



Independent Policing
Oversight Authority

SECURITY MANUAL

Date: April 2015

Contents

1.0	IMPORTANT USE NOTIFICATION	4
2.0	AMENDMENTS	5
3.0	DEFINITION OF TERMS.....	6
4.0	WARNING	9
5.0	POLICY OVERVIEW	10
6.0	GENERAL SECURITY MEASURES	10
6.1	PERSONNEL SECURITY AND SAFETY	11
7.1	SAFETY AND SECURITY WITHIN IPOA PREMISES.....	12
7.1.4	Security and Safety Training.....	12
7.1.5	Alarms and Mobile Phone Tracking.....	12
7.1.6	Action on Alarm Activating:	13
7.1.7	Personal Tracking.....	13
7.2	CARRYING WEAPONS TO IPOA PREMISES.....	13
7.3	USE OF FORCE AND FIREARMS BY THE AUTHORITY MEMBERS.....	14
7.4	SECURITY AND SAFETY IN THE FIELD	16
8.0	PROPERTY/ASSET PROTECTION	17
8.1	AUTHORITY VEHICLES	17
8.2	PERSONAL PROPERTY.....	18
8.3	PREMISES MANAGEMENT	18
8.4	ACCESS CONTROL	20
8.5	VISITORS/CLIENTS/CUSTOMERS.....	21
8.6	VISITORS PASSES.....	22
8.7	PASS ISSUING PROCEDURE.....	23
8.8	LOST/MISPLACED STAFF PASS.....	24
8.9	FIRE AND ELECTRICAL SAFETY	24
8.10	OFFICE SECURITY AND SAFETY	26
8.11	CASH / VALUABLES AND OTHER EFFECTS	27
8.12	RESIDENCE SECURITY AND SAFETY	28
9.0	INFORMATION SECURITY	29
9.1	PROTECTION OF ICT EQUIPMENT.....	30
9.2	COMPUTER DATA BACK-UP.....	31
9.3	SECURITY OF DOCUMENTS AND COMPUTER RECORDS.....	31
9.4	SECURITY OF INFORMATION CONCERNING SERVICE USERS/CLIENTS	32

9.5	SECURITY OF INFORMATION CONCERNING STAFF.....	32
10.0	MISCELLANEOUS	33
10.1	EMERGENCY PROCEDURES.....	33
10.2	ATTACK ON IPOA PREMISES	34
10.3	BOMB THREATS.....	34
10.4	LETTER BOMBS	36
10.5	KIDNAPPING/HOSTAGE SITUATIONS.....	37
10.6	DEALING WITH PUBLIC DEMONSTRATIONS AT IPOA PREMISES.....	38
10.7	ILLNESS OR INJURY	38
10.8	FIRE EVACUATION PROCEDURES.....	39
10.9	WARNING ON USE OF FIRE EQUIPMENT	41
10.10	ROLL CALL PROCEDURES.....	41
10.11	POWERS OF SEARCH	41
10.12	ARREST AND DETENTION	41
10.13	TRAFFIC ACCIDENT/INCIDENT INVESTIGATION	42

1.0 IMPORTANT USE NOTIFICATION

This security manual is strictly for use by the Independent Policing Oversight Authority (IPOA) and must not be scanned, faxed, e-mailed or photo copied under any circumstances, without the permission of the authority



Peer Bala

2.0 AMENDMENTS

The security manual is a "*living document*". This means that the document will be subjected to regular review as informed by the operational environment. It is the responsibility of all Authority members to ensure that they remain fully conversant with these amendments on a regular basis. All amendments and document changes will be done by the Head of Security Services in liaison with the legal services department, upon the recommendation by management and approval by the Board Risk and Audit committee, in the best interest of the Authority.

3.0 DEFINITION OF TERMS

Access Control: The application of means by which the entry of unauthorized persons or unauthorized vehicles, or both, may be prevented. In simplest terms, it consists of physical and electronic controls and procedures.

Asset: An item of value, these include both movable and immovable assets and even capital.

Attendance Protocol: A system that would account for all employees on any given work day and would see the head of department contact any employee(s) if they fail to show for work by a specific time on working days.

Bomb alert: A status of alert put in place by a competent authority to activate an intervention plan intended to mitigate the possible consequences arising from a communicated threat, anonymous or otherwise, or arising from the discovery of a suspect device or other suspect item in a building, vehicle or any such other facility.

Bomb threat: A communicated threat, anonymous or otherwise, which suggests, or infers, whether true or false that the safety of a building, premise, vehicle, person or any other facility may be in danger from an explosive or other item or device.

Competent Authority: A competent authority is any person, department or organization that has the legally delegated or invested authority, capacity, or power to perform a designated function. Similarly, once an authority is delegated to perform a certain act, only the competent authority is entitled to take accounts therefrom and no one else.

Contingency plan: A proactive plan that includes measures and procedures addressing various threat levels, risk assessments and the associated security measures to be implemented, designed to anticipate and mitigate events as well as prepare all concerned parties having roles and responsibilities in the event of an actual act of unlawful interference. A contingency plan sets forth



incremental security measures that may be elevated as the threat increases. It may be a stand-alone plan or included as part of the Crisis Management Plan.

Espionage: The practice of spying or using spies to obtain information about the plans and activities of a competing company or other secret information by means of spies or illegal monitoring devices. It is sometimes distinguished from the broader category of intelligence gathering by its aggressive nature and its illegality. Counterespionage are efforts directed at detecting and thwarting espionage by others.

Field: An area or setting of practical activity or application outside an office especially as concerns the work of investigators, monitoring and inspection and any such related activities by IPOA members.

Information: Facts or details about a subject. In the context of IPOA it refers to soft and hard copy communications from internal and external sources.

Living Document: A document that is subject to regular enrichment as determined by the changing circumstances and new dynamics and developments within the environment.

Member: Someone or something that belongs to or is a part of a group or an organization. Member as used in IPOA refers to Board members, management and staff of the Authority.

Physical Security: Physical security describes measures that are designed to deny access to unauthorized person(s) from physically accessing a building, facility, resource or stored information and guidance on how to design structures to resist potentially hostile acts.

Sabotage: To destroy or damage something deliberately so that it does not work correctly or to cause the failure of something deliberately.

Safety: The condition of being safe from hurt, injury, or loss. Within the context of IPOA this definition refers to the office, field and residence safety.

Security equipment: Devices of a specialized nature for use, individually or as part of a system, in the prevention or detection of acts of unlawful interference.

Security Restricted Area: Those areas which are identified as priority risk areas where in addition to access control, other security controls are applied. Such areas will normally include Strong room, exhibit store and cash office.

Security survey: An evaluation of security needs including the identification of vulnerabilities which could be exploited to carry out an act of unlawful interference, and the recommendation of corrective actions.

Security: Safeguarding persons, property and information against acts of unlawful interference through a combination of measures of human, material resources and technology within a given location or site.

Silent Hours: This refer to inactive hours and generally covers the weekends, public holidays or during night between from 6:00pm to 6:00am daily.

Subversion: A systematic attempt to undermine a system by persons working secretly from within.

