بسم الله الرحمن الرحيم

9040701433

مؤسسة النقد العربي السعودي

إدارة التفتيش البنكي — المركز الرئيسي

الرقم : ٤٠٥٧٠ أ ت/٥٢٥ — التاريخ : ٢٣ شعبان ١٤٢٩

المرفقات : مسوده دليل السلامه الامنيه — الموافق : ٢٤/٨/٢٠٠٨م

تعميم

سعادة /

البنك / **المحترم**

بعد التحية:

الموضوع : تحديث دليل السلامة الأمنية

إشارة إلى تعميم المؤسسة رقم ٤٨٥/ م أ /٣٦ وتاريخ ١٤١٦/١/٧هـ والخاص بدليل السلامة الأمنية ، مرفق طيه نسخة من المسودة النهائية لدليل السلامة الأمنية المحدث .

نأمل إبداء مرئياتكم على المسودة خلال شهر من تاريخه .

وتقبلوا تحياتي ،،،،

وكيل المحافظ للشئون الفنية

د.عبد الرحمن بن عبد الله الحميدي

نطاق التوزيع :

جميع البنوك المحلية العاملة في المملكة

١٩٣٦٦

ص.ب ٢٩٩٢ الرياض ١١١٦٩ ، برقياً مركزي ، تلكس ٤٠٤٤٠٠ تلفون ٤٦٦٢٤٤٠ فاكس ٤٦٦٢٨٦٥

SAUDI ARABIAN MONETARY AGENCY

BANKING CONTROL

(SAMA SEAL)

SECURITY AND SAFETY

GUIDELINES

Table of Contents

Amendment and Revision Record

Amendment and Revision Type	Date		

SECTION 1

REQUIREMENTS AND RESPONSIBILITIES

Synopsis

This section describes the general requirements of the Security and Safety Guidelines and the responsibilities of the banks and SAMA.

SAUDI ARABIAN MONETARY AGENCY

HEAD OFFICE

The Governor (Date)

From: Saudi Arabian Monetary Agency – HO Riyadh

To: All Saudi Banks

Attn: Managing Directors / General Managers

Subject: **SAMA Minimum Security and Safety Guidelines in Saudi Banks**

1. Introduction:

Since the last guidelines were introduced in June 1995 (1/1416) a number of major changes have affected the security and safety responsibilities of the Saudi banks to its staff, assets and customers.

A major consideration is the recent increase of criminal activity against Saudi banks in the form of robbery, theft and fraud. Whilst the initial guidelines provided suitable standards and requirements at the time, it was therefore, assessed that these required a detailed review process followed by a revision of the minimum security and safety standards.

The recent criminal activities and the advances in security and safety equipments, systems and procedures has provided an opportunity to implement more effective measures that incorporate international, regional and local standards that would only benefit the Saudi banks.

2. Security and Safety Standards and Requirements:

SAMA has issued the Security and Safety Guidelines that are designed to provide the minimum standards in the following areas:

a. Implementation of a Corporate Security and Safety Plan

b. Standards for the implementation of Electronic Security and Safety Systems

c. Standards for the implementation of Physical Security and Safety Systems

d. Standards for the Cash in Transit procedures and transportation service providers

e. Standards and Procedures for the Security Guards operating in the main buildings and branches

These documents have been prepared using international consultants and reviewed by SAMA and associated government agencies prior to their dissemination to the Saudi Banks.

3. Security and Safety Unit:

Saudi banks are required to appoint a senior and capable individual as a Security and Safety Manager who will be responsible for the design, planning and implementation of the minimum standards contained within the SAMA Security and Safety Guidelines. The Security and Safety Manager is to be provided the necessary personnel and resources to fulfil these obligations and thereby safeguard the staff, assets, customers and business operations of the bank.

4. Implementation Plan:

A detailed Implementation Plan is attached at Appendix 1 to this Circular. The banks are required, within 30 days of the implementation date, to provide a certificate to the agency from an external security consultant that these requirements and standards have been implemented.

5. Effective Date:

With this Circular is attached the final version of the SAMA Security and Safety Guidelines which supersede the previous guidelines and all memorandums and circulars issued prior to this date. The effective date for the implementation of these requirements is **(Date)**.

To ensure regulatory compliance of the implementation of the new requirements, SAMA and the Joint Security Committee will carry out site visits to the banks using appointed representatives. The failure by a bank to meet the requirements and standards could lead to penalties prescribed under the Banking Control Law.

(Name)

Governor

SUMMARY OF RESPONSIBILITIES

SAMA:

To ensure the effective implementation of the Security and Safety Guidelines the following responsibilities are to be undertaken by SAMA:

1. The Guidelines are to be implemented in full by all banks before the 01st July 2009.
2. The Guidelines are to supersede the previous version and any associated amendments, circulars and memos.
3. All matters regarding the Security and Safety of the banks will be coordinated through SAMA. All correspondences, responses and requirements from external organisations, agencies and ministerial departments will be reviewed, assessed and forwarded as formal amendments to all banks.
4. Amendments and updates to the Guidelines will be provided by SAMA electronically and/or hardcopy as applicable.
5. Regular audits of the Guidelines will be carried out by SAMA or its nominated external consultants to ensure compliance and implementation by the banks.
6. Annual audits of the Guidelines will be conducted to ensure the accuracy and validity of its content. The audits will be conducted internally or by its nominated external consultants.

BANKS:

To ensure the effective implementation of the Security and Safety Guidelines the following responsibilities are to be undertaken by the Banks:

1. The Guidelines are to be implemented in full by all banks before the 01st July 2009.
2. The Guidelines have been prepared to provide the minimum security and safety standards for all banks. It is expected, where applicable, that all banks will exceed these requirements and adopt internal standards and specifications dependant upon their structure and organisational needs.
3. The sections within the Guidelines have been designed to work in unison with each other and a clear understanding of its entire content is required.
4. The appointment of identified and capable personnel is to be undertaken to ensure the implementation of the Guidelines and its compliance.
5. All sections within the Guidelines are to be adhered to in full and will include the implementation of any subsequent amendments sent by SAMA.

SECTION 2

CORPORATE SECURITY AND SAFETY PLAN

Synopsis

This section describes the minimum requirements for the establishment and implementation of the Corporate Security and Safety Plan.

TABLE OF CONTENTS

1.0 INTRODUCTION		
The purpose of the Corporate Security and Safety Plan (CSSP) is to provide a single document that incorporates all the procedures and processes to ensure the security and safety of the banks staff, assets and customers. The CSSP is to include the overall security and safety policy of the bank and identify locations requiring dedicated plans and procedures for specific facilities. The CSSP is to include the minimum requirements contained within this section and be prepared, introduced and implemented by the appointed Security and Safety Manager and/or a nominated external consultant.		
2.0 RESPONSIBILITIES		
The CSSP is considered a strategic document that will have an impact on every aspect of the banks business and therefore requires senior management commitment and approval. The CSSP is to include a Corporate Policy Statement that confirms the commitment by the banks senior management and their enforcement of its content. To ensure the successful enforcement of the CSSP the bank is to appoint a Security and Safety Manager and who is provided the necessary assistance and support to carry out his duties and responsibilities. Whilst the CSSP is to be enforced, controlled and managed by the Security and Safety Manager, its preparation and implementation		

can be undertaken and/or assisted by a nominated external consultant. The CSSP is to include the minimum requirements contained within these guidelines and be available for audit and assessment by SAMA and/or its nominated representatives.		
3.0 CORPORATE SECURITY AND SAFETY PLAN REQUIREMENTS		
The Corporate Security and Safety Plan (CSSP) is to include all aspects that would affect the security and safety of the banks' staff, assets and customers. The CSSP is to incorporate the policies, procedures and processes for both general and detailed requirements. Whilst common elements will affect the bank as a whole, the more detailed requirements will need to be prepared for specific facilities. These facilities include: 1. Regional Buildings 2. Branches 3. Cash Holding Facilities 4. Data Centres 5. Disaster Recovery (DR) Sites 6. Warehouses To ensure a complete and consistent approach is incorporated within the preparation of the CSSP the following sections and elements are to be mandatory.		
3.1 INTRODUCTION		
This section of the CSSP will include the following elements: 1. **Purpose and Regulatory Basis** – identifies the standards, regulatory requirements and authority of the		

