements, procedures, laws, agreements, technologies, payment instruments and institutions that are used in the processing and transferring of funds and securities.

"Non-bank financial institutions" means institutions, other than banking institutions authorised to conduct banking business, that offer payment services.

"Operational resilience" means the ability to maintain essential operational capabilities under adverse conditions or stress, even if in a degraded or debilitated state; and recover to effective operational capability in a time frame and state consistent with this Determination.

"Payment Service Provider" means a person, including a banking institution, licensed under the Act to provide payment services as specified under the Schedule of the Act.

"Payment System Operator" means a person authorised under the Act to operate a payment system.

"Penetration testing" means a test methodology in which assessors typically working under specific constraints, ethically attempt to circumvent or defeat the security features of an information system.

"Recovery Point Objective" means the amount of time between a disaster occurring and an institution's most recent backup or the maximum acceptable amount of data loss after an unplanned data loss incident, expressed as an amount of time.

"Recovery Time Objective" means the longest acceptable length of time that a computer, system, network, or application can be down after a disaster happens.

"Recurring payments" means pre-authorised transactions in which a user, pursuant to an agreed mandate or contractual arrangement, provides consent for a merchant or service provider to automatically deduct funds from the user's payment instrument at specified intervals and for the duration stipulated in such mandate or arrangement. These payments may include subscription fees, instalment payments, or other scheduled charges, and are executed without requiring the user to authenticate each transaction after the initial verification and authorisation.

"Respond" means to implement appropriate activities and measures to take action regarding a detected or suspected incident.

"Risk Indicator" means an occurrence or sign that reveals that an incident or something may have occurred or is in progress. For example, system uptime or availability is a risk indicator.

"Sensitive information" means information or data where loss, misuse, unlawful disclosure or unauthorised access to, or modification of, could adversely affect the public interest or an entity or the privacy to which users are entitled.

"Successful cyberattack" means a cyber incident that compromises the security, confidentiality, integrity, or availability of systems or data beyond preventive controls, or materially degrades a critical service.

"Threat intelligence" means threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes.

"Tokenisation" means a process by which sensitive information and data elements are replaced by dynamic tokens of no intrinsic value, to prevent unauthorised access.

"Tolerance level" means the specified level of risk to be tolerated by a Board and / or Senior Management or the Bank of Namibia of which the level is expressed in either quantitative or qualitative terms.

"User" means any person that uses a payment service in their capacity as a payer or a payee or both.

"Vulnerability" means a weakness, flaw, or susceptibility in a system, process, or design that may be exploited by an attacker or lead to failure, degradation, or compromise of security, resilience, availability, or data integrity due to internal faults, misconfigurations, or unforeseen conditions.

"Vulnerability assessment" means a systematic examination of an IT system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

"Zero trust" means a security model that assumes no user, device, or system is inherently trustworthy. Access to resources is strictly limited and continuously verified based on identity, context, and risk level, regardless of where the request originates.

PART II
STATEMENT OF POLICY

4. **Authorisation** – Authority for the Bank to issue this Determination is provided for under section 45 of the Act.

5. **Purpose –** This Determination provides the principles and key risk indicators for the risk management of cyber security and operational resilience in the National Payment System.

6. **Scope** – This Determination applies to all FMIs, Non-Bank Financial Institutions (NBFIs), participants of FMIs, Retail Payment Systems (such as EFTs, payment card, E-money, etc.), Payment Service Providers, Payment System Operators and any other entities licensed or authorised within the National Payment System.

7. **Position of the Bank** – The payment landscape has evolved significantly with the rise of digitisation, Instant Payment Systems, financial technology (fintech), automation and artificial intelligence (AI), all of which have transformed the way payments are executed. These advancements have introduced alternative payment solutions that are faster, more cost-effective, and more efficient. The increasing interdependencies and demand for interoperability among payment service providers, financial institutions, and third-party platforms have created a more interconnected ecosystem, requiring coordinated resilience and security measures. However, it also increased cyber and operational risks within the National Payment System, as payment service providers and payment system operators have become more reliant on digital networks and third-party IT service providers. This growing dependency requires a higher level of resilience against cyber incidents.