Subvert: To pervert or corrupt by undermining of morals, allegiance, or faith, or generally to create doubt that works against the general good.

Suspect or Unusual Situation: Any situation which in view of the circumstances is not considered to be normal and which is a cause for concern for the safety of persons or property.

Suspicious Behavior: The behavior of any person or persons which, having regard to their manner, demeanor, motivation or actions, gives cause for concern for the safety of other persons or property.

Team: A team is composed of two or more people, also referred to as a group of people who work together for a common goal and purpose.

Weapon: Weapon(s) refer to objects such as knives, guns or any other thing that may be used to intimidate or cause injury or harm.

4.0 WARNING

Divulging information on security practices and procedures relating to the Independent Policing Oversight Authority operations, deliberately or otherwise will be considered as an affront to the code of ethics and a violation to the oath of office and may attract a penalty as guided by the Human Resource Manual and other complementary documents.

 Rose B. B.

5.0 POLICY OVERVIEW

This security manual is designed to operationalize the Independent Policing Oversight Authority security policy. The manual outlines measures to be taken at the individual and departmental levels, and details the specific activities that go towards actualizing the security and safety of IPOA members, assets/property and information. Indeed, security matters cut across every department, neither are they limited to an individual. The sum total of every single individual's effort will yield the kind of environment that IPOA desires to create and operate in. It is true that security is fairly dynamic in nature. This calls for every member to constantly keep abreast with the current trends in the security environment and to remain vigilant at all times while at the work place or office, in the field and their residence. It is only through an informed platform that the members can continuously enrich the security manual to suit the operational environment. Similarly, a sense of patriotism in protecting and owning what is IPOA, will go a long way in ensuring our own security and safety, the security of our assets/property and information. This manual provides parameters to assist IPOA members in their day to day operations and can also be as an Aide Memoir to ensure that everyone working with or visiting IPOA maintains the highest standards of security and safety awareness. All IPOA members must read and fully understand the guidelines provided in this manual and strictly adhere to them.

6.0 GENERAL SECURITY MEASURES

6.0.1 General security measures are hinged on managing the physical environment which entails constant appraisal of one's surroundings to be able to determine, detect and mitigate any emerging risks and threats. The Authority will use diverse measures to manage the physical environment in our area of interest. This will include deployment of early warning resources to evaluate and give indicators of the prevailing situation before our personnel are deployed to such areas. Similar measures will be put in place within the precinct of IPOA premises and in the offices. Security guards from reputable

service providers, barriers, electronic images, intruder alarms and panic buttons will all be used as a proactive means of management of the physical environment.

6.0.2 Resources such as smoke detectors, intruder alarms, vibration sensors and panic buttons will serve as a means of attracting quick response and barring unauthorized persons who may be a threat to IPOA members and assets from gaining access to the premises. Note that our first line of defense is the security service provider. However, the police may be called in for reinforcement in case of overwhelming threat of physical harm to the members or Authority interests.

6.1 PERSONNEL SECURITY AND SAFETY

6.1.1 The security and safety of the Board members, management and staff of IPOA is the single most important obligation of the Authority. It is only when the safety and security of all members is guaranteed, that each one of us can do their utmost in working to achieve our mandate. Towards this end, the Authority will do what is reasonably possible within the means available, to ensure the safety and security of all members, clients and visitors, while within IPOA premises, in the field and during silent hours.

6.1.2 Each individual staff member must always act in a manner as to avoid situations which might compromise their security and safety. The Authority will conduct awareness programs regularly to inform members on security trends in order to empower them to act from an informed platform when the situation demands.

6.1.3 The Authority will also take specific measures including deployment of security guards and use of technology based security systems to enhance the security of members especially while they are at the work place. This will be informed by security risk assessment which will be conducted from time to time, to either downgrade or escalate the security status of each member as determined by the prevailing circumstances.

7.1 SAFETY AND SECURITY WITHIN IPOA PREMISES

7.1.1 The Authority premises is home to every individual member of IPOA. This is where one should feel most secure in order to optimize productivity. Every effort will thus go into ensuring that IPOA premises are safe and secure by initiating measures to educate members on basic security concerns and to generally create an atmosphere where members are confident that their security is a matter of priority to the Authority.

7.1.2 Security Awareness Briefing. Security awareness briefing will be conducted regularly by the department of security to inform the members on possible security and safety challenges at the work place. These will be tailored to ensure that the members are familiar with their working environment and their immediate surroundings and other issues such as work place violence, early detection mechanism and management.

7.1.3 Attendance Protocol. Departments should build teams that will be encouraged to be each other's keeper. In this regard the Authority employees will benefit from an 'attendance protocol' arrangement as determined by each department.

7.1.4 Security and Safety Training. Individuals who have specific security duties will receive appropriate training. Regular security awareness programs in line with the needs of each department will be conducted, to inform and remind individuals of security responsibilities, issues and concerns at the work place. This will particularly target the support staff and drivers who are the first point of conduct or responders in many situations.

7.1.5 Alarms and Mobile Phone Tracking. Panic/duress alarms are fitted at convenient and discreet locations for use by the Authority members to attract attention and get help. The alarms will be activated if there exists reasonable threats to the concerned member.

7.1.6 Action on Alarm Activating:

- The security services department will respond promptly to the first ring. The 2nd ringing will elicit response from the security service provider who will locate and enter the area without delay.
- The security service provider will coordinate with armed police to manage any complex situation.

7.1.7 Personal Tracking. GPS watch, mobile phones and personal tracking devices and real time online tracking is suitable for personal security in case of kidnapping and even the security of children. The supported phones are Nokia, Samsung, Motorola and Sony Ericson.

NOTE: To telephone the individual or location of the panic alarm activation is a violation of procedure and serves no real purpose as the person may be under threat, which will be counter-productive to subsequent security measures.

7.2 CARRYING WEAPONS TO IPOA PREMISES

7.2.1 Clients and visitors to IPOA will not be allowed to access the offices while in possession of a weapon(s). Such items must be deposited with the security officer before the customer/client is attended to. The items so retained will be recorded for accountability purposes and will be returned to the visitor or client upon completion of his/her business at the Authority premises.

7.2.2 All IPOA staff members who possess or are licensed to keep weapons must disclose this fact and avail a copy of the fire arm certificate to the Head of Security.

7.2.3 A staff member who brings his/her personal weapon to IPOA premises, must surrender the weapon(s) to the Head of Security or any other person acting in that capacity, and repossess them only when exiting IPOA premises.



7.2.4 All weapons and ammunitions so surrendered must be kept securely in a safe provided for that purpose.

7.3 USE OF FORCE AND FIREARMS BY THE AUTHORITY MEMBERS

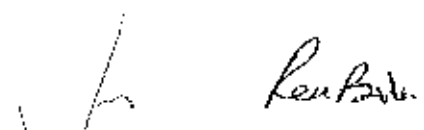
7.3.1 The Independent Policing Oversight Authority recognizes and respects the value and special integrity of all persons and of each and every human life. In particular, IPOA recognizes that the use of physical force (including, without limitation, the use of deadly physical force) by any staff member against another person may constitute a crime or may otherwise give rise to liability for injuries caused thereby, unless the use of physical force (including, without limitation, the use of deadly physical force) is justified by the governing principles of law.