CSSP. 2. **CSSP Security and Control** – identifies the security of the CSSP and its dissemination within the bank. 3. **Reviews and Audit Requirements** – identifies the frequency of reviews, audits and those responsibly for conducting them. 4. **Reference Documentation** – includes the associated material in the construction of the CSSP and related plans, policies and procedures. 5. **Business Description and Assets** – provides a summary of the banks facilities that are included within the CSSP.		
3.2 INTERNAL SECURITY AND SAFETY ORGANISATION		
This section of the CSSP will include the following elements: 1. **Corporate Policy Statement** – signed policy statement from senior management that provides commitment to the CSSP. 2. **Security and Safety Organisational Chart** – identifies the management and reporting chain of all relevant personnel. 3. **Security and Safety Personnel Responsibilities and Job Descriptions** – provides the requirements of each position and their Key Performance Indicators. 4. **External Agencies and Organisations** – identifies the coordination between the banks' security personnel and		

external groups i.e. Contract Guards, Police, Civil Defence, SAMA etc. 5. **Security Coordination Committee** – identifies personnel responsible for review of the CSSP and any amendments and/or updates. 6. **Conduct and Ethical Practices** – provides the standards expected of the security and safety personnel. 7. **Vendor Management and Tendering Process** – identifies the procedures for tendering and contracting security and safety related equipment, services and systems.		
3.3 SECURITY AND SAFETY TRAINING AND DRILLS		
This section of the CSSP will include the following elements: 1. **Security and Safety Awareness Programmes** – provides the training and education requirements delivered to new and existing staff. 2. **General Security and Safety Training** – identifies internal and external training in security, fire prevention and incident control for the banks' dedicated security and safety personnel. 3. **Specialist Security and Safety Training** – outlines specific training to select personnel that would include Retail Robbery, Anti Money Laundering (AML), Fire Marshalls / Floor Wardens and Emergency Evacuation procedures. 4. **Security and Safety Drills** – include practical tests of the physical and		

electrical security and safety systems, measures and procedures.		
3.4 RECORDS AND DOCUMENTATION		
This section of the CSSP will include the following elements: 1. **Purpose and Requirements** – outlines the files and records required to support the CSSP, provide a centralised reference system and assist in the audit process. 2. **Security and Safety Files:** a. Internal and External CSSP Updates and Amendments b. CSSP Distribution List c. Security Equipment List and Floor Plans d. Safety Equipment List and Floor Plans e. Access Control Card Request and Issue Record f. Master Key and Password Register g. Training Courses and Programmes h. Security and Safety Drills i. Fire Marshalls / Floor Wardens j. Reviews, Inspections, Assessments and Audits k. Incidents, Threats and Breaches of Security l. Service and Maintenance Contracts, Schedules and Reports m. Visitor and Control Room Logs n. Approved Vendor List 3. **Maintenance of Records** – identifies the location and security of the records and files that are to be retained for a minimum of five (5) years from the date of preparation.		
3.5 SECURITY SYSTEMS AND PROCEDURES		

This section of the CSSP will include the following elements: 1. **Security Guards** – include roles, responsibilities and post instructions for the access control of the banks facilities. 2. **Entry Point Screening Procedures** – identifies the procedures for permitting access to a facility for staff, visitors, customers and vehicles. 3. **ID Cards / Access Control Cards** – includes the request, issue, replacement and cancellation procedures for the cards. 4. **Locks and Keys** – identifies the distribution, storage, management and recording of all keys, lock changes and master keys. 5. **Restricted Areas** – identifies and lists the locations considered sensitive, high risk and vulnerable whose loss would severely impact on the business operation and the security and safety of the bank. 6. **Security and Safety Equipment Systems** – includes the operational capability, locations, specifications, standards, testing and maintenance for installed equipment and systems in the following locations: a. Main Buildings b. Branches c. Restricted Areas d. Cash Holding Facilities (Vaults and Safes) e. ATMs f. Data Centres and Back Up Sites g. Disaster Recover (DR) Sites h. Warehouses		

7. **Asset Protection** – identifies the cash and types of valuables held by the bank and the levels of security needed for their protection. 8. **Cash In Transit (CIT)** – provides the internal procedures and processes in the receipt, accounting and delivery of cash and the coordination with external service providers in its transportation. 9. **Communications Systems** – identifies the relevant systems used by the security personnel and the effective management of their use. 10. **Disposal of Sensitive Material** – identifies the procedures for the disposal of sensitive electronic data stored on equipment and confidential documentation. 11. **Clear Desk Policy** – identifies the procedures for the accessibility of confidential documents in individual workspaces.		
3.6 SECURITY AND SAFETY THREATS AND RESPONSES		
This section of the CSSP will include the following elements: 1. **Identification of Threats and Risks** – provides a summary of the main threats and risks concerning the banks staff, assets and customers. 2. **Security and Safety Response Procedures** – provide a detailed list of the main events and the response procedures in mitigating their effects. The following are to be included within the CSSP:		

a. Bomb Threats (vehicle and Package) b. Armed Robbery c. Burglary d. Shooting e. Fire 3. **Travel Security** – identifies the risks and mitigation procedures when travelling as individuals and in groups. Considerations are to include the following: a. Air b. Vehicle (Company and Private) c. Hotels 4. **Search Plans** – provide detailed procedures for searching and checking during routine operations and elevated threat levels. The following are to be included within the CSSP: a. Buildings b. Cars c. Armoured CIT Vehicles and Trucks d. Stores Delivery Vehicles e. Personnel		
3.7 SAFETY SYSTEMS AND PROCEDURES		
This section of the CSSP will include the following elements: 1. **Fire Systems and Equipment** – provide a detailed list of the equipment, function, location, specification and operating capability of the installed systems in each facility. The following are to be included within the CSSP: a. Fire Detection Equipment b. Fire Alarm and Control System		

c. Fire Suppression Equipment and Systems (Sprinklers, Extinguishers and Hose Reels) 2. **Emergency Response Procedures** – provide detailed instructions for personnel in the event of discovering a fire or smoke condition. 3. **Emergency Evacuation Procedures** – provide detailed instructions and plans on the emergency evacuation procedures of a facility. 4. **First Aid** – identifies the personnel trained to deal with First Aid and the equipment they have available to use.		

SECTION 3

ELECTRONIC SECURITY AND SAFETY SYSTEMS

Synopsis

This section describes the minimum requirements and standards for Electronic Security and Safety Systems installed throughout the banks facilities.

TABLE OF CONTENTS

1.0 INTRODUCTION		
The purpose of installing electronic security and safety systems is to enhance the physical measures employed to protect, deter and mitigate the effects of a serious incident and/or criminal activity. No single system in isolation is completely effective, and it is only through their layered approach, physical barriers, manned guarding, effective management and clearly identified procedures and policies can their use be fully maximised to best effect. Due to the variety and availability of internationally recognised standards it is left to the bank and its internal policies and practices to dictate the appropriate standards for such systems. The every increasing availability of systems, equipment and changes / advancements in technology provides an extensive selection of products to choose from. The selection of the appropriate systems and equipment is dependant upon the security and business requirements of the bank. The guidelines contained within this document are designed to provide a minimum requirement that must be met and included for all electronic security and safety system installations.		
2.0 CCTV SURVEILLANCE AND RECORDING SYSTEM		
The use of a CCTV Surveillance and Recording system is an essential element in an effective security and safety screen. The systems main functions within the bank environment are as follows:		

