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

BANKING INSTITUTIONS ACT

CIRCULAR – BIA 3/09

TO: ALL BANKING INSTITUTIONS

DATE: 11 AUGUST 2009

MINIMUM SECURITY STANDARDS FOR BANKING INSTITUTIONS

1. ACRONYMS

ATM – Automated Teller Machine
CCTV – Closed Circuit Television
PIR – Passive Infra-Red

2. DEFINITIONS

Anti-bandit door – Attack resistant door for the security of premises where better penetration resistance is a requirement
Seismic detector – A universal application for protection of strong room walls and doors, safes and automatic teller machines.
Door contact – A protective device which monitors the opening and closure of doors and windows.
PIR detector – A passive infra-red detectors – motion detectors using passive infra red (PIR) technology to detect movement of body heat to activate the alarm in the event of an intrusion
Space Detectors – A device that can detect a presence of a human being
Thoroughfares – Path open at both ends

3. Purpose

For the purposes of promoting sound banking practices, the Bank deems it appropriate to prescribe minimum security requirements to banking institutions 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.

This document prescribes the minimum security standards for banking institutions within Namibia which 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.

4. Application

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.

4.1 General Banking Hall

As a minimum required standard practice, there must be armed 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.

4.2 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 58 mm assault rifle resistant glass must be installed. Panic buttons must be installed at all teller points and transaction desks.

4.3 Administration Area

Another threat is an armed attack aimed at accessing the vault, which is usually situated within or from the administration area. Access control and anti-bandit doors should be installed in doorways leading to the administration area.

4.4 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.

4.4.1 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. The main method of protection for this threat is to install a seismic detector on the ATM and connect it to a monitored alarm. The seismic detector will activate with any undue banging on or moving of the ATM. Remote ATM's should have an installed door contact and PIR detector within the ATM room to detect attack from the rear of the ATM.

4.4.2 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 ATM room must be installed with a panic button. The ATM must be installed with a time lock –time delay. ATMs should practically be placed in a well-lit public area and preferably housed within a building.

4.4.3 Client Attack

This is one of the greatest security threats at ATMs. It is difficult to prevent client attack and ATM cards swapping because of its spontaneous nature. It is prescribed that ATM's should be covered by 24 hours CCTV colour cameras, placed in positions to monitor the approach to the ATM, the queuing area and the transacting face. For the after hours period, good lighting must be installed in the area. Should an ATM not be covered by CCTV cameras, then the minimum requirement is a 24 hours armed security personnel on-site. The security personnel should preferably have access to a panic button.

5. MEASURES TO MITIGATE ATTACKS

5.1 CCTV SYSTEM

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

5.2 Cameras

Banking institutions must have fixed CCTV colour cameras positioned in target areas such as the Banking Hall (covering entrances, queuing area and tellers' counters), Tellers' booths, ATM 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 room and the Banking Hall administration area.

5.3 Recording Equipment

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

5.4 Monitoring Screens

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

5.5 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.

5.6 Access Control System

As a minimum required security standard, an access control system must be installed. The system should allow for programming of multiple cardholders. The system must also be able to provide transaction records on all access controlled doors.

5.6.1 Application

When considering access control on a particular door, pedestrian traffic flow through the door and security will dictate the need. Doors which experience high traffic flows usually lead to low risk areas, while high risk areas should have limited access. High risk areas should be accessed on “a need to go principle”.

Banking institutions must conduct regular Security risk assessments and surveys to help them determine their levels of exposures and vulnerabilities. Each Bank must identify as part of their risk analysis the areas, which should have limited access in their banking institution.

The following areas should be considered: the computer network room, doors leading to the vaults, doors in the cash delivery area, treasury offices and doors leading to the administration area from the Banking Hall.

6. IMPORTANT ISSUES TO CONSIDER

6.1 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.

6.2 Control Panels

Panels should be programmable and incorporate dual remote signal transmission by radio and telephone. 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.

6.3 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.

6.4 Space Detectors

6.4.1 Dual technology anti-masking detectors are recommended. 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.

6.4.2 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.

6.5 Panic System

6.5.1 Recessed panic buttons should be placed at all teller points, counters, managers and receptionists desks. Recessed buttons prevent accidental activation by knock or brushing against it.

6.5.2 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 in the manager's office or control room.

6.5.3 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.

6.6 Monitoring and Reaction Service

6.6.1 The alarm system must be monitored off-site by a security company with a secure control centre and which is able to receive both radio and telephone transmissions.

6.6.2 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.

6.6.3 Alarm systems should undergo a physical maintenance check at least every six months. Likewise, regular and controlled testing of the system by the institution must be carried out.

6.7. Cash delivery/ off-loading area

Banking institutions should 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 covered with CCTV colour cameras.

6.8. Vaults

6.8.1 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. Time locks should be installed on vault doors. Electronic time locks, which have the facility to program multiple identity codes and locking times and provide an audit trail for investigation purposes must be installed. Electronic time locks can usually be installed on existing doors. Electronic time locks 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 time lock.

6.8.2 Operating Hours

Electronic time locks should also act as time delay unit during operating hours, opening the vault after a pre-set period of time and only after an authorized code holder has punched in their identity code. This prevents instant access to the vault during working hours. The principle of dual control should be applied when opening the vault and the keys should be secured at all times.

6.8.3 Safety

It is a requirement for safety reasons that an emergency exit, which is opened from the inside of the vault, should be installed when a new bank branch is to be opened.

6.8.4 Vault Keys

A key register should be in place whereby custodians of the keys to the vault should sign for receipt or return of such keys. The register should be signed off by the key 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. This function should be properly segregated. At no time should a single individual be authorized to remove vault keys after hours. The keys must be secured on-site by a security company.

6.8.5 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.

6.9 Home Security

Both key holders to the vault should have security alarms with panic buttons installed in their houses in case of an attack aimed at forcing them to open the Bank premises or in the case of hostage taking.

7. 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.

8. 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.

Regular on-site visit will be made to all banking institutions to ensure that the above requirements are being applied.

9. Effective Date

All banking institutions are required to take note of the effective date for implementing prescribed minimum security standards, which is 1 September 2009.

10. Acknowledgement of receipt

Two additional copies of this circular are enclosed for the use of your banking institution's independent auditors. The attached acknowledgement of receipt should be returned to this Bank as soon as possible, duly completed and signed by both the chief executive officer of the institution and the said auditors.

MICHAEL MAMBO MUKETE
DIRECTOR