Cyberattacks target critical IT infrastructure through multiple entry points, such as FMI, participant banks, linked FMIs, service providers, vendors, and vendor products. This could cause significant disruptions, which may escalate into systemic events within the National Payment System. Such events can undermine the integrity, safety, and efficiency of the National Payment System and, in turn, pose a significant threat to financial stability.

The Bank is cognisant of continuous and emerging cyber risks and threats. Therefore, it is imperative for payment services providers and payment system operators to proactively implement and manage controls for enhanced cybersecurity and a planned response.

Cyberattacks threaten financial stability by disrupting the interconnected operational networks and critical infrastructure of the National Payment System. Inadequate management of operational resilience may cause FMIs and other key National Payment System stakeholders to become sources of financial shocks and channels for its transmission across domestic and international financial markets.

Furthermore, these vulnerabilities can lead to data breaches and the fraudulent loss of funds, ultimately posing a systemic risk to the stability of the financial system. Accordingly, the regulation of cybersecurity and operational resilience is essential to fulfilling one of the Bank's mandates as set out in section 3(1) of the Act, which is to ensure the safe, secure, efficient, and effective operation of the National Payment System. This Determination supports the referred to mandate by establishing minimum requirements and principles for cyber risk governance, monitoring, detection, incident response, and recovery. It also promotes a proactive, risk-based, and adaptive approach to cyber risk management that accounts for emerging and evolving threats. Moreover, it reinforces public confidence in the

National Payment System through the implementation of appropriate safeguards, business continuity plans, and information-sharing mechanisms.

8. **Application of the Act** – Unless expressly stated otherwise, the provisions of the Act, as well as the related Determinations, Guidelines, Circulars, Notices, Directives and any other relevant laws, apply to all payment service providers and payment system operators within the National Payment System.

The principles set out in this Determination, must be implemented in a manner that reflects the nature, size, complexity, and risk profile of the entity. Where terms such as appropriate, adequate, effective, timely, regular, or periodic are used, implementation must be assessed in the same context.

PART III
OPERATIONAL AND CYBERSECURITY STANDARDS

9. **Governance - Role of the Board and Senior Management**

9.1 The Board of the payment service provider and payment system operator (hereinafter referred to as the Board) are responsible for information security, cybersecurity and operational resilience and must establish and approve a Framework in respect thereof.

9.2 The Framework must be defined and continuously adapted to the entity's strategic objectives and risk profile.

9.3 The Board must:

9.3.1 ensure that resources and oversight are proportionate to the nature, scale, and complexity of the entity's risk;

9.3.2 set and approve risk tolerances which are aligned with the key risk indicators contemplated in section 13 of this Determination;

9.3.3 be apprised periodically, at least four (4) times in a year, of the risk profile in terms of this Determination to ensure that it remains consistent with the risk tolerances as contemplated in section 9.3.2 of this Determination;

9.3.4 ensure that the entity participates in industry-wide collaborative efforts to effectively respond to and recover from fraud and cyberattacks within the financial system;

9.3.5 ensure that cybersecurity, operational, and fraud risks are appropriately incorporated into the entity's audit plan to provide adequate assurance on the effectiveness of controls; and

9.3.6 ensure the establishment and maintenance of an effective compliance management program that ensures adherence to all applicable regulatory requirements, internal policies, and industry standards relating to cybersecurity and operational resilience.

9.4 Further to section 9.3.6 of this Determination, the Board must oversee the adequacy of the compliance function to provide assurance of ongoing regulatory conformity.

9.5 The Board may delegate the implementation of this Determination to Senior Management.

9.6 The Board must ensure segregation of duties between itself, as the body responsible for the governance of information security, cybersecurity and operational resilience and the person(s) i.e., security officer(s), within the entity responsible for the implementation of information security, cybersecurity and operational resilience.

9.7 The security officer(s), i.e., Chief Information Security Officer (CISO) or equivalent role, contemplated in section 9.6 of this Determination must have sufficient independence to perform security oversight effectively. This independence is achieved by ensuring the security officer(s) has reporting access to the Board or a designated sub-committee of the Board on all security-related matters.