1. Visual deterrence 2. Proactive and preventative surveillance on suspicious activity 3. Identification of individuals 4. Visual evidence in criminal investigations 5. Visual confirmation in the event of an incident 6. Post event analysis The installation and connection of a CCTV surveillance network should consider the integration with related systems such as the Access Control, Intruder, Building Management and Fire Alarm systems.		
2.1 General Requirements and Standards		
To ensure appropriate equipments, systems, services and their security are incorporated throughout the banks facility, the following are considered a minimum requirement for all locations: 1. All installed equipment is to include a one (1) year warranty period as standard. 2. On expiration of the warranty period all equipment is to be serviced and maintained by a qualified, recognised and registered supplier and/or service provider. A minimum schedule should include two (2) visits per year. **CCTV Cameras:** 1. CCTV camera types employed throughout the banks facilities are dependant upon their purpose and can be a mixture of both fixed and dome type. 2. Dependant upon the purpose and requirement of the camera the		

picture/image type can be: a. Black and White b. Colour c. Combination (Day/Night) 3. To ensure the security of the connections and cabling of the cameras all exposed cabling is to be encased in steel tubes no less than 1.5mm thick. 4. **Pinhole Camera** – Minimum Requirements: a. Resolution: 500 TVL b. Lens: 1/3 inch c. Fixed Iris Lens: 3.8mm d. Back Light Compensation (BLC) e. Illumination: 0.1 Lux 5. **Fixed Camera** – Minimum Specification: f. Resolution: 500 TVL g. Lens: 1/3 inch h. Video Motion Detection (VMD) – through DVR i. Auto Iris Lens j. Back Light Compensation (BLC) k. Illumination: 0.1 Lux 6. **PTZ Camera** – Minimum Specifications: a. Resolution: 500 TVL b. Lens: 1/4 inch c. Optical (x22) and Digital (x10) Zoom d. Auto and Manual Focus e. Pan Range: 340 deg f. Tilt Range: 90 deg g. Pan-Tilt Speed: 300 deg / sec h. Back Light Compensation (BLC) i. Illumination: 0.1 Lux		

7. **External Cameras** – Minimum Requirements: a. Positioned to cover all access and entry points for a facility. b. Provide effective picture quality at both day and night. This can be achieved by correct positioning, shielding from the sun, in-built LED lighting and/or external illumination. c. Fully enclosed in a weatherproof and vandal resistant housings. d. Positioned at a minimum height of 2.5m. 8. **Internal Cameras** – Minimum Requirements: a. Provide effective picture quality at both day and night. This can be achieved by correct positioning, built in LED lighting and/or external illumination. b. Positioned at a minimum height of 2.5m and not vulnerable to approach without surveillance. **CCTV Digital Recording System:** The central element of the CCTV surveillance system is the recording medium. To ensure effective management, recording and storage of surveillance material it is to be undertaken in a digital format. The type of system installed is dependant upon the requirements and capability of the bank. Ultimately, this can be either a hardwire system or an IT based solution. 1. The recording equipment is to be secured (as well as its power supply) separately in an enclosed and lockable cabinet / container that is securely fixed.		

2. To ensure the integrity and continuous operation of the recording and surveillance equipment in the event of a power failure a separate battery back up supply is to be incorporated. The use of a UPS system is to have a minimum back up capability of 30 minutes. 3. The location of the recording equipment is essential in maintaining its integrity and in the prevention of tampering. The following options are available for its placement: a. Security Control Room b. Communication Room c. Data Room d. Cash / Operations Officer (if located within the secure Teller Area) **Monitors:** To ensure effective monitoring and viewing of the CCTV surveillance system a 17" screen is to be considered as a minimum for all identified locations.		
2.2 Detailed Requirements – Main Buildings		
The classification for main buildings includes all facilities not separately covered within these guidelines. They include the following types: 1. Head Office Buildings 2. Regional Buildings 3. Data / Computer Centres 4. Disaster Recovery Sites 5. Warehouses To ensure an effective recording period is adopted for all main buildings a minimum storage period of 1 month is to be retained at 6 fps. If recordings for specific incidents and		

events are requested and/or required by the bank these can be transferred to separate hard disk drives and/or writeable discs as required. In addition to the general requirements listed above the following standards are to be considered as minimum requirements for CCTV surveillance and recording systems in all main buildings: **CCTV Cameras – Surveillance Area:** 1. External coverage of all entry and exit points 2. Internal coverage of customer reception areas and staff entrances 3. Internal coverage of entry and exit points 4. Floor access points that include stairwells and elevator lobbies 5. Restricted Areas that require internal surveillance include: a. Data and Computer Rooms (including individual aisles) b. Security Control Rooms **CCTV Digital Recording System:** The operation and storage of the system is to be located in the Security Control Room. For smaller buildings it can be located in a secure area and monitored from the reception and/or the security guard position.		
2.3 Detailed Requirements – Branches and Cash Holding Facilities		
The primary risks and threats facing the banks are against its branch network and cash holding facilities. The geographic diversity and storage of cash / valuables makes them an attractive target for criminal activities. In combination with other related systems the		

CCTV surveillance capability plays an essential role in deterring, recording and monitoring the potential risks. The requirements covered within these guidelines include male, female and combined branches. Where combined branches are concerned they are to have separate recording and monitoring systems and controlled independently of each other. To ensure an effective recording period is adopted for all branches and cash holding areas a minimum storage period of 3 months is to be retained at 6 fps. If recordings for specific incidents and events are requested and/or required by the bank these can be transferred to separate hard disk drives and/or writeable discs as required. If specific recorded data is requested by SAMA a copy is to be retained by the bank for a period of 1 year. In addition to the general requirements listed above the following standards are to be considered as minimum requirements for all branches and cash holding facilities: 1. **Cash In Transit (CIT) Route** – the bank is responsible for the continuous and uninterrupted CCTV recording of cash and valuables once it has arrived at the property until the time it has left the property. This is to include the following: a. External arrival / departure point b. The transit route through the branch or cash holding facility c. Transfer point to bank staff d. Cash Handling Area e. Transfer to Storage Area f. Storage Area (Vault / Safe / Safety Deposit Boxes) g. ATM service room and access door		

2. **CIT Call Point** – at the recognised access point for CIT operations a Call Point is to be fitted (bell / Video Speaker Phone) to alert the Cash Officer and/or Security Guard. 3. **Branch** – in addition to the above requirements the following areas are also to be covered by CCTV cameras: a. **Tellers** – a camera is to be located behind the teller positions and cover a maximum of two (2) teller locations. The camera is to include facial features of the customers and the area around the teller. The coverage of VIP tellers is also to be covered. b. **Entry and Exit Points** – all doors that exit the building are to be monitored internally. These include main, service entrances and emergency exits. Internal stairwells and access points to upper floors are also to be covered. c. **Customer Lines** – a camera is to monitor the customer lines. 4. **Monitors** – the surveillance and monitoring of the installed cameras is to be undertaken by the Cash Officer and nominated representatives. Security guards are only to be provided surveillance of the external areas, public areas and the entry points to the building. Monitors are to be positioned so that the images are not clearly visible to the customers. No more than sixteen (16) images are to be displayed on the monitor at any one time.		
2.4 Detailed Requirements - ATMs		

In addition to, and for the same reasons, the risk and threats facing the branches and cash holding areas, the ATMs are also a potential target for criminal activities. To ensure an effective recording period is adopted for all ATMs a minimum storage period of 3 months is to be retained at 6 fps. If recordings for specific incidents and events are requested and/or required by the bank these can be transferred to separate hard disk drives and/or writeable discs as required. Whilst the ATMs located in the branches are supported by their security system, all ATMs are to incorporate the following minimum requirements: **CCTV Cameras – Surveillance Area:** 1. **External Camera** – to monitor the activity in front of the ATM and include the immediate area around the customer / vehicle. 2. **Internal Camera** – to clearly monitor the facial features of the customer. **CCTV Digital Recording Equipment:** 1. **Branch ATMs** – are to be connected to the branch recording system. 2. **Off Site ATMs** – are to have a separate recording unit or server based system. Sufficient ventilation and cooling is to be available to the installed equipment to ensure effective and continuous operation.		
2.5 Additional Considerations		
In addition to the minimum requirements listed above for the CCTV surveillance and		

recording system the bank could implement a Central Monitoring System (CMS) which is considered preferable by SAMA. The adoption of a CMS will provide a remote monitoring and (possible) recording capability that will enhance the banks ability to respond to incidents and effectively mitigate the potential losses and damage as a result of a serious event that would affect its staff, assets, business and customers. SAMA is currently reviewing this option for kingdom wide implementation with the following considerations: 1. Bank Controlled CMS 2. Police Controlled CMS 3. Privately Controlled CMS		
3.0 ACCESS CONTROL SYSTEM		
An Access Control System is designed to provide a centralised control, management and recording of personnel throughout the banks facilities. To ensure effective security of the banks facilities; its critical assets, and the prevention of unauthorised access a dedicated system is to be employed. Electronic Access Control Systems include the following types: 1. Proximity Cards 2. Biometric 3. Digital Keypads Access Control utilising mechanical locks and keys are included within Section 4 'Physical Security and Safety Systems'. To ensure the integrity and continuous operation of the Readers in the event of a		

power failure a separate battery back up supply is to be incorporated within the reader / controller. The internal battery is to have a minimum back up capability of 30 minutes. Access control systems that utilise controllers are to have a maximum of eight (8) doors controlled from a single unit. The central database for maintaining the record of authorised personnel and the access log is to have a separate automatic / simultaneous back up capability. To ensure effective security, control and recording of specific locations and Restricted Areas, all banks are to implement one (1) of the above systems, mechanical alternatives or a combination of them and retain a log of events for a period of 6 months. **ID Cards:** All staff, contractors and visitors are to be issued and clearly display an ID Card that identifies them whilst in the banks facility. The cards may be incorporated within the Access Control system technology described above or be independently produced. All banks are to ensure an effective system is adopted for the process of requesting, issuing and managing of the ID Cards.		
4.0 INTRUDER ALARM SYSTEMS		
An Intruder Alarm System incorporates a number of different sensors to detect and alarm in the event of unauthorised access or presence. All alarms are to be controlled through a panel and have both local and remote capability. Remote capability may include one		

