Bank of Namibia
71 Robert Mugabe Avenue
P.O. Box 2882, Windhoek, Namibia
Tel: +264-61-283 5111
Fax: +264-61-283 5228

Bank Supervision Department

BANK OF NAMIBIA

No. 2 **2010**

GUIDELINE UNDER THE BANKING INSTITUTIONS ACT, 1998 (ACT NO.2 OF 1998): MINIMUM SECURITY STANDARDS FOR BANKING INSTITUTIONS

In my capacity as Governor of the Bank of Namibia (Bank) and under the power vested in the Bank by virtue of section 3(1)of the Banking Institutions Act,1998 (Act No 2 of 1998), I hereby issue the guideline on **MINIMUM SECURITY STANDARDS FOR BANKING INSTITUTIONS (BIG-2).**

I.W. SHIIMI
GOVERNOR

Windhoek, 05 May 2010

Guideline No BIG-2

MINIMUM SECURITY STANDARDS

Arrangement of paragraphs

PART I: PRELIMINARY

1. **Short Title** – Minimum security standards

2. **Authorization** - This valuation guideline is issued in terms of section 3 of the Banking Institutions Act, 1998 (Act No 2 of 1998).

3. **Application** - This guideline applies to all banking institutions authorised by the Bank to conduct banking business in Namibia.

4. **ACRONYMS:**
   ATM – Automated Teller Machine
   CCTV – Closed Circuit Television
   PIR – Passive Infra-Red

5. **Definitions** – Terms used within this guideline are as defined in the Act, as further defined below, or as reasonably implied by the contextual usage.

   a. **Anti-bandit door** – Attack resistant door for the security of premises where better penetration resistance is a requirement.

   b. **Door contact** – A protective device which monitors the opening and closure of doors and windows.

   c. **High risk areas** – Must be as defined in the policies of the respective banking institutions, taking into consideration criteria such as the location, escape routes, history and population density and proximity of police station.

   d. **PIR detector** –Motion detectors using passive infra red (PIR) technology to detect movement of body heat to activate the alarm in the event of an intrusion.

   e. **Seismic detector** – A universal application for protection of strong room walls and doors, safes and automatic teller machines.

   f. **Space Detectors** – A device that can detect a presence of a human being

   g. **Thoroughfares** – Path open at both ends

PART II: STATEMENT OF POLICY

6. **PURPOSE** - This guideline is intended to ensure that banking institutions provide the safety to their clients while transacting as well as protect their clients' money in and around their premises. The guideline also aims to improve and strengthen physical security at banking institutions. It is believed that the prescribed requirements will eventually reduce or mitigate the risks of theft and armed robberies targeting these banking institutions. The prescribed requirements are not exhaustive and banking institutions are expected to do more than the minimum requirements in order to continuously improve on these security measures.

7. **SCOPE** - Each banking institution is expected to have a policy on client interaction. Based on each banking institution's operating environment and circumstances, this policy will impact on the level of security standard required and achieve security within the banking institution's premises.

PART III: IMPLEMENTATION AND SPECIFIC REQUIREMENTS

Each banking institution is expected to have a policy on client interaction. Based on each banking institution's operating environment and circumstances, this policy will impact on the level of security standard required and achieve security within the banking institution's premises.

The following areas should be paid particular attention when it comes to safety and security.

8. **General Banking Hall** - As a minimum required standard practice, there must be security personnel monitoring and observing the main entrance and the movements of people within the banking hall. There must be a monitored CCTV coverage to complement the security personnel. The combination of CCTV coverage and security personnel will provide a higher level of deterrence to criminals. The security guards must be equipped with radio`s or some sort of communication, where possible.

9. **Tellers** - The greatest threat in the Banking Hall is an armed attack on the tellers and customers. Customers can also be taken hostage and used as human shields. To mitigate these threats, transaction windows of a minimum 26 mm handgun bullet resistant glass must be installed in all high risk areas.

Panic buttons and/or hand-held devices must be installed at the desks of selected frontline staff.

10. **Administration Area** - Another threat is an armed attack aimed at accessing the vault, which is usually situated within or from the administration area. Where doorways separate the customer' s area from the administration area, it must be fitted with digital pad or key pad. All future and revamped administration areas should have an installed doorway leading to the administration area, which must contain either a pin-pad mechanism or remote control facility.