7.3.2 The Authority members involved in various activities, especially investigations, inspection and monitoring teams, and security services may carry personal weapons. It is therefore necessary to have clear restrictions and guidelines regarding the justifiable use of physical force and firearms. The laws guiding the use of firearms should be consulted in connection of the use of force and firearms. These laws are contained in the Firearms Act, Cap 114, which is an Act of Parliament for regulating, licensing and controlling the manufacture, importation, exportation, transportation, sale, repair, storage, possession and use of firearms, ammunition, airguns and destructive devices and for connected purposes.

7.3.3 In this regard, IPOA members may only use firearms or deadly force in self-defense or when he/she reasonably believes the life of another member is under serious danger or threat. In no event must the officer use deadly physical force in the defense of himself or herself or of another if the officer could avoid the necessity of doing so by retreating or escaping with complete safety to the officer and the person whom the officer is defending or IPOA property under threat.

7.3.4 In determining whether or not the use of firearms is justified, IPOA members shall be guided by the following:

- A firearm shall be viewed by an officer only as a defensive weapon.
- Reasonable alternatives to the use of a firearm shall be utilized by an officer before resorting to the use of his or her firearm.
- A firearm shall not be discharged at a threatening animal unless no other reasonable means exists for bringing the animal under control and the animal poses an imminent danger to the safety of the officer or of another person.
- An officer shall not discharge a firearm as a warning.
- An officer shall not discharge a firearm as a signal to summon assistance unless the safety of the officer or of another person is immediately threatened and no other reasonable alternative is available.
- An Officer shall not carry a firearm unless he or she has received training for that firearm in accordance with the applicable policies and he or she is authorized to carry the firearm and the ammunition used therein.
- An officer shall not discharge a firearm at or from a moving vehicle unless the occupants of another vehicle are using deadly physical force by means of an instrumentality other than for which the other vehicle itself and the officer would otherwise be justified in using deadly physical force under the circumstances.
- The safe keeping and security of the fire arm shall be the sole responsibility of each individual member and must always endeavor to ensure that the weapon is not used for any other reason other than for the a foregoing reasons.
- High standards and professional handling of the weapon(s) is expected from each officer. Incidents of accidental discharge will be viewed as gross misconduct on the part of the member and will elicit investigations and appropriate disciplinary action including recommendation for the revocation or cancellation of the firearms license.

A handwritten signature in black ink, appearing to read "Ken B. B.", is located in the bottom right corner of the page.

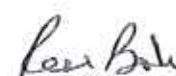
7.4 SECURITY AND SAFETY IN THE FIELD

7.4.1 Security and safety of staff in the field is of paramount importance. Staff members involved in investigations, Inspections and monitoring rely on information that must be obtained from the field. This cannot be possible without deliberate security and safety measures. Hence, movement of IPOA staff to and from the field will be coordinated by respective departments in collaboration with the security services department to ensure that appropriate liaison is done in advance where necessary for security and safety reasons.

7.4.2 A detailed movement plan will be shared with the relevant department for purposes of intervention whenever it becomes necessary. The team leader will be responsible for the security and safety of personnel and equipment and the successful accomplishment of the mission. He will conduct a briefing for the rest of the team members before departure and debrief them after completion of the task. Any issues touching on security will be reported to the department of security, either immediately or within 24 hours upon return to the office, depending on the seriousness of the matter being reported. This will be done through the chain of command or at least the head of the concerned department must be in the know for the sake of coming up with all-inclusive solutions.

7.4.3 The pre-task briefing shall include but not limited to the following:

- Brief overview of the situation.
- Nature of task.
- Conduct of the task.
- Timings.
- Route(s), Distance, Speed and Critical points.
- Possible threats and risks.
- Security of personnel, equipment, information and exhibits.
- Communication.
- Accommodation – where applicable.



- Medical facilities-(First Aid kits, location of health facilities, ambulance services) etc.
- Repair and recovery plans.
- Code words and nicknames for radio communication.
- Standby, rescue or reinforcement arrangements.

8.0 PROPERTY/ASSET PROTECTION

Property/asset protection is important for the successful accomplishment of the Authority tasks. The Authority will strive to ensure that its property and assets are harnessed and utilized for the sole purpose of achieving IPOA mandate. Property and asset protection entails the combined effort of every member of the Authority to ensure that sufficient precautions are taken to minimize damage or loss of property and assets entrusted to them by the Authority for use and benefit of IPOA service consumers.

8.1 AUTHORITY VEHICLES

8.1.1 The individual(s) responsible for overall management of the IPOA vehicles will ensure timely servicing and maintenance of the vehicles, tasking of drivers in liaison with the relevant departments, and must be aware of the location of the vehicles on a 24 hour basis. He/she will ensure effective fuel accountability by individual drivers by logging in mileage as necessary.

8.1.2 Authority vehicles will operate between 6:00am and 6:00pm in line with government policy, unless the situation demands to operate outside these time limitations, in which case the relevant authority will be given.

8.1.3 Details of vehicle movement will be entered into the work ticket and drivers will ensure that they stick to the movement plan and will report any incident or accident involving the Authority vehicles immediately and not later the six hours from the time of occurrence.

Lesi Boko

1/4

8.1.4 The individual responsible for IPOA vehicles will similarly be accountable for all car keys which will be secured under lock and key in a safe provided for that purpose unless the situation demands otherwise.

8.1.5 All vehicles will be parked in the designated areas in the Authority car park and shall only leave with the full knowledge of the section/department responsible.

8.1.6 Any vehicle leaving the parking lot will be booked out by the driver responsible and book in when the vehicle returns to the parking.

8.1.7 The appointed senior driver must conduct inspection of all vehicles every day before they are allocated any tasks and report to the Administration Officer in the event of any challenges.

8.1.8 The administration Officer must ensure that one (1) vehicle with a driver is kept on standby every day or on weekly basis to react to any unforeseen situation.

8.2 PERSONAL PROPERTY

8.2.1 The Authority does not provide insurance cover against loss or damage to personal property of members. This includes private cars whilst parked within IPOA premises or any such other sites. Staff are therefore solely responsible for their own property. In this regard, risk transfer is encouraged. It is advisable not to bring items of value or large amounts of cash to the place of work. Personal effects should be stored in the lockers or cupboards provided.

8.2.2 The department of security will ensure that a reasonably secure environment prevails for service user's property. However, IPOA does not take responsibility for loss or damage of service user's valuables and personal effects while within the Authority's premises.

8.3 PREMISES MANAGEMENT

8.3.1 The ACK Garden Annex which houses several other organizations. This means that individual organizations will operationalize independent security



Leslie Bala

measures up until a collective approach to security in the building is established. In this regard, IPOA has establish a system for opening and closing its office block which is being implemented by the administration officer and heads of departments. At the end of a working day, staff must ensure that doors and windows are securely locked and that any fitted security equipment (intruder alarm, CCTV, motion or vibration detectors) are activated. All staff will refer to the locking up and opening procedure developed by line managers as part of the security risk management. Staff must NOT tamper with, or alter in any way, equipment or other measures designed to enhance security.