(1) or a combination of the following options: 1. External and separate Building / Branch / Security Control Room 2. Regional Building 3. Centralised Monitoring Station (CMS) The remote location must have a 24 hour monitoring capability to ensure an effective response. The bank is responsible for the preparation and implementation of effective response procedures in the event of receiving an alarm from any one of the identified systems. The Intruder Alarm panel can either be a separate system or be combined with the Fire Alarm System. The panel is to be located in a secure location and situated within a Restricted Area. Remote keypads for arming / disarming are to be located close to the exit of the area to be alarmed and not in a public area of the building or branch. To ensure the integrity and continuous operation of the Intruder Alarm panel and its sensors / detectors in the event of a power failure a separate battery back up supply is to be incorporated. The use of a UPS system is to have a minimum back up capability of 48 hours. The following sensors / alarms are to be fitted in the locations identified: **Hold Up / Panic Buttons:** These are designed to be activated if the operator / user is being attacked or threatened. The buttons are to be fitted in the following locations: 1. Teller Positions		

2. Cash Officer 3. Cash Handling Area 4. Branch / Operations Manager 5. Vault / Safety Deposit Room 6. Security Guard (Branch) 7. Reception Desk (Main Bulldings) 8. ATMs The buttons can be of double operation and suitably protected and positioned against false activation. **Passive Infra Red (PIR) Sensors:** PIR sensors are designed to detect movement in a given area under their surveillance. Sensors are to be a minimum of dual technology and include enhanced features to minimise false alarms. The sensors are to be fitted in the following locations: 1. Access points to the Teller Area 2. Access route and door to the Vault / Safe / Safety Deposit Room 3. Emergency Exit doors (Ground Floor) 4. Data / Computer Room 5. Disaster Recover (DR) Sites 6. ATM Cabinet 7. ATM Service Room The PIR sensor is to have a visual LED self test capability to demonstrate when movement is detected. This is to be active when in the armed or disarmed mode. **Seismic / Vibration Sensors:** Seismic sensors are used to detect vibrations from all types of attacks through solid structures. The primary purpose of the sensors is to protect and prevent access to the vault, cash holding areas and ATMs. All sensors are to be flush mounted within the floor (where applicable), wall and ceilings and be suitably protected using a protective cover		

to prevent damage and as a trip hazard. Locations to be fitted with seismic sensors are as follows: 1. **Vaults** – to cover all 4 walls, ceilings and floor (where there is a basement) 2. **ATMs** – to be fitted inside the body / cabinet of the unit Additional sensors are to be fitted to walls and ceilings adjoining other commercial or private properties. **Magnetic Door Contacts:** Restricted Areas identified above that do not have Electronic Access Control Systems are to incorporate Magnetic Door Contacts and linked to the Intruder Alarm Panel. Additional locations include all ground floor Emergency Exit doors. Magnetic Door Contacts are to be fitted to the internal side of the door and located at the top open corner. Dependant upon the construction material and design of the door alternative contacts / switches may be used. All doors with Magnetic Contacts are to have effective heavy duty door closures fitted. **Glass Break Detectors:** Glass Break Detectors are to incorporate dual technology that is capable of analyzing both flex (impact) and audio (shattering) frequencies. Prior to the fitting of the sensors the glazed areas are to be checked for their type (sheet / tempered / laminated) to ensure their effectiveness. If the glazed panels have film fitted, are of tempered or laminate type there is no		

requirement for the detectors. Where sheet glass is used it is to be supported by the detectors.		
5.0 FIRE DETECTION, ALARM AND SUPPRESSION SYSTEMS		
The installation of a dedicated, integrated and effective fire detection, alarm and suppression system is critical for the safety of the banks staff, assets, business and customers. The installation of smoke detectors is to be included in all rooms, stairwells, corridors, lift shafts, and public areas of a banks facility. Fixed temperature thermal detectors are to be fitted to all kitchen and tea room facilities. Special attention is to be given to the fitting of thermal detectors within ATMs. To ensure effective identification and response to a potential alarm activation a maximum of 20 detectors are to be registered in each zone if the system is not of the addressable type. Manual Call Points are to be installed next to emergency exits, escape routes and located close to the fire extinguisher and hose reel points. The distance between Manual Call Points should not exceed 30m. On the activation of an alarm an audible ringing is to be heard throughout the entire facility. An audible bell and visual strobe is to be visible from outside the facility. The internal bells are to be rated at 108 dB and external bells at 120 dB. The strobe is to remain active until the system has been reset.		

Both the strobe and bells must be tamper resistant. All cabling is to be fire rated and not run alongside power cables. All banks are to ensure the fire alarm panel has both local and remote capability. Remote capability may include one (1) or a combination of the following options: 1. External and separate Building / Branch / Security Control Room 2. Regional Building 3. Centralised Monitoring Station (CMS) The remote location must have a 24 hour monitoring capability to ensure an effective response. To ensure the integrity and continuous operation of the Fire Panel, detectors and suppression systems in the event of a power failure a separate battery back up supply is to be incorporated. The internal battery is to have a minimum back up capability (under normal load) of 48 hours and then maintain the activation of the alarm for a further 5 minutes. The bank is responsible for the preparation and implementation of effective response procedures in the event of receiving an alarm from the panel. The Fire Alarm panel can be implemented as a separate system or combined along with the Intruder Alarm System. It is to be located in a secure room and remote annunciator panels near personnel operating on a 24 hour shift. All installed equipment is to include a one (1) year warranty period as standard. On expiration of the warranty period all		

equipment is to be serviced and maintained by a qualified, recognised and registered supplier and/or service provider. A minimum schedule should include two (2) visits per year. To ensure the effectiveness and capability of the system, regular internal tests are to be conducted. These tests are to be conducted on a monthly basis and the results recorded. Evacuation procedures and floor plans identifying exit routes are to be prepared and positioned throughout the facility for maximum exposure. All Emergency Exit doors are to be fitted with mechanical push bars / levers to facilitate a quick and easy access and open outwards in the direction of escape (Section 4). To facilitate the safe evacuation process from a building once a fire alarm has activated the recruitment and training of Floor Wardens / Fire Marshalls is to be done from with the banks' staff. Careful selection of individuals and their deputies will ensure all relevant areas are considered and included.		
6.0 LIGHTING		
Internal and external lighting can enhance the security and safety requirements of the bank and assist the surveillance capabilities of the security guards and CCTV surveillance system. Application, placement and types of lighting are to be carefully considered as part of the overall requirements. All CCTV camera locations that do not have built in illumination are to be supported by external lighting.		

