GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$8.00 WINDHOEK - 21 December 2022 No. 7984

CONTENTS

Page

General Notice

BANK OF NAMIBIA

No. 737 2022

DETERMINATION UNDER THE PAYMENT SYSTEM MANAGEMENT ACT, 2003
(ACT NO. 18 OF 2003), AS AMENDED

In my capacity as Governor of the Bank of Namibia (The Bank), and under the powers vested in the Bank under Section 14 of the Payment System Management Act, 2003 (Act No. 18 of 2003), as amended, I hereby issue this **Determination of the Operational and Cybersecurity Standards within the National Payment System (PSD-12).** This Determination becomes effective on 1 July 2023.

J. !GAWAXAB
GOVERNOR
BANK OF NAMIBIA Windhoek, 12 December 2022

Payment System Determination (PSD-12)

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

Arrangement of Paragraphs

PART I
PRELIMINARY

PARAGRAPH

PART II
STATEMENT OF POLICY

PART III
IMPLEMENTATION AND SPECIFIC REQUIREMENTS

PART IV
OTHER REGULATORY REQUIREMENTS

PART I: PRELIMINARY

1. **Short Title** – Operational and Cybersecurity Standards within National Payment System (NPS)

2. **Application** – This Determination shall apply to all persons within the NPS.

3. **Definitions** – In this Determination, unless the context otherwise indicates, the words and expressions used herein shall have the same meaning assigned to them in the Payment System Management Act, 2003 (Act No. 18 of 2003), as amended and cognate expressions shall have corresponding meanings:

3.1. **"Act"** means the Payment System Management Act, 2003 (Act No. 18 of 2003), as amended.

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

3.3. **"Availability loss"** means all events that stop planned production for an appreciable amount of time, in minutes.

3.4. **"Critical operations"** means activity, function, process, or service, the loss of which, would affect the continued operation of the NPS, its customers and/or the broader financial system.

3.5. **"Critical systems"** means all systems required for the efficient and effective operation of the National Payment System as per the following levels:

1. Financial Market Infrastructures (FMIs).

2. Interoperable Retail Payment Systems such as Payment Card, Electronic Fund Transfers (EFT), Electronic-Money (E-money) and any payment activity as may be authorised or designated by the Bank.

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

3.7. **"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 financial and data loss.

3.8. **"Cybersecurity or resilience"** means the ability to anticipate, withstand, contain and rapidly recover from a cyberattack.

3.9. **"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 an entity.

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

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

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

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

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

3.15. **"Identification"** means to develop the organisational understanding required to manage cyber risk to systems, assets, data and capabilities.

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

3.17. **"Integrity"** means the status of not having been modified or destroyed in an unauthorised manner.

3.18. **"National Payment System (NPS)"** means the payment system as a whole, and includes any payment system, settlement system, clearing systems and payment system arrangement used in the process of effecting payment between payers and beneficiaries.

3.19. **"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.

3.20. **"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."

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

3.22. **"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.

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

3.24. **"Respond"** means to develop and implement appropriate activities to be able to take action when it detects a cyber event.

3.25. **"Person"** means a natural or juristic person.

3.26. **"Principles for Financial Market Infrastructures (PFMI)"** are international standards for financial market infrastructures, i.e. payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories, issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) and the Bank for International Settlements (BIS).

3.27. **"Protect"** means the development and implementation of appropriate safeguards, controls and measures to enable the reliable delivery of critical infrastructure services.

3.28. **"Successful attack"** means the gaining of access by threat actors, who try to gain unauthorized access, steal data or cause damage to various computing systems.

3.29. **"Tolerance level"** means the specified level of risk to be tolerated by a Board and / or Senior Management or the Bank of Namibia. For example, 2 hours up time or availability is a tolerance level.

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

3.31. **"Two-factor authentication"** means a two-step verification method which provides users with two different authentication factors to verify themselves.

3.32. **"Vulnerability"** means a weakness, susceptibility or flaw in a system that an attacker can access and exploit to compromise system security. The vulnerability arises from the confluence of three elements: the presence of susceptibility or flaw in a system; an attacker's access to that flaw; and an attacker's capability to exploit the flaw.

4. **Authorisation** – Authority for the Bank to issue this Determination is provided in section 14 of the Act.

PART II: STATEMENT OF POLICY

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 Financial Market Infrastructures (FMIs), Designated Non-Bank Financial Institutions (NBFIs), participants of FMIs, Retail Payment Systems (such as electronic funds transfers, payment card, electronic-money etc.), Payment Service Providers (PSPs) and any other entities licensed or authorised within the National Payment System, including participants in the Financial Technology (FinTech) Regulatory Framework of the Bank.