10. Framework

10.1 The Framework must:

10.1.1 clearly determine information security, cybersecurity, fraud and operational resilience objectives, and tolerances;

10.1.2 at a minimum, include measures of identification, protection, detection, response and recovery as contemplated in section 11 of this Determination. Testing, situational awareness and learning and evolving must be continuously adopted across each measure;

10.1.3 clearly define the roles and responsibilities for managing information security, cybersecurity, fraud and operational resilience, including in cases of emergencies and/or in crisis; and

10.1.4 be reviewed and updated at least once every three years, or after a significant change, to ensure that it remains relevant.

10.2 The strategies and measures in the Framework must cover people, processes, data and technology as well as measures for information security as it relates to data in use, data at rest and data in motion.

10.3 The adequacy of and adherence to the Framework must be internally assessed and measured periodically through independent compliance programmes and audits.

11. Vulnerability Management – Identification, Protection, Detection, Response and Recovery

Identification

11.1 The entity must identify its business functions and supporting processes, including those managed by third-party service providers.

11.2 Further to section 11.1 of this Determination, the identified business functions and supporting processes must be classified in terms of criticality. This classification must guide the prioritisation of protective, detective, response, and recovery efforts.

11.3 A risk assessment must be performed at least once (1) every year, or when there is a significant change that affects the business functions or processes, to ensure that there is an understanding of the importance of each business function and supporting processes, and its interdependence within the National Payment System.

11.4 The entity must periodically conduct fraud risk assessments to identify potential fraud vectors within its environment, including risks to which it or its users may be exposed, and to evaluate the effectiveness of existing controls in mitigating those risks.

11.5 The entity must conduct Vulnerability Assessments and Penetration Tests as follows:

11.5.1 vulnerability assessments must be performed regularly, or whenever the environment undergoes significant changes or updates; and

11.5.2 penetration tests must be conducted at least annually, or whenever critical systems or the environment undergo significant changes or updates.

11.6 The entity must maintain an inventory of all its information assets, including but not limited to location, ownership, and roles and responsibilities for managing the IT assets. The entity must maintain accurate and up-to-date network diagrams to ensure all connections and devices are identified and secured, and data-flow diagrams to demonstrate how data moves across networks and between systems. These records must be reviewed at least once (1) every year and updated whenever significant changes occur.

Protection

11.7 Appropriate protective controls must be implemented in line with best practice standards to minimise the likelihood and impact of a successful cyberattack on identified critical business functions, information assets and data. At a minimum, the following controls must be implemented:

11.7.1 Access to IT systems and information assets must be limited to authorised users, processes, devices, and managed commensurate with assessed risk. Access rights must follow the principle of least privilege and be governed by Zero Trust principles, including, but not limited to, strong, consistent authentication controls and secured remote access protocols. The adoption of these principles must be proportionate to the entity's size, complexity, and risk profile and must be reviewed quarterly to ensure ongoing effectiveness.

11.7.2 Development of comprehensive data loss prevention policies for sensitive information across all states and implement measures of such sensitive information, to prevent unauthorised data access, modification, or theft. Sensitive information must be encrypted or protected by strong access controls and permanently deleted upon disposal or contract termination.

11.7.3 Adoption of security-by-design in software development to minimise vulnerabilities and reduce the attack surface. Security requirements for system access, authentication, data integrity, and logging must be incorporated from the outset of the system development lifecycle, and changes to business-critical applications must be reviewed and tested.

11.7.4 Pursuant to 11.7.3 of this Determination, this must include the application of secure system engineering principles, coding standards, and programming techniques throughout the system development lifecycle, which covers both internally developed applications and externally sourced solutions.

11.7.5 Adequate network security measures must be implemented to secure connections between the entity, the internet, and third parties.

11.8 Agreements with third parties for relevant outsourcing arrangements and critical IT service providers must include a provision for safeguarding the entity's information, data and operational resilience objectives. The entity must:

11.8.1 Require the third-party service provider to implement security policies, procedures, and controls that are at least as robust as they would expect for their own operations, taking into account relevant best practices and standards where applicable. This includes:

a) the effectiveness of the risk-mitigating measures as defined by the service provider's risk management framework;

b) the continuity of technology services and information systems; and

c) that contracts and service level agreements (both for normal circumstances as well as in the event of service disruption), include cyber resilience requirements as well as security incident handling procedures for escalation and reporting.