All identified Restricted Areas are to maintain constant illumination. All branches are to maintain constant lighting throughout the ground floor. External lighting is to be available for all entry and exit points of a building including emergency exit doors. Emergency lighting incorporating an internal battery back up capability is to be available in the event of a power failure and automatically activate. Emergency lighting is to be fitted in the following locations: 1. Emergency Exit Routes 2. Emergency Exit Doors 3. Fire Extinguisher and Hose Reel Locations 4. Manual Fire Alarm Points 5. Restricted Areas Emergency lighting must be capable of operating for minimum of 3 hours and fitted no less than 2m from ground level. Emergency Exit signs that are not self illuminating and to be covered by the back up system.		
7.0 POWER SUPPLY		
Whilst the main power for the banks facilities will be supplied from the electrical grid there may be occasions where a disruption or power failure is experienced. As identified above, all the main security and safety systems are to incorporate an emergency battery / UPS back up system that will provide sufficient power for a minimum		

of 30 minutes. This is designed to provide sufficient time to secure the premises until normal power is resumed. In critical facilities the use of emergency generators is to be used. The following locations are to incorporate generators: 1. Head Office Buildings 2. Regional Head Office Buildings 3. Data / Computer Buildings 4. Cash Centres / Main Cash Holding Facilities Dependant upon business and bank requirements, additional buildings / facilities may be identified for generator back up.		
8.0 SERVICE AND PREVENTIVE MAINTENANCE		
Once systems have been installed it is essential they are properly serviced and maintained by qualified, approved and experienced service providers. The adoption of a comprehensive service and preventive maintenance contract will mitigate the possibility of system failure in the event of an incident and prolong the life of the equipment. A minimum schedule of three (3) visits is to be conducted for all locations. Locations include main buildings, branches, data and cash centres, ATMs and warehouses.		
8.1 Disposal of Equipment		
To ensure the security of information contained on hard drives, internal memory and recordable mediums an effective disposal procedure is to be adopted. Equipment identified for proper disposal are		

as follows: 1. ATMs 2. Point of Sale Hardware 3. PCs and Laptops 4. Fax Machines 5. CCTV Recording Hardware 6. Servers and Back Up Units 7. CDs and DVDs Disposal is to take the form of electronic (erasing), or physical (destruction), or a combination of both to ensure the data is permanently removed. Clear procedures are to be in place for the disposal of the above equipment/items and coordination between the Security and Safety Manager and the Information Security department is to identify the responsibilities dependant upon the internal processes of the bank.		

SECTION 4

PHYSICAL SECURITY AND SAFETY SYSTEMS

Synopsis

This section describes the minimum requirements and standards for Physical Security and Safety Systems installed throughout the banks facilities.

TABLE OF CONTENTS

1.0 INTRODUCTION		
The purpose of installing physical security and safety systems is to enhance the electronic and procedural measures employed to protect, deter and mitigate the effects of a serious incident and/or criminal activity. No single system in isolation is completely effective, and it is only through their layered approach, physical barriers, manned guarding, effective management and clearly identified procedures and policies can their use be fully maximised to best effect. Due to the variety and availability of internationally recognised standards It is left to the bank and its internal policies and practices to dictate the appropriate standards for such systems. The every increasing availability of, equipment and changes / advancements in technology provides an extensive selection of products to choose from. The selection of the appropriate systems and equipment is dependant upon the security and business requirements of the bank. The guidelines contained within this document are designed to provide a minimum requirement that must be met and included for all physical security and safety system installations.		
2.0 EXTERNAL SECURITY AND SAFETY MEASURES		
The first line of deterrence and protection for any facility is the application of measures to secure the external perimeter.		

The effective use of measures and systems will greatly reduce the risk of criminal elements considering the facility a potential target for their activities and in preventing easy access.		
2.1 Windows and Glass Panels		
The increased use of glass in buildings and branches provide an alternative entry point to the much better protected main entrances. Glass panels provide both a security and a safety risk to a facility, its personnel and customers. The most vulnerable areas are on ground level and those obscured from public sight. To protect and secure these locations the following options are to be installed: 1. **Sheet/Tempered Glass** – is to have security/blast film (min 200 microns) attached to the inner surface and be secured within the frame. A minimum thickness of 10mm is to be used for the glass panels. 2. **Laminate Glass** – does not require additional measures added to the panels. Laminate glass panels are to be capable of multiple attacks and be tested/certified by internationally recognised standards. All ground floor windows/glass panels are to be of clear glass (or maximum 10% tint) and lighting is to be left on during 'out of working' hours to maximise external surveillance. The use of grills and shutters to secure the facility during 'out of hours' can be used but will not reduce the above requirements for the glass panels. Windows and glass panels in upper floors still		

require an element of protection for personnel who may be at risk from flying/broken glass. To ensure the safety of personnel in the upper floors the following options are to be installed: 1. **Sheet Glass** – is to have security/blast film (min 150 microns) attached to the inner surface and be secured within the frame. 2. **Tempered / Laminate Glass** – does not require additional measures added to the panels.		
2.2 Main Entrances		
All bank facilities are to have at least one main entrance that is to be used for its primary access control point. These entrances are to be kept to a minimum to ensure their control of access and surveillance capability. All staff and service entrances are to be treated in the same way. All glass doors are to conform to the above standards (2.1) in the type and protection required. All non-glass doors are to be of solid wood or steel construction and fitted with an eye-hole if an observation window is not available. All access doors to the main entrances are to have a manual locking capability regardless of its primary operating action. Dependant upon the use of the main entrance, the results of a Security Risk Assessment (SRA) and the procedures identified within the Entry Point Screening procedures of the Corporate Security and Safety Plan (CSSP), the following screening equipment may be required: 1. Baggage X-Ray Screener		

2. Archway Metal Detector 3. Hand Held Metal Detectors		
2.3 Emergency Exits		
Emergency exit doors are the primary means of exiting a facility in the event of an incident and should provide unrestricted use from the inside. As these locations are easily accessible from the outside they are to be secured using the following measures: **Internally:** 1. A mechanical push bar/lever is to be fitted to the internal surface. 2. Electronic locking systems are to be on a 'fail open' setting. 3. Magnetic Contact connected to the Intruder Alarm System 4. CCTV Camera 5. An eye-hole. 6. Appropriate exit signage and lighting. **Externally:** 1. Flat door plate with no handle. 2. CCTV Camera and PIR. As part of the fire safety requirements, all routes leading to the emergency exit are to be clear of obstructions and have appropriate signage and lighting to facilitate easy exit.		
2.4 ATM Locations		
In addition to a facilities' cash holding areas the Automated Teller Machines (ATM) are to be considered high risk. The diversity in their locations (Branch, Drive Up, and Stand Alone) and the cash they hold make them an attractive target compared to highly secured locations such as vaults and safes contained within buildings and branches. Only internationally recognised standards and		

providers are to be used in the purchase of ATM units. Whilst the locations are dictated by the bank in conjunction with SAMA and Police approval, there are a number of minimum security requirements and are as follows: 1. All ATM units are to be securely fixed to a solid base using at least four (4) points. 2. All cabling is to be buried/hidden where possible. 3. All exposed cabling is to be contained within a steel conduit. 4. All waste paper containers should only facilitate the use of receipt slips and be self extinguishing. 5. All ATM units are to have external lighting on 24 hour operation. 6. All intruder/fire panels are to have tamper sensors fitted. 7. All ATM cabinets are to have the following security measures: a. Access via high security lock and cylinder or electronic access control. b. Door contact connected to intruder alarm panel. c. Seismic/Vibration Sensor (Section 3) d. PIR connected to the intruder alarm panel (Section 3). e. Hold Up Button (Section 3). f. Smoke and Heat Sensor. g. External alarm bell and strobe. All ATM units are to have CCTV surveillance (Section 3) that is recorded on its own Digital Recording system, or remotely, through the system incorporated within branch it is attached to. All ATM units are to be connected to a remote Central Monitoring Station (CMS) for the		

activation of alarms from any of the fitted sensors.		
3.0 INTERNAL SECURITY AND SAFETY MEASURES		
Should the external security and safety measures be defeated and/or bypassed the internal systems are designed to delay and deter criminal activity as part of a layered methodology. The internal security measures primarily concentrate on the Restricted Areas identified within a facility so that security can be effectively and efficiently focused. **Restricted Areas**: are considered as follows: 1. Vaults, Safes and Safety Deposit Rooms 2. Teller Areas 3. ATM Service Rooms 4. Cash Holding Areas 5. Cash Handling Areas 6. Building Access / Entry Points 7. Security Control Room 8. Data / Computer Rooms 9. IT / Communication Rooms 10. Disaster Recovery (DR) Sites 11. Electrical Rooms Additional locations can utilise either electronic and/or mechanical means to secure their access and include the following: 1. ATM Cabinets 2. Generator Rooms 3. PTT/PABX Room 4. SCECO Switch Room 5. Electrical Rooms All Restricted Area doors are to have effective heavy duty door closures fitted.		