11. **ATM** - There are three possible threats to be considered: direct attack on the ATMs; attacks during the replenishment process and attacks on clients using the ATM. Appropriate security measures must be taken into account to mitigate these threats.

    a. **ATM Attack** - The ATM may be forcefully dislodged from its housing or bombed. Cash can be removed at the scene of crime or the complete machine could be taken to another location where cash is removed at the criminals' convenience. All ATM's should have an installed door contact and PIR detector within the ATM room to detect attack from the rear of the ATM.

    b. **ATM Replenishment Attack** - Remote ATM's are more prone to this form of attack. To address this threat, the following must be implemented; varying replenishment times and having armed security presence during the replenishment time. The remote ATM`s must be installed with panic buttons. Where the ATM forms part of a branch, the alarm system should be extended to the ATM room. ATMs should practically be placed in a well-lit public area and preferably housed within a building.

    c. **ATM Card Fraud** - This is one of the greatest security threats at ATMs. It is difficult to prevent card fraud at ATM's because of its spontaneous nature. One form of card cloning technology utilizes a skimming device and a hidden micro camera to capture the card information and PIN number as the client enters it.

       In this regard, all banking industry must put in place the following measures to minimize incidences of ATM card fraud:

i. Privacy shields, where compatible with existing ATM's, to hide the customer's hands from the camera as they enter their PIN number would prevent the camera from capturing the PIN number as well as prevent onlookers from easily noticing the PIN as they are entered. Furthermore, Banks must react, where possible, by modifying the facade of the ATM's and the surrounding walls to make it difficult to attach cameras and to allow for the installation of privacy shields on the number pads. This should be enforced for all future ATM installations.

ii. Regular visual inspections of the ATM by the banks. These inspections should be carried out either as frequently as cash is replenished or as determined by the risk classification of the ATM.

iii. Access and maintenance visits to the ATM should be carefully controlled with audit trails of who has accessed the interior of the machine.

iv. Banking institutions must utilize their existing fraud management and control systems and processes efficiently to monitor trends on individual accounts to spot suspicious ATM withdrawals as far as possible. Banking institutions have fraud monitoring systems in place and should be able to quickly detect irregular ATM withdrawals on customer accounts, which should be verified with the customer.

v. All high risk ATM sites must have daily security personnel on-site from 06h00 in the morning until at least until 12 o'clock (midnight). The security personnel should preferably have access to a hand held or fixed panic button.

12. MEASURES TO MITIGATE ATTACKS

a. **CCTV SYSTEM** - The CCTV system is installed for two purposes, namely; as security management tool and for prosecutorial/evidential purposes.

b. **Cameras** - It is advisable to have fixed CCTV colour cameras positioned in target areas. This must include the Banking Hall (covering entrances, queuing area and tellers' counters), Tellers' booths, cash delivery area (internal and external), staff entrance door (external) and the vault. Other areas which should be considered for coverage are the computer network rooms, the Banking Hall administration area, where possible ATM booths.

c. **Recording Equipment** - Recording equipment must be located in a secure place away from the main target areas.

d. **Monitoring Screens -** Monitoring screens should be located in offices or control room where they will be best utilized for security purposes.

e. **Management of CCTV System -** A CCTV system is only as good as its operators and as it is managed. Only trained and authorized Operators/Administrators must be allowed to use the system. The functionality of the system and the effectiveness of the recording must be checked on a regular basis.

13. IMPORTANT ISSUES TO CONSIDER

a. **Security Alarm Design -** There are two distinct and separate threats, which must be considered in the alarm design, these being burglary and robbery. Burglary is largely a passive threat of theft by illegal entry into a facility and usually after normal operating hours. Robbery is the aggressive threat of a direct attack on a facility, with the use of weapons and usually during operating hours. To mitigate these threats, the following aspects must be taken into account when installing a security alarm.

b. **Control Panels -** Panels should be programmable and incorporate dual remote signal transmission by radio and/or telephone where possible. The panel should allow for sufficient zoning of sensors, so that the area of breach can be identified. It is important that the panel provide for future expansion either through extendable boards or spare capacity. Banking institutions should ensure the utilization of alternative communication protocols.

c. **Dual Transmission -** Dual transmission of the alarm signal to the monitoring station by radio and telephone is a backup system. In the event that one of the transmission devises being incapacitated or faulty, the second devise should ensure that a signal is received by the monitoring station. Dual transmission should be installed, where possible.

d. **Space Detectors -** Detectors should cover all target areas and also the main thoroughfares to those areas. As far as possible, each detector should be individually zoned to minimize exposure to faults.