7. **Position of the Bank** – The advent of digital transformation and the rising prominence of digital payments poses an increased risk of cyberattacks, which further poses a significant threat to financial stability. The Bank understands that cyberattacks will happen. Therefore, it is imperative for financial institutions to proactively implement and manage controls for enhanced cybersecurity and planned response.

Cyberattacks can threaten financial stability by disrupting interconnected operational networks and their critical nodes, which affects operational resilience. If operational resilience is not properly managed within the NPS, FMIs and other key stakeholders within the NPS can be sources of financial shocks and a major channel through which these shocks are transmitted across domestic and international financial markets.

The above can create vulnerabilities which can result in the loss of data and the fraudulent loss of money, which can lead to the collapse of the financial system. Thus, the regulation of cybersecurity and operational resilience is dutiful to the achievement of one of the Bank's mandate in section 2 (1) of the Act, i.e. to ensure the safe, secure, efficient and cost-effective operation of the NPS.

8. **Application of the Act** – Unless expressly stated otherwise, the provisions of the Act, as well as the related Determinations, Guidelines and Directives, shall apply to all persons within the National Payment System.

PART III: OPERATIONAL AND CYBERSECURITY STANDARDS

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

9.1. The Boards of the entities to which this Determination applies 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 organisation's strategic objectives.

9.3. The Board must set and approve risk tolerances which are aligned with the key risk indicators contemplated in section 13 of this Determination.

9.4. The Board must 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 of this Determination.

9.5. The Board must ensure participation in industry-wide collaborative efforts to effectively respond to and recover from cyberattacks within the financial system as a whole.

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

9.7. 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 an entity responsible for the implementation of information security, cybersecurity and operational resilience.

9.8. The security officer(s) contemplated in section 9.7 of this Determination must-have reporting access to the Board.

10. Framework

10.1. The Framework must clearly determine information security, cybersecurity and operational resilience objectives, and tolerances.

10.2. The Framework must, at a minimum, include measures of identification, protection, detection, response and recovery as contemplated in section 11 of this Determination.

10.3. The Framework must clearly define the roles and responsibilities for managing information security, cybersecurity and operational resilience, including in emergencies and in a crisis.

10.4. The Framework must be reviewed and updated periodically to ensure that it remains relevant.

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

10.6. 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. There must be an identification of business functions and supporting processes and a risk assessment performed, at least once every year, or when there is a significant change that affects business functions or processes, to ensure an understanding of the importance of each business function and supporting processes, and their interdependencies within the NPS.

11.2. The identified business functions and supporting processes must be classified in terms of criticality, which in turn must guide the prioritisation of its protective, detective, response and recovery efforts.

11.3. Pursuant to section 11.11, there must be threat intelligence processes to identify threats, vulnerabilities and payment fraud that the entity could be exposed to, including but not limited to one penetration testing every three years for critical systems.

Protection

11.4. 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.

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

Detection

11.6. Capabilities must be established to continuously monitor and detect anomalous cyber activities and events, including the monitoring of all payments for the detection of any fraudulent or suspicious activities.

Response and Recovery

11.7. Upon detection of a successful cyberattack or fraudulent payment transaction as a result of a successful cyber-attack, an investigation must be performed to determine the nature, extent and damage inflicted.

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

11.9. An 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.

11.10. 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 NPS by the end of each business day.

11.11. An entity must 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.

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

11.13. All successful cyberattack incidents must be reported to the Bank, at least within 24 hours for the preliminary notification of the cyber incident.

11.14. After the completion of the reporting contemplated in section 11.13, 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.

11.15. The reporting required in section 11.14 must at least indicate any financial loss, data loss and availability loss.

12. Safety Standards

12.1. Encryption or tokenization or masking of transmission of data across open and public networks is required in line with best practice encryption or tokenization or masking standards.

12.2. Prior to the effecting of any payment transaction during payment initiation on a payment instrument, website, and mobile application, two-factor authentication must be required. This means two-factor authentication is required for every payment.

12.3. The Bank may require the implementation of best practice standards from time to time.

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 NPS.

Risk Indicator	Tolerance Level
Uptime or Availability of Critical Systems	99.9%
Recovery Time Objective	Within two (2) hours
Recovery Point Objective of Critical Systems	5 minutes
Test response, resumption, and recovery plans	Two successful tests in a year

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

15. Administrative Penalties – Any person that contravenes or otherwise fails to comply with any provisions of this Determination will be subjected to administrative penalties as provided for under the Act.

16. Effective Date – This Determination becomes effective on 01 July 2023.

17. Enquiries – All enquiries related to this Determination must be directed to:

The Director: National Payment System
Bank of Namibia
P.O. Box 2882
Windhoek