11.8.2 The use of cloud computing service (s) by the entity must be as follows:

11.8.2.1 A banking institution must use cloud computing services as provided in the Determination on Cloud Computing (BID-19) issued in terms of the Banking Institutions Act, 2023 (Act No. 13 of 2023), or any subsequent amendment thereto.

11.8.2.2 A non-bank financial institution must ensure that cloud computing services are subject to the same risk management, governance, and oversight expectations applicable to all outsourcing arrangements:

a) The entity must conduct thorough due diligence prior to engaging any cloud service provider, assessing legal, sovereignty, technical, operational, and jurisdictional risks, including multi-tenancy, data commingling, cross-border processing, and the security posture of the provider.

b) Cloud-based services must be approved by the entity's board and subject to a clearly defined exit and transition strategy to ensure continuity of critical business functions in the event of service disruption or contract termination.

c) The entity must ensure that the cloud service provider(s) implement adequate safeguards for data confidentiality, integrity, recoverability, and access control. Data stored or processed in cloud environments must be encrypted.

d) The entity must maintain oversight of all cloud services, ensuring that service agreements permit regulatory supervision and internal control.

e) Where sensitive data or critical systems are involved, the entity must use private or hybrid cloud models. Public cloud usage may be permitted where adequate safeguards are demonstrated and approved at the board level.

f) Section 11.8.2.2 of this Determination is not exhaustive and may be supplemented as determined by the Bank.

11.8.3 Third parties must provide assurance of the level of compliance with the cyber resilience objectives, measures and performance targets as defined by the entity and it must be regularly reviewed. Where direct audit assurance is not feasible, the entity may:

a) assess alternative assurance mechanisms, including but not limited to independent third-party certifications;

b) evaluate summaries of audit findings, compliance attestations, or redacted reports as part of ongoing vendor monitoring; or

c) understand the limitations of assurance provided by the third-party service provider and ensure these risks are accounted for in the entity's third-party risk assessment.

11.9 The entity must establish and oversee policies governing the ethical use and protection of user data. These must at a minimum ensure:

11.9.1 user data is used only in ways that are fair, transparent, lawful, and consistent with ways that users would reasonably expect as per the given user consent.

11.9.2 the entity must not disclose or process user data beyond what is permitted by law; and

11.9.3 the entity must extend equivalent data protection and compliance obligations to all, but not limited to, outsourced service providers, providers of emerging technologies, including cloud computing, and parties involved in open banking or Application Programming Interface (API)-based integrations.

11.10 The entity must develop, implement and maintain policies and procedures to ensure the effective, secure, and ethical adoption, development, and use of emerging technologies, including but not limited to AI and Machine Learning (ML), within its processes.

11.11 The entity must implement preventative controls to reduce the likelihood of unauthorised or fraudulent transactions. These controls must be commensurate with the entity's operations and risk exposure, including those participating in the Instant Payment Switch, real-time or high-frequency environments and at a minimum, and where applicable, include velocity checks, transaction pattern analysis, use of negative and positive datasets, geo-location tracking, risk scoring models, and address verification service.

11.12 The entity must establish an awareness and training programme that includes:

11.12.1 A comprehensive information security awareness training program that must be established to enhance the overall information security awareness levels within the entity's organisational structure. The training program must cover information security policies and standards, as well as each employee's individual responsibility to safeguard information system assets. The program must ensure:

a) the board undergoes training to raise their awareness on risks associated with the use of technology and enhance their understanding of cyber risk management practices;

b) the entity must ensure, as part of its third-party due diligence and onboarding processes, that third-party service providers have appropriate cybersecurity awareness training programmes in place, commensurate with the nature and criticality of the services provided;

c) the information security awareness training program must be conducted throughout the year using multiple communication methods and include periodic testing to reinforce learning and measure effectiveness; and

d) the information security awareness training program must be reviewed at least annually, or whenever new threats emerge, to ensure its relevance and effectiveness. Reviews must take into account technological developments, emerging risks, and address a range of threats.

11.12.2 A structured fraud awareness program to ensure that all employees, users and third-party service providers, understand the nature of fraud risks and their role in preventing, detecting, and reporting such incidents. These must be conducted and updated at least annually to account for changes in the fraud threat landscape and fraud threats identified through threat intelligence.

