# GOVERNMENT GAZETTE

## OF THE

# REPUBLIC OF NAMIBIA

N$6.00 WINDHOEK - 24 October 2017 No. 6448


CONTENTS

*Page*



## General Notice

**BANK OF NAMIBIA**

No. 425 2017

DETERMINATIONS UNDER THE BANKING INSTITUTIONS ACT, 1998:
INFORMATION SECURITY

In my capacity as Governor of the Bank of Namibia (Bank), and under the powers vested in the Bank by virtue of section 71(3) of the Banking Institutions Act, 1998 (Act No. 2 of 1998) as amended, I hereby issue the Determination on Information Security (BID-30), which Determination shall become effective 1 March 2018.

**I. SHIIMI**
**GOVERNOR**

**Determination No. BID-30**
**INFORMATION SECURITY**
**Arrangement of Paragraphs**

PART I
PRELIMINARY

**PARAGRAPH**



PART II
STATEMENT OF POLICY



PART III
IMPLEMENTATION AND SPECIFIC REQUIREMENTS



PART IV
FREQUENCY OF REVIEW

PART V
CORRECTIVE MEASURES

PART VI
EFFECTIVE DATE

The effective date of this Determination shall be 1 March 2018.

## PART I: PRELIMINARY

**1.** **Short Title** - Information Security

**2.** **Authorisation** - Authority for the Bank to issue this Determination is provided in Section 71(3) of the Banking Institutions Act, 1998 (Act).

**3.** **Application** - This Determination applies to all banking institutions authorised by the Bank to conduct banking business in Namibia and banking groups to which they belong.

**4.** **Definitions** - Terms used within this Determination are as defined in the Act, as further defined below, or as reasonably implied by contextual usage:

**4.1** **"Availability"** - ensuring timely and reliable access to and use of information.

**4.2** **"Bank"** - the Bank of Namibia as referred to in section 4 of the Bank of Namibia Act, 1997;

**4.3** **"banking institution"** - a public company authorised under the Act to conduct banking business. Also referred to as the "bank".

**4.4** **"Confidentiality"** - preserving access or disclosure of sensitive information (including privacy and proprietary information) to unauthorised individuals, entities or processes.

**4.5** **"Data at rest"** - means data held or stored on some form of storage system.

**4.6** **"Data in transit or motion"** - means data being transferred over some form of communication link.

**4.7** **"Data in use"** - means data that is being accessed or used by a system at a point in time.

**4.8** **"Firewall"** - is a system or combination of systems that enforces a boundary between two or more networks typically forming a barrier between a secure and an open environment such as the Internet;

**4.9** **"Information"** - knowledge or facts essential to an institution. It can exist in many forms i.e. printed or written in paper, stored electronically, transmitted by post or electronically, shown on films, or spoken in conversation;

**4.10** **"Information security"** - controls that seek to maintain and protect confidentiality, integrity and availability of information;

**4.11** **"Integrity"** - guarding against improper information modification or destruction, and includes ensuring non repudiation of information and authenticity;

**4.12** **"Malware"** - a collective term used to describe a variety of malicious programs (including viruses, worms, Trojan horses, ransomware, spyware, adware, shareware etc.) designed to spread and replicate from computer to computer through communications links or through sharing of electronic files to interfere with or damage computer operation.

**4.13** **"Material activities"** means activities of such importance that have a significant impact on the banking institution's business operations or its ability to manage risks effectively should such activities be disrupted;

**4.14** **"Need to know basis"** - the restriction of sensitive data using a tight security method in which information is only given to those who need it, to do a particular task;

**4.15** **"Outsourcing arrangement"** - means a written, legally binding agreement between a banking institution and a service provider, whereby a service provider performs a business activity, function and/or process that could ordinarily be undertaken by the banking institution itself;

**4.16** **"Penetration testing"** - the practice of testing a computer system, network or web application for security weaknesses or vulnerabilities that might potentially be exploited;

**4.17** **"Security incident"** - An event or series of events that indicate a compromise of the confidentiality, integrity or availability of an organisation's system or data;

**4.18** **"Vulnerability assessments"** - the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system;

## PART II: STATEMENT OF POLICY

**5.** **Purpose** - This Determination is intended to ensure that banking institutions put in place a robust information security program that will ensure that the business impact from the occurrence of operational information security vulnerabilities or security incidents are kept at a minimal or within the banking institution risk appetite levels.

**6.** **Scope** - This Determination applies to all banking institutions authorised and operating in Namibia.

**7.** **Scope exclusions** - None

**8.** **Responsibility** - The Board of Directors of each banking institution shall be responsible to ensure that an information security policy and program is established and implemented to comply with the requirements in this Determination. The policy, program, the overall institution's strategy and objectives, as well as the risk appetite of the institution should be aligned with the principles contained herein.