3.1 Mechanical Locks		
Mechanical locks using keys are a standard means of securing doors throughout a facility. In addition to the considered use of an electronic access control system, appropriate mechanical locks can be used in conjunction, or as a replacement, for the security of Restricted Areas (Section 3). To compliment the electronic security and safety measures the physical requirements are as follows: 1. All doors are to be of solid wood or steel construction with same quality material for door frames. 2. All locks/cylinders are to be of high security standard with deadlocking mechanism and resistant to the following: a. Picking b. Drilling c. Overlift and Reading d. Rap and Rake 3. All hinges are to be of steel heavy duty standard with non-rising or removable pins. 4. All doors are to have heavy duty door closures fitted. 5. All doors are to have appropriate security signage for Restricted Areas. Restricted Areas are to be completely sealed outside the main entry points that are secured by the above / or electronic means. All false ceilings, floors, AC vents and other access points are to be considered and secured. All walls are to be of brick/block construction. The other major consideration concerning		

mechanical locks is in the security and control of the keys. As part of the requirements of the Corporate Security and Safety Plan (CSSP) the following is to be established for keys that access Restricted Areas: 1. Log of all keys and the controlling department. 2. Secure storage and issue procedures. 3. Cylinder / Lock / Key replacements. 4. Regular audits / inspections of the keys and issue log. 5. Issue, storage and security of master keys and blanks.		
3.2 Teller Areas		
The teller areas are considered a Restricted Area and incorporate a number of electronic security systems/sensors (Section 3) to protect them during working and silent hours. The main threat against the tellers is a hostile attack from a customer, armed robbery and direct access to the vault, safe and/or cash holding area. In consideration with the electronic systems, security guards and effective procedures that accommodate the main threats, the following options are available for protecting the teller area: **Option 1: Open Cash Drawer** 1. Tempered/Hardened glass (Min 10mm in thickness) is to be fitted to the top of the teller counter and extend for a minimum of 2m in height. 2. Construction below the counter is to be of double brick/block with an external layer steel sheet.		

Option 2: Automated Cash Dispenser 1. An Automated Cash Dispenser is fitted to each teller position. The dispenser is to be securely fixed to the floor using at least 4 points and have the following security measures: a. Mechanical / Electronic access control mechanism. b. Seismic / Vibration sensor (Section 3). 3. Suitable and appropriate signage is to be used to identify the use of Automated Cash Dispensers. The main purpose of the above options is to provide additional delay for the police to respond as well as maximising the protection of the teller personnel, branch staff and customers. As a result of a Security Risk Assessment (SRA) of the branch there may be a requirement to fit tempered/hardened glass to the top of the teller counter for Option 2. This will be dependant upon the risks identified in the area.		
3.3 VAULTS AND SAFES		
The primary storage, security and safekeeping for the majority of cash holdings, valuables and high value documents in a facility are kept in the designated vault and/or safe. **Vault** In addition to the electronic security systems identified in Section 3, the following physical measures are to be incorporated: 1. Vaults are to have walls, floor and ceiling of steel reinforced concrete		

with a minimum thickness of 30cm. 2. Reinforcing is to be in horizontal and vertical staggered rows of 10cm forming a grid pattern using No5 diameter deformed steel bars. A minimum of at least two (2) grid patterns shall be used. 3. The grids are to be in parallel with the face of the walls and secured using beam bolsters, wall ties or upper continuous high chairs and fastened together at the corners. 4. The use of modular panels can be used if materials are rated to provide protection against attack using a cutting torch (oxyacetylene), mechanical and/or electrical tools for a net working time of 60 minutes. 5. The main door is to be constructed of high strength stainless steel with a minimum thickness of 10cm. The door is to provide protection against attack using a cutting torch (oxyacetylene), mechanical and/or electrical tools for a net working time of 60 minutes. 6. A double rotary mechanical combination and key system is to be used for access control of the main door. The keys are to be under dual control of two (2) senior bank/branch officers. Spare keys are to be kept and combinations are to be kept in a neighbouring branch vault. 7. The frame of the main door is to be welded to the walls reinforcing bars and filled with concrete. 8. A steel day gate is to be fitted with two (2) high security cylinders on		

both sides. 9. If an optional emergency door is installed it must conform to the specifications of the main door. 10. An emergency vault ventilator must be provided in the wall or vault door. 11. A telephone is to be fitted inside the vault. 12. All cables connected to the vaults security and safety systems are to be secured and protected within steel conduit.		
Storage Requirements		
The purpose of the below table is to provide a minimum security requirement for the identified amounts of cash and valuables. Where extremely high amounts (in excess of SR 20,000,000) are stored, protection levels and specifications are to be investigated and assessed separately.		

Storage Requirement for Cash and Valuables

Amount / Value (Cash and Valuables)	**Storage Type**			
Over SR 2,000,000	Vault			
SR 500,000 to SR 2,000,000	Safe 'Type A'			
Up to SR 500,000	Safe 'Type B'			

Safes A safe is defined as a free standing, prefabricated secure storage unit whose protection originates in the prefabrication		

and which does not have holes through the protection other than those for locks and cables for anchoring. The safe is to be designed and manufactured to meet stringent international testing authority standards and be approved and/or listed by an international recognised testing laboratory or agency. The safe is to have a dual control mechanism that consist of one (1) of the following: 1. 2 x Combination Locks 2. 2 x Key Locks 3. Combination and Key Lock The safe is to be fire tested and certified to international standards for a resistance of one (1) hour. The safe must be positioned in a Restricted Area will the associated protection and systems identified within these guidelines. **Type A:** The minimum weight for this safe is 750kg (empty) and must be securely anchored to the concrete floor using two (2) internal bolts that is only accessible from inside the safe. All six (6) sides (including the door) must be resistant to a cutting torch (oxyacetylene), mechanical and/or electrical tools for a net working time of 30 minutes. **Type B:** The minimum weight for this safe is 200kg and must be securely anchored to the concrete floor using two (2) internal bolts that is only accessible from inside the safe. All six (6) sides (including the door) must be resistant to a cutting torch (oxyacetylene),		

mechanical and/or electrical tools for a net working time of 15 minutes.		
3.4 Safety Deposit Box Room		
Customer safety deposit boxes are to be contained within a room that incorporates the same requirements and standards as listed above for a vault. The electronic security systems (Section 3) are also those required for this location. Special attention in the fitting of the internal CCTV camera is to be considered to ensure it does not cover the area designated for the customer to inspect its content. All safety deposit boxes are to have dual control high security cylinders.		
3.5 Strong Rooms		
In addition to the use of the above listed vault and safes there may be a requirement to store other sensitive material and documents separately. These items may include the following: 1. Documents classified Confidential and above. 2. Stocks of Cheque Books. 3. Bills, Securities and Guarantees. 4. Official Seals 5. Shares and Bond Documents 6. Spare Master Keys If existing facilities for storage are not available the strong rooms are to have the same requirements designated for the vault. The only differences are as follows: 1. Vaults are to have walls, floor and ceiling of steel reinforced concrete with a minimum thickness of 15cm.		

2. The main door is to be constructed of high strength stainless steel with a minimum thickness of 10cm. The door is to provide protection against attack using a cutting torch (oxyacetylene), mechanical and/or electrical tools for a net working time of 15 minutes.		
3.6 Cabinets		
In addition to the above listed secure storage rooms there may be a requirement to secure and protect other materials. The use of cabinets primarily provides protection against fire and environmental damage. Whilst they do provide a level of security this should be considered limited. All cabinets are to have locks that, if tampered with, will provide visual evidence. **Fire Resistant Cabinets:** The safe is to be fire tested and certified to international standards for a resistance of one (1) hour. The fire resistant cabinets are designed to protect environmentally sensitive items such as: 1. Microfilms and Microfiche 2. Insurance Files 3. Documents classified below Confidential **Steel Cabinets:** The steel cabinets are designed to protect sensitive items such as: 1. Account Documents		