Dual technology passive infra-red eyes should be installed in high risk areas of the branches. These detectors monitor heat and movement and prevent "screening", where an object is placed directly in front of the detector to blank out its view.

e. **Panic System -** Where possible, recessed panic buttons should be placed at all teller points, counters, and reception desks. Each button should be individually zoned and linked to the main panel. A display panel, which identifies the button that has been activated, should be located for easy reference. Regular training should be provided to all staff on how to handle emergency situations. In particular, staff should be briefed that the member under direct threat should not be responsible for activating a panic button, but rather a person away from the immediate attack.

f. **Monitoring and Reaction Service -** The alarm system must be monitored off-site by a security company with a secure control centre. Where possible, the security company should receive either radio or telephone transmission.

   A physical response to the activation is necessary. In the case of a burglar signal, the security company should be the first to the scene and thereafter report if necessary to the Police or key holders as instructed. On receiving a robbery signal, the security company should first report the activation to the Police who will attend directly to the threat.

   Alarm systems should undergo regular and controlled testing of the system by the banking institution and must be carried out at least every second week.

g. **Cash delivery/ off-loading area -** There are some banking institutions that provide a secure cash delivery/off-loading area for cash consignments. The security company's personnel collecting or dropping consignments should be vetted and pre-authorized to access the off-loading area and they should be clearly identified as the persons authorized to enter. The cash delivery/off-loading areas should only be accessed on a "need to go principle". This area should be access controlled and where possible covered with colour CCTV cameras.

14. **Vaults**

a. **Door Category -** The value of cash being held in a vault will determine the minimum category rating required. This should be confirmed by your relevant insurance consultant. Any dual control key and/or combination mechanism should be installed on vault doors with two key locks where no combinations are fitted. These mechanisms should be used as an overt security tool and preferably a signboard should be placed in the Banking Hall advising the public that the vault is protected by such tools and particularly in areas that holds cash.

b. **Vault keys and/or combinations -** A key and/or combination register should be in place whereby custodians of the keys and/or combinations to the vault should sign off on such key and or combinations. The register should be signed off by the holders as well as persons in a supervisory capacity. Opening and closing of the vault at the commencement and end of each business day should be assigned to at least two different persons who are not residing at the same residential address.
This function should be properly segregated. This register must be checked by management on at least a weekly basis.

c. **After-hours monitoring -** The premises' alarm must be monitored for after-hours opening. A signal should be send to the alarm company if the premises are opened outside of normal operating hours and a reaction crew should attend to identify the person and reason for opening and the Police should be contacted to attend. The security company that is monitoring the alarms system should be informed before hand about employees that are assigned to work overtime.

15. **CLIENT EDUCATION -** The onus lies with each banking institution to educate their clients about the dangers of crime while around their premises. This could be done by way of putting up flyers or posters by the responsible department, namely the marketing department on different practices that are discouraged, for example the use of cellular phones and two-way radios in the banking hall.

a. **Public awareness campaigns -** must be launched through assorted media channels by the industry through Payment Association of Namibia structures. Pamphlets, newspaper articles, radio broadcasts can empower the public to protect themselves from card skimming devices.

The public could then be aware that if their card is swallowed by an ATM they should not just leave it there without first contacting the bank who owns the ATM.

b. **Additionally banks should:**

Display warnings about skimming devices on or near the machine with details of a customer helpline to report incidents.

i. Banks must incorporate internal awareness campaigns for staff.

ii. Banks must ensure that when issuing cards to customers that they are properly informed on the security document, all card limits available and possibly to introduce a dummy ATM at branches to show customers how to use ATM.

16. **ADMINISTRATION** - The Security requirements will be administered by Banking Supervision Department in collaboration with the Banking Services Department.

The Bank of Namibia has adopted the risk based approach in examining the banking institutions. When new branches are opened, the Bank will rely extensively on the internal and external audits' work in order to carry out a review of the risks associated with each functional area of the banking institution as well as an assessment of risk management systems of each functional area. Therefore the examination scope is predefined by the risk ratings allocated.

17. **On-site visits** - Regular on-site visit will be made to assess the application of these guidelines. This will be done by authorized personnel from Bank of Namibia that may include, Bank Examiners as well as Protection Services Personnel.

PART IV: REPEAL

18. **Repeal of Circular BIA 3/09** - This Guideline effectively repeals and replaces Circular BIA 3/09 on Minimum Security Standards for Banking Institutions issued in August 2009.

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