8.3.2 Following an incident and subsequent investigation, if it is determined that a breach of physical security was a direct result of staff failing in their duty to ensure the integrity of the premises, or assets/property of the Authority, the Authority may consider taking action against any identified member of staff.

8.3.3 Any potential breaches in physical security should be reported immediately to the head of security through a tool provided for monitoring security trends within IPOA premises and in any other location. Repairs or maintenance to restore physical integrity as each case demands must be carried out as soon as possible. This will be done through established procurement channels.

8.3.4 The Department of Security Services will carry out regular crime reduction survey for the premises together with the security service provider, to highlight security gaps that will inform subsequent action or direction from the CEO/Board. The crime reduction survey will be conducted annually using either internal or outsourced resources.

8.3.5 All directorates/departments are to ensure that security is fully integrated early in the process of planning, selecting, designing and modifying facilities. They are required to:



Rosa Bello

- Select, design and modify their facilities in order to facilitate the control of access.
- Demarcate restricted access areas, and have the necessary entry barriers, security systems and equipment based on threat and risk levels.
- Include the necessary security specifications in planning and tender documentation and incorporate related costs in funding requirements.

8.3.6 Departments to ensure the secure storage, transmittal and disposal of classified and protected information in all forms, in accordance with the requirements of information and physical security standards.

8.4 ACCESS CONTROL

8.4.1 Access control is the single most important aspect of physical security. This calls for briefing of members on the access privileges and prohibitions. Similarly, clients, visitors/customers, contractors and service providers must not be allowed access out of their area of concern. Even then, such persons will have to be escorted or supervised by IPOA staff while they remain in the premises. Security guards, physical barriers, technology and specified procedures will be applied in controlling access to IPOA premises.

8.4.2 Entry and exit points to offices in the building will be controlled electronically. All Authority members will be registered or programmed to electronically open and close access doors. The access cards remain the property of IPOA and must be surrendered on request.

8.4.3 Apart from finger prints, security access cards to IPOA premises must be kept secure, and if stolen, lost or damaged or compromised, it should be reported immediately to the head of security services for appropriate action.

8.4.4 Consultants, auditors and other short-term visitors shall receive security access with restricted access for their needs. Such access must be approved by the head of security services.

8.5 VISITORS/CLIENTS/CUSTOMERS

8.5.1 The Authority in its peculiar role as a public service provider will host persons from different backgrounds, color and race. Clients, visitors or customers will be received, frisked and ushered to the reception by the security guards. Once at the reception, the staff concerned will be informed of the presence of the visitor/client and will be responsible for the movement of the visitor/client until he/she completes her/his business in the premises. Visitors/clients must not be left to find their own way around the premises but will be guided until you are certain that it is safe to leave them, ideally at the reception or once they exit the entrance. Always ensure that having let them in, that they also leave the premises.

8.5.2 Visitors will be booked in the visitors register by the security personnel on production of their identification document(s). A visitor will not be allowed to make entries or book himself or herself in the visitors register. Where applicable they should also sign the visitor's book as shall be guided by the relevant IPOA staff.

8.5.3 The staff being visited will be prompted by the receptionist to pick their visitors from the reception on second floor. Visitors will be given visitors cards in exchange with their personal identification document(s) which will be used while such a visitor is in IPOA premises and must be surrendered upon departure or in exchange of his/her identification documents. Under no circumstances are visitors to be allowed access without the appropriate clearance being granted from the intended host.

8.5.4 Visitors of suspicious character or whose intention is unknown will be handed over to the department of security services who shall determine the next course of action.

8.5.4 The procedure for processing a visitor is as follows:

- Visitor enters the designated entry point.
- The security guard welcomes the visitor/client in a compassionate way, inquires the purpose of the visit, and once satisfied the visitor/client is in the right place, he or she explains the procedure of gaining entry to the Authority offices, part of which requires that the visitor or client be frisked.
- The security guard frisks the visitor/client and request the visitor to provide the officer with identification document(s) e.g. National identity card or passport.
- The officer records the visitor's particulars in the visitors log/database and guides the visitor to the reception for further assistance.
- The visitor is issued with a visitors permit in exchange with his/her identification documents and allowed access accompanied by the intended host.

8.5.5 The procedures for processing a visitor after the visit has been completed is as follows:

- The visitor/client is escorted back to the reception by the host.
- The visitor returns the visitors pass and is given back his/her identification document(s) by the security guards who record the time handing in the visitors pass and leaving the IPOA premises.

8.6 VISITORS PASSES

8.6.1 All visitors to IPOA are required to hand in their identification documents for a visitor's pass issued at the security desk or reception. A number of passes will be available to suit the status of the individual(s) as follows:

- 'T' - Temporary pass to be issued to persons who require access for a short period.

- 'V' - Visitors Pass to be issued to those persons who are not employees and do not warrant VIP status but need to conduct a visit to a particular person.
- 'CT' - Client Pass to be issued to those persons who come to IPOA premises either to make a complaint, interview or when under investigations.
- 'C' - Contractor Pass to be issued to those persons who are undertaking work in the premises.
- 'VIP' - Very Important Person Pass to be issued to those persons who, by virtue of their status warrant the issue of the said pass. Special arrangements will be made by the relevant department for the reception of such persons.

8.7 PASS ISSUING PROCEDURE

8.7.1 Specific instructions on the procedure of issuing passes have been given to the security guards and the reception. The visitors registers/database have been provided at the entrance to IPOA premises to record among others, the Name of visitor, member being visited, Company, Time in/out, Type and pass number issued.

8.7.2 The visitor(s) must display the pass clearly at all times while in IPOA premises. The visitor must be picked from the reception by the member of staff responsible, who will also ensure the visitor's Pass has been surrendered before being given his/her Identification documents. Loss of a visitors Pass should be notified to the security services department immediately before the visitor is handed his/her identification documents and the loss recorded in occurrence book (OB). It will be made clear at the point of issue of the visitor's pass that loss or misplacement of the same may attract a penalty.

8.8 LOST/MISPLACED STAFF PASS

Should an employee lose/misplace a staff pass, the employee is to be issued with a 'T' or temporary staff pass until his/her Pass is located or a new card issued. In the event that the Pass is lost, this must be reported immediately to the head of security services explaining the circumstances under which the loss occurred. The affected member will further report to the police and obtain a police abstract to that effect. Investigations into the loss and appropriate recommendations will be conducted to establish culpability and appropriate disciplinary action taken where necessary.

8.9 FIRE AND ELECTRICAL SAFETY

8.9.1 Measures and procedures put in place for fire and electrical safety to safeguard The Authority members, clients/visitors and property should be adhered to. Common sense precautions concerning fire and electrical safety must be observed at all times.