2. Unclassified Mail 3. Specimen Signatures 4. Date, Authority and Signature Stamps 5. Registers 6. Security and Safety Plans		
3.7 Fire Safety Equipment		
The risk of a fire in a facility is potentially greater than any other form of hazard or incident type. The ability to effectively detect and quickly extinguish a fire is critical in minimising the potential damage to life and the assets of the bank. In addition to the electronic safety systems (Section 3) it is the use of automated and hand held fire suppression systems that will ensure an effective response. The positioning, quantity and use of these equipments are available through international standards (eg NFPA), Civil Defence standards and requirements. These should also be clearly identifies within the Corporate Security and Safety Plan along with the identification of responsible personnel, their training on how to use the equipment and in emergency evacuation procedures. The main suppression equipment types are as follows: **Water Sprinkler Systems:** Dependant upon Civil Defence requirements on the locations, standards and specifications the bank is to install an automated water sprinkler system to all underground car parking areas. **Clean Gaseous Systems:** In sensitive electrical locations there is a requirement to minimise the damage to the		

equipment in the event of an automated system activating. This is achieved by using a system such as FM200 (or equivalent) but will require the room to be sealed against air leaks. Due to the non toxic nature of this type of system it is also considered essential in similar areas that are occupied by bank staff and/or contractors. **Fire Extinguishers and Fire Hoses:** A wide range of fire extinguisher types are available (water, powder, chemical) and their positioning will be dependant upon the locations they are designed to protect. The majority of extinguishers will be water based (Class A Fires). Electrical / Computer rooms will require the use of dry powder types (Class C Fires) and positioned accordingly. The minimum capacity for any extinguisher is to be not less than 6kg. Should extinguishers over 10kg be required they should be trolley based. The positioning of fire hoses is to ensure sufficient coverage is achieved between them so that no area cannot be reached or is inaccessible. Emergency water supplies are to be available to support the hoses in the event of a failure of the mains water supply. This can be achieved by reserving a given amount of water in the existing water tanks or by having a separate tank specifically for the fire fighting system. The use of generators (Section 3) will also be required to support the pumps in the event of power loss. Signage is to be located at each position		

where extinguishers and fire hoses are fitted. As a minimum requirement they are to be located in the following areas: 1. Floor lobby areas 2. Emergency Exits 3. Restricted Areas (Fire Extinguishers dependant upon type required)		

SECTION 5

CASH IN TRANSIT – BANK PROCEDURES

Synopsis

This section describes the minimum requirements, procedures and standards for Cash in Transit (CIT) operations for all banks.

TABLE OF CONTENTS

1.0 INTRODUCTION		
The Cash in Transit (CIT) operations currently pose the greatest risk to the banks. It is during the transit and movement of cash and valuables between the secure storage locations that it is most vulnerable. This section describes the internal procedures and requirements of the bank for the movement, handling and safeguarding of cash and valuables. As all banks outsource the CIT function a separate document has been prepared for companies that provide this service. This section is designed to work in coordination and conjunction with the other section requirements outlined within the SAMA Guidelines.		
2.0 DEFINITION OF TERMS		
Cash: Includes both local and foreign currency bank notes and coins. **Valuables:** Includes all negotiable documents and materials such as cheques, bills, bonds and guarantees. This also includes precious stones, metals and customer safety deposit boxes. **CIT Manager:** This person is assigned by the bank and responsible for the internal coordination of the CIT service and is to be assisted by identified personnel for kingdom wide operations.		

Consignor: The person or party involved in the dispatch/sending of the cash or valuables. **Consignee:** The person or party involved in the receipt of the cash or valuables.		
3.0 RECORDS AND DOCUMENTATION		
To ensure the security and safety of the CIT operations the bank is responsible for maintaining and coordinating the necessary documentation for the movement and handling of cash and valuables. The following records and documentation is required: 1. **CIT Operating Schedule** – an operating schedule is to be prepared by the bank or CIT service provider for all transportation, deliveries, pick ups and ATM replenishments. The schedule is to be sent to the police by the end of the previous working day. Copies of the schedule are to be held by the bank and CIT service provider. 2. **CIT Transfer Record** – a transfer record of all cash and valuables is to be maintained by the bank and include the following: a. Names and signatures of carriers, consignees and consignor b. Date and time of transfer c. Cash amount or content of consignment d. Condition of consignment e. Seal numbers f. Departure and destination 3. **Corporate Security and Safety Plan**		

(CSSP) – the CSSP is to include a detailed list of procedures and processes for the internal movement and handling of cash and valuables. These procedures are to be sent to SAMA for verification and approval. Procedures are required for the following: a. Custodians / ATM replenishment teams b. Branches (Vaults / Safes / Safety Deposit Boxes) c. Cash Centres / Holding Areas The bank is responsible for the compliance of these guidelines and may utilise the services of an external security consultant to ensure the CIT requirements are met for all applicable facilities and equipment. The CIT Manager and/or the Security and Safety Manager are responsible for the implementation, coordination and maintenance of the above requirements.		
4.0 TRANSPORTATION REQUIREMENTS		
The external transportation of cash and valuables is primarily undertaken by CIT service providers. The requirements, procedures and regulations for these companies are contained within the separate document 'Cash in Transit Procedures for Transportation Companies'. To ensure the secure and safe movement and handling of cash and valuables, the minimum requirements for banks are as follows: 1. **Canvas Bag Container** – to have a double flap and be capable of attaching a uniquely numbered plastic or metal seal. 2. **Cassette Container** – to be		

constructed of heavy duty plastic or metal and be capable of attaching a uniquely numbered plastic or metal seal. 3. **Self Sealing Container** – to be constructed of thin gauged plastic and be individually coded and/or numbered. The bank is responsible for the coordination, verification and performance of the CIT service provider. Regular assessments of the service providers' procedures are to be conducted by the CIT Manager, Security and Safety Manager and/or external consultant. The transportation of cash and valuables outside the banks property is to be notified to the appointed police contact by the bank or CIT service provider. Should the CIT service provider not be able to deliver a consignment in time the SLA is to clearly identify the procedures for storing and securing it until it can be delivered. The use of the above mentioned CIT Operating Schedule will ensure the police are aware of the routes, locations and activities. Whilst it is preferable to have a police escort and presence during the delivery operations and ATM replenishment it may not be possible due to availability of resources. It is the banks responsibility to ensure they are informed and maintain the CIT schedule they, or the service provider, has established. The CIT Manager is responsible for the coordination of the schedule and that the police are provided sufficient notice.		
5.0 CIT – PREPARATION		
To ensure suitable supervision, accountability		

and security in the preparation of the cash and valuables for transportation, this is to be a dual control operation. A minimum of two (2) bank employees are responsible for the counting, packing and sealing of the bags/containers. Ultimate responsibility is with the following personnel: 1. Cash Officer 2. Chief Cashier / Teller Nominated deputies can undertake this task but must be authorised by the above. Dual control is to be maintained until the transfer has taken place and the CIT Transfer Form has been completed. The Branch Manager or Cash Centre Manager is to coordinate with the above staff to identify the transfer of cash and valuables for the next working day with the CIT service provider. The CIT Manager or representatives are to ensure the CIT Transfer Forms and Records are correctly completed, maintained and securely stored for each location.		
6.0 CIT – DISPATCH		
Once the preparatory phase has been completed the two (2) authorised personnel are to recheck seals and the security of the bags or containers and verify the transporting personnel against their ID cards. On completion and signing of the CIT Delivery Receipt Form the bags or containers are to be handed over to the authorised carriers. The original and a copy of the CIT Transfer Form are to be sent in a sealed envelope to the consignee.		

If cash or valuables are being sent to SAMA an authorised bank employee is to be present during the handover. The authorised employee is to acknowledge the receipt of the consignment from the carriers after checking the bags or containers are securely sealed. The authorised bank employee is then to deposit the consignment, forward the deposit receipt and record the transaction.		
7.0 CIT – RECEIPT		
Only authorised bank employees are to receive the cash and valuables from the carrier along with the CIT Transfer Form. On verifying that the bags or containers are securely sealed the two (2) authorised bank employees are to sign the CIT Delivery Receipt Form. On confirming the contents of the bags or containers are correct and in order, the two (2) authorised bank employees are to sign the CIT Transfer Form. On completion and recording of the checks and receipt of the consignment, a copy of the CIT Transfer Form is to be sent to the consignor. The Cash Officer or Cash Centre Manager is responsible for checking the forms and records in line with the procedures laid down in the CSSP. Cash and valuables being received from SAMA is to follow the above (6.0) requirements.		
8.0 CIT – DISCREPANCIES		
If a discrepancy is identified during the		

preparation, receipt or delivery of cash and valuables the following actions are to be undertaken: 1. **Insecure Bags or Containers** – in the event of tampering, missing seals and/or any other signs of insecurity of the bags or containers they are to be refused unsigned and returned to the carrier immediately for investigation. The authorised checking personnel are to make a report and the following are notified and sent a copy of the report: a. Cash Officer / Cash Centre Manager b. Branch Manager c. CIT Manager / Regional Representative d. Consignor Manager When returned consignor the bag or container is to be checked by the original authorised personnel for verification. In the event of a loss of cash or valuables a report is to be prepared and signed by both the consignor and consignee. 2. **Discrepancy in Cash or Valuables** – in the event of a discrepancy between the CIT Transfer Form and the contents of the bag or container the above actions are to be followed once a confirmation has been made between the Branch Manager / Cash Centre Manager and the consignor regarding the CIT Transfer Form.. All original reports are to be held and maintained by the CIT Manager for safe keeping.		