## PART III: IMPLEMENTATION AND SPECIFIC REQUIREMENTS

**9.** **Overview**

Information is a key resource for all enterprises and from the time information is created to the moment it is destroyed, technology plays a significant role. Given the increasing trend of data breaches from a global perspective and the escalation of security incidents such as cyber attacks, there is an increasing need for the banking institution to improve and maintain proactive security programmes to protect information against unauthorised access, disclosure, inadvertent modifications as well as to ensure that services are continuously available to internal and external stakeholders.

Consequences of failure to protect information include financial and reputational risk amongst other risks. Equally, there are significant operational and financial costs related to containing, investigating, and remediating security breaches, which can impact the banking institution that has suffered a breach.

Effective management of information security risks can be implemented through a variety of technologies or internal control systems appropriate to the types of services offered, which could potentially change over time. The general principle is that the banking institution is expected to implement information security arrangements that are "fit for purpose" (i.e. appropriate to the risk management systems of the banking institution, without compromising the minimum laid down principles prescribed in this Determination).

Other than the requirements provided in this Determination, the Bank does not prescribe specific information security standards to be used by the banking institution. The banking institution should take into account relevant industry information security standards and

sound international best practices [1] as appropriate. The banking institution should keep up with the most current information and information security issues and use this information to regularly update their information security program.

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

10.1 The banking institution should establish, implement, and maintain an information security policy. The policy should be in accordance with business requirements, relevant laws and regulations and approved by the board.

10.2 The banking institution should establish, implement, maintain and continually improve an information security program. The board or board appointed committee should approve the information security program.

10.3 The board should ensure that the information security program is aligned with the banking institution's strategic direction and integrated in the institution's processes.

10.4 The board may appoint a committee to assist with its IT governance and may delegate implementation of the principles to management.

10.5 The banking Institution should implement a formal security awareness as part of the program to make all employees and relevant external parties aware of the information security policy, their contribution towards the effectiveness of the information security program and the implications of non-conformance.

10.6 The Board should be regularly appraised of the banking institution's information security risk profile to ensure that it remains consistent with the banking institution's risk tolerance as well as the banking institution's overall business objectives.

10.7 Senior management should closely oversee the institution's implementation of its information security policy, procedures and controls that support it.

**11. Information Security Program**

11.1 The banking institution should establish a documented information security program to clearly articulate how it plans to effectively identify the information security risks that it faces, determine its information security objectives and risk tolerance, and mitigate and manage its information security risks to support its objectives.

11.2 The banking institution's information security program should be consistent with its enterprise risk management framework or a similar framework which addresses enterprise wide risk. Such consistency is important and recognises that an institution's information security program is likely to overlap with the policies, procedures and controls that it has established to manage other areas of risks. (For example, information security risk should also be a consideration in the banking institution's IT policy to limit access to critical Information and Communication Technology infrastructure) and its human resource policies (i.e. to manage "insider" threats).

**12. Information Security Policies and Procedures**

12.1 The banking institution should establish and maintain an information security policy as referred to in paragraph 10.1.

[1] Examples of industry information security standards and sound practices include: ISO, ISF, NIST, COBIT-5, PCI-DSS standards.

12.2 The banking institution should extend their information security practices to third parties through Service Level Agreements (SLAs) i.e. the banking institution should ensure that information security controls are considered and enforced by third parties.

12.3 The banking institution should ensure that information security operational procedures for protecting information are documented and implemented.

12.4 The banking institution should establish documentation and business justification for the use of all services, protocols, including documentation for security features implemented for those protocols which are considered to be insecure.

**13. Vulnerability Management Program**

13.1 The banking institution should perform vulnerability scans of business applications, systems, equipment, and network devices to help identify known technical vulnerabilities, to determine the extent to which the banking institution is exposed to threats (e.g. checking whether powerful system utilities/commands have been disabled or weak passwords are being used), to prioritize the remediation of vulnerabilities and to provide a high-level view of vulnerabilities across the organization's technical infrastructure.

13.2 The banking institution's vulnerability scans should be performed using automated vulnerability scanning software or a commercial vulnerability scanning service and restricted to a limited number of authorised individuals (e.g. using a dedicated account that is only used for vulnerability scanning). Technical vulnerabilities should be remediated by using a patch management process or as per the institution's vulnerability management practices.

13.3 The banking institution should run internal and external network vulnerability scans on a periodic basis or after any significant changes in the network (i.e. new components to critical systems, upgrades, firewall modifications etc.)

13.4 The banking institution should Identify and document internal and external vulnerabilities. The likelihood of an occurrence, potential business impact and applicable risk responses should be identified and documented.

**14. Third Party Service Providers / Partnerships**

14.1 Agreements for all material outsourcing arrangements and critical IT service providers should include the provision for safeguarding the banking institution's information. Material outsourcing arrangement should follow the principles set out in the Determination on Outsourcing of Certain Activities or Functions of Banking Institutions (BID-26).

**15. Protection of Systems and Networks**

15.1 The banking institution should install and maintain an intrusion detection system (IDS) and an intrusion prevention system (IPS) configuration to automatically detect and block unauthorised network access including wired, wireless and remote access.