8.9.2 Although fire extinguishers and hose reels are available within the Authority premises, fire can spread rapidly. Key elements for action by first responders include:

- Sounding the internal alarm bells and summoning the fire brigade and police.
- Ensuring that personnel are evacuated safely.
- Ensuring that the emergency doors remain open up until the premises is fully evacuated.
- Where safe to do so, attempt to put the fire out using available firefighting equipment.
- Ensuring that the Authority property is not unlawfully removed during evacuation.
- Ensuring that neither fire fighters nor police unlawfully remove any property during the freedom of movement given to them.



8.9.3 All persons within the Authority premises will be directed to the marshalling/assembly point located at the car park by appointed fire marshals

8.9.4 Minimum general guidelines for fire and electrical safety include:

- **Fire extinguishers:** Installation and regular inspection of fire extinguishers useful for all possible fires at convenient locations in IPOA premises, residences and in vehicles. All members should be aware of the location of fire extinguishers and fire alarm if present in offices, residences and hotels.
- **Regular physical checks of firefighting equipment** will be conducted by the security services department in liaison with the building administrator to ascertain their serviceability. The Department of security will ensure that:
 - Fire extinguishers and hose reels are in place and in good condition.
 - No obstructions prevent access to all appliances.
 - All extinguishers are fitted on their brackets on the wall.
 - Seals are intact and the extinguisher shows no sign of being discharged.
 - Hose reels are in full working order by discharging a small amount of water into a bucket.
 - Signage, clearly identifying the presence of the fire appliance, is in place.
 - The date of the next due inspection should be noted and filled in on the report.
- **Emergency/Fire exits:** Always take note of fire exits and plan ahead on how to exit the office, residence or hotel room in case of fire outbreak. Some windows may be designated as emergency and fire exits.
- **Smoking areas:** The Authority premise is a **NO** Smoking area. Smoking by staff members, clients or visitors will only be allowed at the designated

smoking areas outside the building. Cigarette remains must be disposed of properly.

- **Electrical safety:** Regular inspections of offices and residences shall be conducted to mitigate any danger that would arise. Electrical cutout or main switch for the premises and offices including residences should be known or be clearly marked, be free from any obstruction and never be in a locked space. Note; everyone should know the location of the main switch.
- **Tamper resistant smoke detectors** will be placed where there is cooking or a heat source (lounges with microwaves, coffee pots, kitchens, etc.) and by the main electrical circuit box.
- **All employees are encouraged to acquaint themselves with the fire orders** and evacuation guidelines provided by the Authority for ease of compliance during planned fire drills and in the event of actual need for evacuation.

8.10 OFFICE SECURITY AND SAFETY

8.10.1 Office and Stores Keys. Every staff member that has an office will be issued with one key. Support staff responsible for cleaning the offices or supervising cleaners will keep one key for each office. These keys must always be kept in a safe, preferably in the Administration Officer's office or any other designated area in IPOA premises, and must never be taken away from the premises. Keys to sensitive stores including the strong room/armoury must be kept by the person responsible for each store. All spare keys will be kept by the admin officer.

- The opening of the Strong room and exhibit store may only occur if there are two persons in attendance. There are to be no exceptions to this rule.
- Duplicate keys shall not be made without permission and a record of who has each duplicate key kept. If a key is lost under suspicious circumstances, appropriate investigations shall be carried out but in the meantime, a new lock shall be fitted. Keys to the strong room and other

Lee Bok

1

stores shall not be duplicated except with the authority of the Head of Security.

8.10.2 Doors: The Authority premises has several entrances and exits. However, access to the offices will be limited to one entrance only on 2nd floor, through the reception, and two entrances on 3rd floor. Staff members will access their offices through designated entrances. All visitors and clients will report to 2nd floor where they will be guided by the security guards and receptionist accordingly. All fire exits will remain closed at all times unless the situation demands otherwise. Main entrance doors shall be fitted with intruder alarms to reinforce the biometric locking system. Fire exits/escape doors will be fitted with "deadlocks" which can only be opened from inside the building, in addition to intruder alarm system and grills. Sensitive areas such as the strong room, exhibit store, forensic laboratory and server room shall be fitted with the right description of doors in addition to vibration sensors and door alarm system.

8.10.3 Windows. Windows on sensitive offices, must be fitted with bars/grills to deter unwanted entry but must not jeopardize emergency and fire exits. Windows designated for emergency exit shall have working locks on them with keys kept nearby in an easily accessed and well-marked location.

8.10.4 Clear Desk Policy. Clear desk policy entails that all members will at all times ensure that there are no documents left on their table or work station unattended. Similarly every member must endeavour to fully understand the dynamics of the work place to the extent that any interference is noticed at the first instance. This calls for each member to survey their environment carefully securing all items that need to be kept away at the end of a working day, and beginning the next day by ensuring that every item is intact.

8.11 CASH / VALUABLES AND OTHER EFFECTS

8.11.1 Cash is an attractive item which must be kept under lock and key at all times. The accounts department is discouraged from holding excess cash in their office since this could easily be a recipe for break in. Similarly, cash in transit must always have police escort. This will be arranged by the security

Ree Bode *1/10*

services department whenever necessary. The department must ensure that all cash, other financial instruments and accounting records are kept secure at all times. Invoices and expense claims must be supported by appropriate documentation to prevent fraud. During silent hours, a clean desk policy must be adopted to prevent unauthorised access to sensitive information, whether of a financial or commercial nature. To augment the security measures, the accounting staff will be facilitated to control entry to the accounting office during working hours by installing door opening system which can only be operated by the office occupants.

8.11.2 Losses and Damage. Staff members must take all reasonable precautions to ensure that losses or damage are not incurred by the Authority for cash, valuables and other effects (computers, iPad, cell phones, and furniture) and similar other items entrusted to the members by the Authority for safe custody and use. In this regard, each member must demonstrate ownership by endorsing relevant forms for whatever item(s) that are put under their custody for their use. Accordingly, any damage to the Authority property will be investigated by the security services department and appropriate recommendations made to make good any such damage or loss.

8.11.2 Care of property is essential for financial viability as constant replacements are expensive and untoward use is not covered by insurance.

8.11.3 Asset tagging of valuable and attractive items such as televisions, video recorders, computers, projectors etc., should be enforced by the procurement department for ease of identification in the event of loss.

8.11.4 Loss or damage of any property must be reported immediately to the department of security services and the due process will then follow.

8.12 RESIDENCE SECURITY AND SAFETY

5.12.1 The safety and security of one's residence begins as early as when the building is being designed. The need for certain safeguards should be factored in at this stage. The need for fire escape; the location of the gas cylinder either



to be outside the house or face the outer wall are some of the precautions that must be considered at this early stage. However, security and safety can also be enhanced by making sure that basic measures such as ensuring the availability of fire extinguishers and training all family members, including the key users (house help) on the use of electrical appliances and the inherent dangers, is critical to security and safety at the residence.

8.12.2 Residence Locks and Keys: It is important that good quality locks are used to ensure that they cannot be easily broken or opened by other keys. Always ensure that once the doors are securely locked, the keys are removed and kept centrally in the inner house for ease of exit whenever necessary.