Detection

11.13 Proactive capabilities must be established to continuously monitor and detect anomalous cyber activities, events and must be integrated with incident response processes across systems, networks and transactions, including the monitoring of all payments for the detection of any fraudulent or suspicious activities. These must at minimum include:

11.13.1 performing continuous vulnerability scanning of the external and internal environment which may include but not limited to automated scanning that support the changed and current system landscape;

11.13.2 establishing proactive security monitoring capabilities, which include a Security Operations Centre (SOC) or equivalent or engaging managed security service providers to enable continuous monitoring and analysis of cyber events, as well as timely detection and response to cyber incidents;

11.13.3 establishing and maintaining a process for secure collection, retention, and review of audit logs to support security monitoring operations. The audit logs must be retained for a minimum period of twelve (12) months. This process must include the correlation of log events to detect suspicious or anomalous activity patterns, and ensure that logs are protected against unauthorised access, modification, or deletion; and

11.13.4 implementing and maintaining fraud monitoring and detection processes that are aligned with the fraud risks prevalent within the entity's ecosystem, impacting both the entity and its users, and commensurate with its risk exposure and operational complexity. These processes must incorporate

preventive, predictive, and detective controls, and may include, but are not limited to, systems utilising behavioural analytics, transaction pattern analysis, or other emerging technologies to detect, prevent, and respond to suspicious or anomalous activity.

11.14 The entity must establish and maintain cyber threat intelligence capabilities to collect, analyse, and monitor cyber and fraud-related information relevant to its business functions, detect internal and external threats, and participate in trusted information-sharing arrangements with external parties to ensure actionable intelligence on fraud and cyber threats, vulnerabilities, and incidents.

Response and Recovery

11.15 The entity must develop and maintain a Cyber Incident Response Plan that enables the timely containment and mitigation of cyber incidents, supports the secure and timely restoration of affected services, and which outline clear procedures for communication, coordination, and response across cyber threat scenarios. The plan must be tested annually to ensure its effectiveness against both current and emerging threats and must be aligned with the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements defined in section 13.1.

11.16 The entity must develop a Fraud Response Plan that specifies the approach to manage actual or suspected fraud incidents. The plan must include clear procedures to facilitate timely identification, resolution and corrective measures and must be tested annually to ensure its effectiveness against both current and emerging threats.

11.17 Upon detection of a successful cyberattack or a fraudulent payment transaction resulting from such an attack, an investigation must be conducted to determine the nature, extent, and impact of the incident.

11.18 While the investigation is ongoing, actions must be taken to contain the incident to prevent further damage and commence recovery efforts to restore operations or redress the fraudulent payment transaction based on the response planning.

11.19 The entity must design and periodically test its payment systems and processes to enable the safe resumption of critical operations within two (2) hours of a disruption. Notwithstanding this capability to resume critical operations within two (2) hours, reasonable judgment must be exercised in effecting resumption so that risks do not escalate while taking into account the completion of settlement within the National Payment System by the end of each business day.

11.20 The entity must maintain and test data backup and restoration procedures quarterly and develop scenarios and test response, resumption, and recovery plans at least twice every year for critical systems. The aforesaid test response, resumption, and recovery plans must support objectives to protect and, if necessary, re-establish the integrity and availability of its operations and the confidentiality of its information assets, at a recovery point objective of at least 5 minutes.

11.21 The entity must consult and coordinate with relevant internal and external stakeholders during the establishment of its response, resumption, and recovery plans.

11.22 The Data Centre (DC) and Disaster Recovery (DR) sites must be geographically separated so that both sites are not affected by a similar threat associated with their location.

11.23 All successful cyberattack incidents must be reported to the Bank as follows:

11.23.1 Within a maximum of 24 hours for the preliminary notification of the cyber incident;

11.23.2 This must be coordinated through the Preliminary Incident Notification Report, as per Annexure A of this Determination;

11.23.3 The entity must direct these written notifications to the Director responsible for the National Payment System or the person(s) acting on his or her behalf;

11.23.4 Any further updates should be provided as new information emerges from the investigation; and

11.23.5 Also, where required, additional documents may be provided and appended to the Incident Progress Report, as per Annexure B of this Determination.

11.24 After the completion of the reporting contemplated in section 11.23 of this Determination, the entity is required to conduct an impact assessment on the successful cyberattack incident and report to the Bank within a month from the time the incident becomes known.