15.2 The banking institution should install perimeter firewalls between all shared and/or public networks and the internally managed data environment to control access.

15.3 The banking institution should use appropriate encryption (e.g. end-to-end encryption) and authentication measures on a risk based basis to safeguard data during transmission across open and public networks as per the institution's classification scheme on criticality and sensitivity of information.

15.4 The banking institution should protect all systems against malware, filter incoming traffic such as emails and downloads, and regularly update anti-virus software or programs. The banking institution should implement and maintain preventative, detective, and corrective measures (i.e. especially up-to-date security patches and virus control measures) across the enterprise to protect data from malware (e.g. viruses, spyware, spam and cyber attacks).

15.5 The banking institution should have logging mechanisms and have the ability to track user activities that are critical in preventing, detecting, or minimising the impact of a data compromise. Key information relating to system/network monitoring should be retained long enough to meet legal/regulatory requirements. The banking institution should retain an audit trail history of at least three (3) months, immediately available for analysis (for example, online, archived to portable storage media and or restorable from backup).

**16. Identity and Access Control Management**

16.1 The banking institution should establish capabilities to continuously monitor the network, physical environment and employees to detect anomalous activities and events.

16.2 The banking institution should establish adequate controls over systems by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as roles-based access, logging and reviewing of the systems activities of privileged users regularly, strong authentication, and monitoring for anomalies should be implemented.

16.3 The banking institution should implement appropriate measures to protect data at rest, data in motion and data in use, as per the criticality and sensitivity of the information. This should include, but not be restricted to, appropriate encryption and authentication measures (e.g. multifactor authentication).

16.4 Physical and logical access to systems should be permitted only for individuals who are authorised, and authorization should be limited to individuals who are appropriately trained and monitored. Access to data should be dealt with absolute security and confidentiality. The Banking institution should ensure that such access is restricted only to those with a legitimate business requirement and according to job responsibilities.

16.5 The institution should put controls in place to manage all mobile devices connected to the institution's network in accordance with the relevant security standard.

**17. Incident Response and Recovery Plan**

17.1 The banking institution is required to report all material information security related incidents to the Bank immediately as and when it happens. The banking institution should also communicate with internal and external parties to ensure coordinated response to incidents as well as determine the type of information to be reported and when.

17.2 Should security of the banking institution be breached in any way, the banking institution should perform a thorough investigation to determine its nature and extent as well as the damage inflicted. While the investigation is on going, the banking institution should also take immediate actions to contain the situation to prevent further damage and commence recovery efforts to restore operations based on their response planning.

17.3 The banking institution should be able to resume critical operations rapidly and should design and test its systems and processes to enable the safe resumption of critical operations.

17.4 The banking institution should execute recovery processes and procedures to control the scope of the incident and restore affected data. Expansion of the event should be prevented by addressing its cause and eliminate any malware or remediate any security vulnerabilities.

17.5 The banking institution should evaluate the incident and incorporate lessons learned into future activities by meeting with senior management and other appropriate personnel to discuss potential improvements so as to prevent similar incidents in the future. The banking institution should engage independent auditors or non-audit institutions such as network security consultants / specialist every 3 years or when significant changes are made to the systems so as to evaluate their security and monitoring systems, identify weaknesses and suggest improvements.

**18. Regular Monitoring and Testing**

18.1. The banking institution should establish a comprehensive testing program to validate the effectiveness of all elements of its information security program. The results of the testing program should be used to support on-going improvement of its information security program.

18.2. The banking institution should have proper procedures in place to ensure that at least a member of its board and representatives from senior management are involved appropriately (e.g. as part of crisis management teams) and informed of test results.

18.3. The banking institution should perform vulnerability assessments as and when required to identify and assess security vulnerabilities in their systems and processes. The banking institution should establish a process to prioritise and remedy issues identified in vulnerability assessments and perform subsequent validation to assess whether gaps have been fully addressed.

18.4. The banking institution should implement a methodology for vulnerability assessments and penetration testing in different areas within the technical infrastructure that is based on industry-accepted penetration testing approaches (based on applicable standards) to identify vulnerabilities that may affect their systems, networks, people or processes. The tests should simulate actual attacks on the systems. The banking institution should ensure that these tests are conducted regularly and whenever systems are updated or deployed.

**PART IV: FREQUENCY OF REVIEW**

The banking institution's information security policy and program should be reviewed and updated as and when required, or at least after every 3 years, to ensure that it remains relevant.

**PART V: CORRECTIVE MEASURES**

If a banking institution fails to comply with this determination, then the Bank may pursue any remedial measures as provided under the Act or any other measures the Bank may deem appropriate.

**PART VI: EFFECTIVE DATE**

The effective date of this Determination shall be 1 March 2018.

Questions relating to this Determination should be addressed to the Director, Banking Supervision Department, Bank of Namibia, Tel: 283 5040.

---