8.12.3 Domestic Workers: Domestic workers are basically strangers who one may ordinarily not require in their tight families. However, by virtue of their services, they become part of the family. It is critical that a thorough background check is carried out before hiring domestic workers. This must include vetting through the assistance of reputable private service providers and facilitation of a certificate of good conduct, if the would be employee is off age. Note that it is an offence in the laws of Kenya to hire under age persons to perform house chores

8.12.4 Safety of Children. The safety of children especially toddlers is critical when left under the care of a domestic worker or house help. In 99% of the cases, a house help rarely gets enough time to pay attention to the toddler considering the enormity of the house chores that they must accomplish every day. Safety therefore starts by ensuring that, any harmful substance(s) such as drugs, oils, etc. are safely locked away. Hanging cables are also dangerous and must be out of reach of children.

9.0 INFORMATION SECURITY

9.0.1 The Independent Policing Oversight Authority is an information, communication and technology (ICT) driven organization. Information systems

must be secured against rapidly evolving threats that have the potential to impact their confidentiality, integrity, availability, intended use and value. To defend against these threats, an ICT security strategy that accommodates changes in threat conditions, which may be sudden, and supports the continuous delivery of services will be put in place by ICT department to mitigate any scenario that may prejudice the Authority operations. Similarly, it must be recognized from the onset that all information to the Authority is meant for the strict consumption of IPOA and under no circumstances will such information be disseminated to any other source for whatever reason unless duly authorized through the due process. Violation of this requirement will be viewed as a serious affront and a threat to the core values of the Authority.

9.0.2 The Independent Policing Oversight Authority Board and staff are expected to comply with all policies and procedures that explain how to manage confidentiality and security issues relating to paper and electronic information and telephone technology.

9.0.3 To prevent the compromise of ICT systems, departments must implement security controls articulated by the ICT department and any additional controls identified through a threat and risk assessment.

9.1 PROTECTION OF ICT EQUIPMENT

The following precautions will be taken to protect communication Equipment:

9.1.1 Avoid carrying or storing laptops in obvious computer carrier case. Considerations should be made to have padded laptop protector and placing it into a backpack or other generic carrier case.

9.1.2 Consider purchasing foam-lined cases that protect and disguise expensive equipment. If the equipment is often transported by vehicle, consider purchasing local storage containers commonly used for tools or spare parts. This makes them less attractive targets and protect them from damage.

9.1.3 Keep a low profile when using communication equipment. Discrete use limits the chances of thieves targeting the equipment.

9.1.4 When storing portable communication equipment (GPS, laptops, etc.) in the office/store, ensure it is kept in a secure area or container. Designate someone to verify its presence each day.

9.1.5 Concerned departments are to implement an effective accountability procedure if equipment is pooled for checkout. This may include signing for the equipment by individual or team users.

9.2 COMPUTER DATA BACK-UP

9.2.1 Routine computer file backup will be undertaken to prevent loss of critical historical data if the computers are damaged by fire or stolen.

9.2.2 Routine backup will be undertaken automatically, ideally on weekly basis. ICT department will design a way of managing this activity, preferably in the data backup policy.

9.3 SECURITY OF DOCUMENTS AND COMPUTER RECORDS

9.3.1 Financial and personnel records should be shredded before discarding. Personnel files and records should be kept in a secure location with restricted access.

9.3.2 Passwords and other computer-based security measures should be enforced to prevent unauthorized access.

9.3.3 Clearly laid down guidelines on handling of documents especially hard copies should be issued by HR to all concerned departments for ease of monitoring the movement of such documents.

9.3.4 Photocopying of documents and or copying of data on personal flash disks will only be done with permission or knowledge of the relevant department.

9.4 SECURITY OF INFORMATION CONCERNING SERVICE USERS/CLIENTS

9.4.1 A service user has the right to expect that information given in confidence will be used only for the purpose for which it was given and will not be released to any other person or entity without their consent, except in extreme circumstances in order to protect others from the risk of significant harm.

9.4.2 Staff must recognize the fundamental right of the service users to have information about them held in secure and private storage but without violating the fundamental freedoms and right to information as provided in the constitution.

9.5 SECURITY OF INFORMATION CONCERNING STAFF

9.5.1 Staff information must be kept in secure cabinets, this includes supervision records. Access to information concerning staff is on a "need to know" basis to which only nominated administrative and financial staff have access. Permission to receive information from personnel or payroll files other than nominated staff must first be obtained from the person in charge of the records through the due process.

9.5.2 Request for information. To ensure that staff are confident that their personal information is secure, any requests by third parties for staff personal information must be authorized in writing by the member of staff concerned before the information is released. In addition, queries for personal details should be placed in writing prior to any information being divulged over the telephone.

9.5.3 Disposal of Litter. Disposal of litter is critical to the Authority. Information on the Authority can be leaked through improper disposal of litter. Also, disposal of litter can serve as a conduit to pilfer items and materials unnoticed. Therefore all litter generated from the Authority premises will be checked by the security guards before being disposed off. The administration officer will also appoint a permanent staff to check the litter from time to time to compliment

Lee Bob

1

checks by the security personnel. Similarly loose documents due for disposal will be shredded before they are disposed off.

10.0 MISCELLANEOUS

10.0.1 Reporting of Incidents. All incidents that have implications on the security and safety of IPOA members, clients/customers, property/assets and information must be reported promptly to the head of security. In all cases the security services department will investigate and make appropriate recommendations on all incidents of serious nature.

10.0.2 Crisis Management Plans. Each department will formulate crisis management plans. Such plans will cover ICT crisis as well as those of a criminal nature to complement guidelines given in this manual.

10.0.3 Behavioral Emergencies. In instances where a client/visitor becomes uncontrollable by ordinary means, the security guards will be called in to arrest the situation and shall have the powers to restrain or prevent the subject from causing harm or injury to himself/herself or others. In the event that such behavior is as a result of a medical condition, the security officers will render first aid care, until the person concerned stabilizes or he/she is turned over for proper medical care. In case of an unruly client/visitor, the subject will be promptly handed over to the police. Depending on the situation, the services of counselors may also be necessary.

10.1 EMERGENCY PROCEDURES

10.1.1 Possible scenarios include:

- Attack on premises
- Bomb threat
- Kidnap/hostage situation
- Dealing with public demonstrations at IPOA premises
- Fire
- Illness or Injury

10.1.2 The primary task of Security officers in an emergency is to assume a leading role in protecting the Authority members and property if the situation allows. The nearest police station or post must be alerted without delay and emergency alarm buttons activated to send an immediate signal to the security service provider. If time permits, the head of security should be consulted before activating the emergency alarm so that all available information can be passed to enable security service providers and the police to deploy an appropriate response.

10.2 ATTACK ON IPOA PREMISES

10.2.1 In the event of an attack on IPOA premises, by an armed intruder, depending on the time of the incident, the security service provider will be alerted immediately, who together with the police will react to the situation. Similarly, the Head of Security will work out an arrangement with the nearest police station to respond to any such situation when an alarm is raised.

10.2.2 Initial response would be immediate by the security service provider's alarm response team located within the vicinity of IPOA premises, and the police from Capitol Hill Police Station or Kilimani Police Station as shall be determined by the prevailing circumstances.