Dependant upon the nature of the incident and whether it was resolved or not, the CIT Manager may involve the Security and Safety Manager and/or other identified personnel should further investigations be required. Training is to be provided for personnel authorised to conduct these operations that includes the following: 1. Anti Money Laundering (AML) 2. Procedures and processes for the movement of cash and valuables as per the CSSP 3. Procedures in the event of armed robbery and/or criminal acts		
9.0 ATM		
The replenishment and servicing of Automated Teller Machines (ATM) is to be regarded as a CIT operation when the machine cannot be replenished within a secure area. The replenishment operation is to be undertaken by a minimum of two (2) authorised personnel. All replenishment operations are to be conducted in the presence of armed guards. **Lobby ATMs:** Where relevant, all doors and access points to the ATM lobby or replenishment area are to be secured and locked prior to the opening of the ATM. The use of blinds and screens are to be maximised to prevent unnecessary visibility of the replenishment operation. **External ATMs:**		

The replenishment teams will be assisted by the team in the armoured car. The cash containers are to remain in the vehicle until they are required and are as close to the ATM as possible. During the replenishment the armoured car team is to remain vigilant and is responsible for the protection of the team and the cash containers. Dependant upon availability the police may also be present to provide additional security and protection to the replenishment teams and the cash containers. Should the replenishment schedule change from the prepared itinerary this is to be communicated back to the CIT Manager or regional representative. Any changes are to be sent to the nominated contact in the police to ensure their presence during transit and replenishment operations. Police presence is dependant upon availability of resources and CIT operations should maintain their schedule of timings and identified routes. Training is to be provided for personnel authorised to conduct these operations that includes the following: 4. ATM Security and Safety Systems 5. Procedures and processes for the movement of cash and valuables as per the CSSP 6. Procedures in the event of armed robbery and/or criminal acts		

SECTION 6

SECURITY GUARDS FOR MAIN BUILDINGS AND BRANCHES

Synopsis

This section describes the minimum requirements and standards for Security Guards operating throughout the banks Main Buildings and Branches.

TABLE OF CONTENTS

1.0 INTRODUCTION		
In addition to the installation and implementation of other security and safety measures to protect the banks' main buildings and branches, a security guarding service to be used. The purpose of using security guards is to enhance the electronic and procedural measures employed to protect, deter and mitigate the effects of a serious incident and/or criminal activity. No single system in isolation is completely effective, and it is only through their layered approach, physical barriers, manned guarding, effective management and clearly identified procedures and policies can their use be fully maximised to best effect. The guidelines contained within this document are designed to provide a minimum requirement that must be met and included for the use of security guards for the banks main buildings and branches.		
2.0 RESPONSIBILITIES AND REQUIREMENTS		
The security guard(s) is intended to compliment the use of other security and safety systems, measures and equipment. The deployment of security guards throughout the banks main buildings and branches is to be closely monitored and supervised by the service provider and the banks personnel. To ensure sufficient guards are available to carry out their responsibilities, an assessment is to be carried out to identify the quantity		

and requirements. This can be part of the Security Risk Assessment or undertaken as a separate report. The security guards can be contractors or directly employed by the bank. Detailed responsibilities and requirements are to be identified within the Corporate Security and Safety Plan (CSSP) and controlled, monitored and enforced by the Security and Safety Manager. The primary responsibilities of the security guard is as follows: 1. Provide an effective physical and visual deterrent. 2. Provide effective control of access and entry points. 3. Provide an effective response to security and safety incidents. The primary requirements of the security guard is as follows: 1. They are to be a Saudi national. 2. Clearly identifiable and appropriate uniform is to be worn at all times. 3. Maintain the Security Guard Shift Report. 4. Fully trained and prepared for their function and location. All security guard reception/entry locations are to maintain a Shift Report that records all the events and activities for each shift. The security guard/supervisor is to include the following information: 1. Date, time and guard names for each shift changeover. 2. Suspicious activity identified during the shift period. 3. Incidents/Events during the shift period.		

4. Activation of Alarms. 5. Security and Safety equipment check and test. The Security and Safety Manager is to ensure that the information contained within the Security Guard Shift Report is reported, acknowledged and any appropriate action taken. Apart from immediate/emergency actions the report is to be checked and acknowledged at the start of each working day. Prior the changeover between shifts, the oncoming guard is to have physically checked his area of responsibility and acknowledged the content of the previous shift report. All security guard locations are to have detailed Post Instructions that clearly identify their function, responsibilities, incident response and reporting chain. These will form part of the CSSP (Section 2). The effective use of security guards will greatly reduce the risk of criminal elements considering the facility a potential target for their activities and in preventing easy access.		
3.0 ACCESS CONTROL		
One of the primary responsibilities of the security guard is the control of access to the building or branch. To assist in the control and identification of personnel an ID Card system is to be employed by all banks. All security guards are to be aware of the Restricted Areas within their area of responsibility. All buildings and branches are to have 24 hour security guard presence and working hours		

and overtime are to conform to the regulations laid down in the Saudi Labour Laws and are the responsibility of the service provider. The security guards are responsible for the enforcement of a Clear Desk Policy and are to report any infringements within their shift reports.		
3.1 Main Buildings		
To ensure the identity and control of the different personnel working and visiting the building, the following are to be clearly identified: 1. Permanent Employees 2. Contractors 3. Visitors The security guard is to enforce the wearing and prominent display of the issued ID cards by all personnel working and visiting the building. A Building Log Sheet is to be maintained at each reception/access point. The log sheets are to include all personnel (without ID) and visitors that enter the building. The information is to include the following: 1. Name, contact number and date 2. Type of ID used 3. Person Visited / Employee Dept 4. Time in and out Visitors are issued temporary ID cards once the following has been confirmed: 1. Confirmation of visit/appointment by bank employee. 2. Confirmation of visitor by official identification (picture and name).		

Visitors are not to be given access without being escorted by the visited bank employee or a security guard. The bank employee is responsible for their visitor until they are returned to the reception desk and logged out. The bank is to establish clear policies and procedures on the identification, issuance and control of an ID card system. These are to be contained within the CSSP (Section 2).		
3.2 Branches		
To ensure the identity and control of the different personnel working in the branch, the following are to be clearly identified: 1. Permanent Employees 2. Contractors The security guard is to enforce the wearing and prominent display of the issued ID cards by all employees and contractors whilst working in the branch. Customers are only permitted entry during the banks official opening hours. Cash In Transit (CIT) operations are considered a separately and can be found in Section 5. Bank employees are only permitted access to the branch during out of hours if prior permission has been provided by the Branch Manager or his nominated deputy. Access to the branch out of working hours, regardless of permission, is to be visually confirmed by the guard prior to allowing entry. The bank is to establish clear policies and procedures on the identification, issuance and		

control of an ID card system. These are to be contained within the CSSP (Section 2).		
3.3 Cleaning Personnel		
All cleaning personnel are to be escorted and/or supervised whilst working within Restricted Areas during out of hours. This can be undertaken by a bank employee or the security guard dependant upon the policy of the bank. The contract company providing the cleaning services are to issue a list of all personnel, and their duty hours, to the building reception desk or branch security guard. Changes to the names and/or hours are to be confirmed in writing by the nominated supervisor/manager of the service provider.		
4.0 ADDITIONAL CONSIDERATIONS		
Whilst it is mandatory for all buildings and branches to maintain 24 hour security, the installation of a remotely monitored alarm/surveillance capability may be considered for the reduction in security guard numbers and presence. All implemented and/or proposed systems should be prepared in writing and sent direct to SAMA for review and consideration.		