11.25 The reporting required in section 11.24 of this Determination must indicate any financial loss, data loss, or availability loss. Additionally, incident closures must be accompanied by the completed Incident Closure Report, as per Annexure C of this Determination.

11.26 Pursuant to section 11.23 of this Determination, the entity must prepare use cases, which may include but are not limited to the causes of the incident, how it was detected, indicators of compromise (IOCs), preventative measures, and post-incident controls implemented. This information must be shared with the relevant sectoral and/or national cybersecurity coordination and response bodies, within a reasonable period following the completion of the post-incident review process, in a manner that is cognisant of the confidentiality, personal identifiable information (PII), and other sensitive data, to support collective learning and strengthen sector-wide and national cyber resilience.

11.27 The entity must:

11.27.1 assess physical and transition climate risks that could disrupt core payment systems, clearing, and settlement infrastructures, including but not limited to:

a) Power grid failures or energy supply disruptions.

b) Data centre vulnerabilities (for example, flooding, extreme temperatures).

c) Geopolitical risks affecting critical supply chains (for example, IT hardware/software dependencies).

11.27.2 integrate climate risk findings into operational resilience frameworks, ensuring:

a) Contingency plans address climate-related disruptions (for example, backup energy solutions, geographically dispersed infrastructure).

b) Recovery Time Objectives (RTOs) account for climate-induced delays (for example, extended outages due to natural disasters).

12. Safety Standards

12.1 The entity must implement encryption, tokenisation, or masking for the transmission of data across open and public networks, in accordance with industry best practice standards or applicable laws.

12.2 Payment card data, including Primary Account Numbers (PANs), must be tokenised or encrypted using an equivalent strong cryptographic mechanism for both storage and internal processing. The tokenisation or cryptographic method must follow best practice security standards and ensure that the original card data cannot be read or recovered outside a secure system, where tokens are stored and encryption keys are securely managed.

12.3 Prior to effecting any payment transaction during initiation, whether through, but not limited to, a payment instrument, website, or mobile application, MFA must be applied in a risk-based and adaptive manner.

12.4 MFA is mandatory for high-risk transactions, including but not limited to once-off payments, first-time payment instructions that establish or activate a recurring payment mandate, transactions involving unusual spending patterns, or those flagged by fraud detection systems.

12.5 Where MFA is not technologically feasible due to limitations inherent in the access channel or technology in use, the entity must implement alternative compensating controls that offer an equivalent level of security and are demonstrably effective in mitigating the associated risks.

12.6 Low-risk transactions, such as recurring payments, do not require repeated MFA following the initial verification, provided that adequate monitoring mechanisms are in place to detect anomalies

12.7 The entity must adopt relevant best practice standards to complement the requirements of this Determination, taking into account the nature, size, complexity, and risk profile of its operations. The Bank may, where necessary, prescribe or require the implementation of specific standards or frameworks in line with industry developments and evolving risks.

13. Risk-Based Risk Indicators and Tolerance Levels

13.1 The entity is required, at a minimum, to consider and adhere to the following risk indicators and tolerance levels for the efficient, effective, and safe operation of the National Payment System.

Risk Indicator	**Tolerance Level**
Uptime of Critical Systems (calculated daily, scheduled downtime not included)	99.9%
Recovery Time Objective	Within two (2) hours
Recovery Point Objective of Critical Systems	5 minutes

Test backup and restoration procedures	At least four (4) successful tests in a year
Test response, resumption, and recovery plans	At least two (2) successful tests in a year

PART IV
OTHER REGULATORY REQUIREMENTS

14. Oversight

14.1 The Bank may inspect all records, data, or other relevant information to ensure compliance with this Determination.

15. Administrative Penalties

15.1 Any person or entity who contravenes or otherwise fails to comply with this Determination will be subject to administrative penalties or criminal investigation or prosecution as provided under the Act.

16. General

16.1 This Determination is not exhaustive and may be supplemented and/or amended from time to time.

17. Repeal

17.1 This Determination repeals and replaces the Determination on the Operational and Cybersecurity Standards within the National Payment System (PSD-12), published in Government Gazette No. 7984, General Notice No. 737, issued on 21 December 2022.