10.3 BOMB THREATS

10.3.1 Chances of a bomb threat to the Authority premises by disgruntled or well organized syndicates cannot be dismissed. Bomb threats are to be taken seriously. During working hours the decision to evacuate the Authority premises will be made by a competent authority. When a threat is received, the concerned member should keep the caller talking for as long as possible. This is fundamental to tracing the call, identifying both the caller and reasons for it. Should the need to evacuate the premises become necessary, it is of paramount importance that order prevails to avoid accruing injury and collateral damage due to panic. Hence, the designated point persons or Fire Marshall will guide the rest of the members on the exits to use bearing in mind

that the closest exit points will be preferred. In such situations, lifts will not be used.

10.3.2 Action on Receipt of a Bomb Threat. Any Member of IPOA receiving a bomb threat must report the matter to the security department immediately. If the threat is in form of written material, envelope or container, further unnecessary handling must be avoided. All possible effort must be made to retain evidence such as fingerprints, handwriting, postal marks, etc. that may help in identifying the writer. If the threat is by telephone, the following actions should be taken:

- Discreetly, though urgently getting a colleague to inform the Head of security, or any other officer around, the Police and security service provider.
- Letting the caller finish without interruption, then asking for the whole message to be repeated so that the main points can be written down to prevent any mistake.
- Establishing exactly what the device is, where it has been placed and when it is primed to explode. If the caller does not indicate the location of the bomb or time of possible detonation, ask for this information.
- 'Subtlety' is the key word, do not challenge, confront, and demonstrate disbelief, dismay or fear. Ending the call abruptly must be avoided at all costs.
- Whether it is feasible or wise to search for the device before alerting the police and other security agents will depend on information received from the caller and the decision of the head of security or the officer on the ground.
- Signals from personal cell phones can trigger some devices, so care must be exercised in the use of cell phones during such an emergency.
- Inform the caller that the building is occupied and the detonation of a bomb could cause death or serious injury to many innocent people.

- Pay particular attention to background noises such as, motor running, music or any noises which may give a clue to the location of the caller.
- Listen closely to the voice (male, female), voice quality (calm, excited), accents and speech impediments.

10.4 LETTER BOMBS

10.4.1 Letter and parcel bombs are usually designed to harm the recipient of the letter or parcel, or the person responsible for opening it. They can be made quite thin, (small envelope) with a trigger mechanism that is linked to the action of opening the seal. Enough explosive can be packed within, to cause extremely serious injuries to limbs and eyes.

10.4.2 Occasionally an indication of fine wire around the seal can be felt within the envelope or wrapper. However, in most instances, stains such as those associated with grease from cooking oil can be noted on envelopes or packaging. Many explosive compounds sweat, and leave visible traces of this nature while others, do not show any of these characteristics. Persons designated to handle correspondences/letter must be on the lookout for such indicators.

10.4.3 Other indicators may be the faint smell of marzipan. If any of these traces are suspect, all such devices must be isolated away from people and if possible buildings. This act can be undertaken quite safely as the device will have travelled through the postal system without exploding, therefore it can be assumed safe to remove it to an area of safety to await expert attention.

(NB). Do not place any suspect parcel or envelope in a bucket or container filled with water or other liquids, this will compound the problem of disarming, as well as give a higher explosive value to the device. It will also cause additional risk from fragmentation of the holding container should it explode.

10.4.4 Action on finding a Suspicious Package/Suspected Bomb. In the event that one locates a suspicious package or suspected bomb or explosive, do not touch the package. The immediate recourse is to inform the security who will in turn call the police or security service provider to take charge of the situation.

Phones or radios must not be used within the vicinity. Phone and radio transmission can cause premature detonation.

10.5 KIDNAPPING/HOSTAGE SITUATIONS

10.5.1 Kidnapping and hostage taking for various reasons has become common place. Kenya is listed as one of the countries where one is likely to be kidnapped. Members of the Authority must maintain a high level of vigilance at all times and watch for any suspicious or unusual activity. In the event of a kidnap the Authority will work closely with other security providers within the framework of the official government policy as it relates to such situations to ensure that all appropriate actions to resolve the situation is pursued actively.

10.5.2 The Authority will endeavor to provide information to the family of those affected without jeopardizing the rescue effort. The government's long standing policy is that it does not make payments or concessions to kidnappers, since this is considered as an incentive and increases the risk of further kidnappings.

10.5.3 The main target of kidnap are children. Areas that a child can easily be kidnapped especially in Nairobi are clearly mapped out. Hence if a member happens to frequent such areas, they should be alert and take appropriate personal security measures or seek professional security advice.

10.5.4 Kidnapping cases differ in the motivations of the kidnappers, the demands being made for the release of the hostages, and the circumstances where the kidnapping has occurred. Terrorist and criminal groups use kidnapping as a tactic to achieve their goals. Criminal groups often kidnap subjects who they force to withdraw money from ATMs. This is known as "express kidnapping". In some cases victims have been killed or injured while attempting to resist the kidnappers.

10.5.5 The use of ATMs located inside banks, hotels and shopping centers during daylight hours may reduce the risk. Some criminals pose as unlicensed taxi

Reserve

✓

drivers. Once the victim is in the cab they are kidnapped until they agree to their terms.

10.5.6 Another trend is "virtual kidnapping". This is when extortionists, posing as law enforcement officials, call the family or friends of the victim and demand payment in return for release of the allegedly arrested family member or friend. You should avoid divulging financial, business or personal information to strangers.

10.6 DEALING WITH PUBLIC DEMONSTRATIONS AT IPOA PREMISES

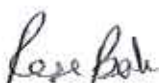
10.6.1 The Independent Policing Oversight Authority is seen as the most promising and authentic avenue to address public complaints against the police. It is therefore highly possible that, large numbers of people could turn out at IPOA to report grievances and in the process become rowdy. If there is a public demonstration at IPOA premises, the officers at the main entrance to the building must relay the information to the security services department, giving an estimated number of the demonstrators.

10.6.2 In the event that the demonstration is expected, the security service provider will be on standby to provide re-enforcements. The security services department will meet the demonstrators, calm them and ensure orderly handling of their grievances through the due process or as shall be determined by the situation on the ground.

10.6.3 If the situation is very fluid and dangerous, the police will have to be called in to disperse the demonstrators. However, if the demonstrators are calm, their leaders will be identified and allowed access to IPOA leadership where they can present their grievances. The demonstrators must not be allowed to enter the premises. The Police will be called to give assistance outside the premises.

10.7 ILLNESS OR INJURY

10.7.1 Professional assistance must be sought immediately from the closest service provider to deal with the condition or injury unless a member available



at the scene or security officer has particular first aid or nursing skills. However, the following basic action should be taken whenever possible to minimise further harm:

- Prevent further injury – e.g. switch off electricity before touching a casualty if anywhere near electricity, remove from gas filled room, extinguish or remove from fire, etc.
- Sustain life - by artificial respiration if breathing has stopped, placing in prone position if unconscious or stemming blood flow, using a handkerchief if nothing else is available, from serious wound.
- Prevent condition worsening - by not moving in the case of head or spinal injuries, immobilising broken limbs.
- Minimise shock - by loosening tight clothing, keeping casualty warm, though not overheating, appearing calm and confident, etc.
- Obtain assistance - preferably of same gender or anyone with commensurate skills, particularly if checking pockets for a medical treatment card, etc.

10.8 FIRE EVACUATION PROCEDURES

10.8.1 An individual on discovering a fire should:

- Raise the alarm by shouting "**Fire! Fire! Fire!**"
- Activate the nearest fire alarm break glass unit. The fire alarm system in the entire building will sound.
- Contact the fire service department (Fire Brigade) and inform security service provider giving the location, size and nature of fire.
- If safe to do so, try to put out the fire by means of the nearest available firefighting equipment.
- On hearing the fire alarm, or being advised over the PA system or any other means, or hearing someone shout "Fire! Fire! Fire; all IPOA members, clients and customers on 2nd on 3rd floor must stop whatever they are doing and walk briskly and in an orderly manner out of the building through the immediate fire exit next to their

office. The designated fire marshal shall be responsible for speedy opening of all fire exits and must ensure that the floor is fully evacuated before proceeding to the marshalling point for roll call.

10.8.2 Fire exit doors are all marked appropriately. If there is no fire or smoke contamination in the vicinity of the fire exit, do not open the doors without the instructions of the floor fire marshal or security officer present. If there is a fire or dense smoke in the immediate area, the nearest fire exit is to be used and this should be opened without delay.

10.8.3 For personnel who for any reason, are outside of the main building when the fire alarm activates, it is your responsibility to make your own way to the assembly point by the quickest means possible. You are then to join your respective department and await instructions from your department head. You are not to make your way back inside the building.

10.8.4 The signal to evacuate from the building will normally be given by security department over the PA system if available or relayed by telephone.

10.8.5 The security department will co-ordinate all internal emergency actions until the fire response team arrives.

10.8.6 No entry by any personnel other than emergency services will be allowed back into the premises / building until the head of security has given '**ALL CLEAR**'.

10.8.7 A security audit will be conducted by the department of security together with the security service provider and where necessary the police, to determine the cause of fire and the damage caused to property and materials of the Authority immediately the fire has been contained.

10.9 WARNING ON USE OF FIRE EQUIPMENT

Hose Reels	-	Use only if trained
Red Coloured	-	Not for electrical, liquid or oil fires
Blue Coloured	-	For oil, chemical, petrol, spirit fires
Black Colour	-	Use on any fire

10.10 ROLL CALL PROCEDURES

On evacuating the premises, the head of each department or representative who is familiar with other members will conduct roll call. On completion of the roll call, roll callers should report the results to the head of security. Roll callers should be aware that members of their department may be involved in the Fire Response Team and may be absent from the assembly point. Names of those involved in the fire party will be confirmed by the Fire Response Team Leader.

10.11 POWERS OF SEARCH

10.11.1 Security officers who are on duty are empowered to search any individual or vehicle entering or leaving IPOA premises. When conducting the search, security officers should be aware that search is incidental to custody. Therefore, the security officer can search the person and effect arrest or conduct a search on the person(s) taken into custody and seize any article in his/her possession or under his control as evidence tending to show his guilt.

10.11.2 Once the person is taken into custody and searched, preliminary interrogation can take place but the person must be delivered immediately to the police. The officers involved are to provide the Police with assistance as required relating to the case.

10.12 ARREST AND DETENTION

Any person who commits an offence on the Authority premises will be arrested. The security officer who witnesses the act or is given credible information of the act can arrest the suspect. Before the arrest, the officer should identify him/herself and tell the person the reason of the arrest. The arrested person will be handed over to the police immediately for further investigation. It is

however important for the arresting officer to appreciate that behaviors such as, disorderly conduct and intoxication etc., are not indictable offences. Persons who exhibit such behavior will be escorted and removed from IPOA premises to prevent any escalation or injury.

10.13 TRAFFIC ACCIDENT/INCIDENT INVESTIGATION

10.13.1 Traffic accidents are a common phenomenon on our roads. Drivers must exercise caution, demonstrate courtesy on the roads and act professionally in the event that the Authority vehicle is involved in a traffic accident.

10.13.2 Traffic accident investigation is similar in principle to any other type of investigation and the initial management of the scene of accident is crucial. For the purposes of procedure, when a vehicle is involved in a traffic accident, the law requires that one should not move. However, if the security of the driver and passengers is at stake, they should exit the scene of accident with or without the vehicle immediately and report the accident to the nearest police station immediately and not later than six hours.

10.13.3 **Investigation of the Traffic Accident.** The aim of any investigation is to establish the facts of what occurred. The traffic accident inquiry requires a conclusion which shows culpability for the accident. This is necessary for insurance purposes and where possible to protect the Authority from unjustified claims for the accident or damage. When investigating a traffic accident the following guidelines are to be followed:

10.13.4 Arrival at Scene:

- Secure the scene.
- Attend to the injured (knowledge of first aid is necessary)
- Identify the drivers of the vehicles involved immediately.
- Identify any witnesses
- Do not move the vehicles until you have photographed the scene and drawn a sketch plan of the scene.

Rosa Red

1

10.13.5 Scene Examination

- Take note of weather conditions:
- Road conditions.
- Speed restrictions in the area.
- Regulatory traffic signs in the area.
- Measure the scene (endorse measurements on sketch plan).

10.13.6 Statements/Interviews - Statements recorded from drivers involved and witness must include:

- Direction in which they were traveling.
- Estimated speed at the vehicle was traveling.
- The gear the vehicle was in at the time (where applicable).
- How long they had been driving prior to the accident.
- Any alcohol involved, how long before the accident.
- Any distractions immediately prior to the accident.
- Weather conditions at the time.
- Time of accident.
- What the other vehicle was doing immediately prior to the accident.
- Depending on the location of the accident, the driver's knowledge of the road traffic regulations for the area.

10.14 Traffic Accident Reports. A written report is to be submitted at the completion of the investigation and must contain all the facts relevant to the investigation. The layout is the same format used for other types of investigations. However, it may include separate headings for issues such as speed, weather and light. Other requirements are:

- Statements of drivers and witnesses.
- Sketch Plan of accident.
- Photographs of accident and vehicle damage.
- Repair cost estimates for the vehicles
- Doctors certificate for:

Reserve

for

- ✓ Any alcohol tests carried out;
- ✓ Any injuries sustained by persons involved;
- ✓ Invoices showing cost of treatment.
- Non IPOA drivers insurance documents (if possible).

10.15 Sketch Plans. A Sketch Plan is the principal way of describing the scene to persons reading the report. It is not drawn to scale in relation to the accident area, but a scale should be used to put the drawing in perspective for the viewer. It is important that the sketch shows all the measurements and can be used to accurately place the vehicles in the exact position, should a reconstruction be required. This may not be required in non-injury or for minor traffic accidents. It is however necessary if the accident was fatal. In every case a sketch plan is to be prepared for each accident that involves a non-IPOA vehicle and driver.

Signed... 
Chief Executive Officer / Secretary

Signed... 
Chair, Risk & Audit Committee

Signed... 
Board Chairman