18. Effective Date

18.1 This Determination takes effect on the date of publication in the Government Gazette. However, existing payment service providers and payment system operators will be granted a six (6) month grace period to comply with this Determination from the effective date.

19. Enquiries

19.1 All enquiries related to this Determination must be directed to:

THE DIRECTOR
NATIONAL PAYMENT SYSTEM AND FINANCIAL
SURVEILLANCE DEPARTMENT
BANK OF NAMIBIA
P.O. BOX 2882
WINDHOEK
NAMIBIA

Annexure – Cyber Incident Notification to the Bank of Namibia

<table>
<tr><th colspan="10">ANNEXURE A: PRELIMINARY INCIDENT NOTIFICATION REPORT</th></tr>
<tr><td>Entity's Name</td><td colspan="9"></td></tr>
<tr><td>Incident Reference Number</td><td colspan="3"></td><td>Date of Report</td><td colspan="5"></td></tr>
<tr><td>Severity Impact Rating</td><td colspan="3"></td><td>Time of Report</td><td colspan="5"></td></tr>
<tr><td>Type of Incident</td><td colspan="9"></td></tr>
<tr><td rowspan="5">Incident Root Cause Areas</td><td colspan="9">Mark X in the appropriate box</td></tr>
<tr><td>Asset Management</td><td></td><td>Access Controls</td><td></td><td>Operational Security</td><td></td><td>Communications Security</td><td></td></tr>
<tr><td>Third-Party Relationship</td><td></td><td>Human Resource</td><td></td><td>Cryptography</td><td></td><td>Physical and Environmental</td><td></td></tr>
<tr><td>Security Audit and Testing</td><td></td><td>System Acquisition, Development and Maintenance</td><td></td><td>Information Security Business Continuity Management</td><td></td><td>Other</td><td></td></tr>
<tr><td colspan="9">If other, please specify.</td></tr>
<tr><td>Description of Incident</td><td colspan="9"></td></tr>
<tr><td>Estimated Value of Loss (NAD)</td><td colspan="9"></td></tr>
<tr><td>Indicators of Attack (IoA), if any?</td><td colspan="9"></td></tr>
<tr><td>Indicators of Compromise (IoCs), if any?</td><td colspan="9"></td></tr>
<tr><td>Description of Impact</td><td colspan="9"></td></tr>
<tr><td>Timeline of incidents and how it was discovered</td><td colspan="9"></td></tr>
<tr><td>Description of mitigation effort</td><td colspan="9"></td></tr>
<tr><td>Response Lead (Contact) Name</td><td colspan="3"></td><td>Signature</td><td colspan="5"></td></tr>
</table>

ANNEXURE B: INCIDENT PROGRESS REPORT					
Entity's Name					
Incident Reference Number		**Severity Impact Rating**			
Current Situation as of	**Date:**		**Time:**		
What has happened since the last notification?					
When did changes happen?					
How, when and by who was anything new discovered?					
Current understanding of what caused the incident?					
Was source internal, external or unknown?					
What other entities or systems might become affected?					
Impact Update (In terms of operations, users, data/ systems, monetary, legal or regulatory and reputational.)					
Estimated Value of Loss (NAD)					
What response actions have taken place so far?					
How effective has the actions been?					
What challenges remain to be resolved in the situation?					
Estimated resolution time?					
Indicators of Compromise (IoC), if any?					
Response Lead (Contact) Name		**Signature**			

ANNEXURE C: INCIDENT CLOSURE REPORT				
Entity's Name				
Incident Reference Number		**Severity Impact Rating**		
Current Situation as of	**Date:**		**Time:**	
Incident Timelines	**Incident Response Start Date**		**Incident Response Closure Date**	
Description of Incident				
Incident Root Cause				
Indicators of Compromise (IoCs) identified				
Description of Incident response plan and action				
Description of parties involved in response action				
Description of Bank of Namibia's role, if applicable				
Description of Role Played by Third Parties, if applicable				
Original estimated resolution time (as reported in incident notification report)		**Actual resolution time**		
Impact (In terms of operations, customers, data/ systems, monetary, legal or regulatory and reputational.)				
Estimated Value of Loss (NAD)				
Challenges in recovery process				
Lessons learned and planned developmental actions				
Response Lead (Contact) Name		**Signature**		