GUIDELINES FOR PREPARING A SAFETY MANAGEMENT AND SECURITY PLANS

Under the Guns, Explosives and Weapons Control Act 2021, applicant must submit comprehensive Safety Management and Security Plans when applying for GEW licences. These documents outline the management of safety risks and security measures associated with regulated activities involving guns, explosives, and weapons (GEW).

Guidelines for Preparing a Safety Management Plan

2 A safety management plan is a comprehensive document (or set of documents) in English that outlines how you will manage safety risks associated with regulated activities involving GEW. This plan is required for applications for GEW licences.

Essential Components

a. Risk Management Procedures

The plan must detail:

- Specific procedures for managing hazards and risks related to your regulated activities
- Clear documentation of risk assessment methodologies
- Steps for identifying and controlling potential safety hazards

b. Safety Policies and Protection Measures

Include detailed policies and procedures for:

- Protecting people from alarm, death, or injury
- Safeguarding property from unlawful destruction or damage
- Maintaining public safety during operations
- Implementing preventive measures

c. Record Keeping System

Establish a robust system for:

- Maintaining comprehensive safety records
- Documenting incidents and responses
- Tracking compliance with safety procedures
- Ensuring records are accessible for inspection by Licensing Officers

d. Mandatory Content Requirements

i. Policy Documentation

- Include detailed policies and procedures for all applicable matters listed in the First Schedule
- Ensure policies are specific to your regulated activities

ii. Risk Assessment

- Provide comprehensive assessment of risks related to:
  - Handling GEW
  - Possessing GEW
  - Using GEW

iii. Emergency Response Plan

Your emergency response plan must cover:

- Spillage control procedures for explosives/explosive precursors
- Firefighting equipment provisions

- First aid arrangements
- Detailed evacuation procedures

iv. Compliance Monitoring

Detail internal policies and controls for:

- Monitoring compliance with the Act and Regulations
- Ensuring adherence to licence conditions
- Following applicable standards
- Implementing the approved safety management plan
- Ensuring employee compliance with all requirements

3 The following are some best practices when putting up Safety Management Plans

- Write procedures in clear, straightforward language
- Include relevant diagrams and flowcharts where helpful
- Regularly review and update procedures
- Ensure all staff are trained on the procedures
- Maintain clear documentation of all safety-related activities

Guidelines for Preparing a Security Plan

4 These guidelines outline the mandatory components of a Security Plan detailing the security measures and risk management strategies for handling or storing GEW. The Security Plan must be submitted when applying for GEW licences under the Guns, Explosives and Weapons Control Act 2021.

Essential Components

a. Security Risk Identification

Your plan must:

- Identify all potential security risks associated with your regulated activities
- Provide detailed assessment of each identified risk
- Document the methodology used for risk identification

b. Security Measures and Procedures

Detail the facilities, systems, and procedures for:

Physical Security

- Description of security infrastructure
- Where applicable, deployment plans for armed auxiliary police officers
- Facility access control measures
- Security monitoring systems

Personnel Screening

Detail screening procedures, which may include:

- Equipment-based searches (non-contact scanning)
- Frisk searches (quick manual inspection of outer clothing)
- Inspection of personal property
- Entry and exit screening protocols

Chain of Possession Controls

- Procedures for tracking explosives/explosive precursors
- Documentation systems for transfers between authorised handlers
- Verification processes for authorised recipients
- Record-keeping procedures for chain of custody

c. Authorised Personnel Management

The following must be included:

- List of nominated individuals approved for unsupervised access
- Verification procedures for authorised personnel
- Access control protocols
- Training requirements for authorised personnel

d. Record Keeping Requirements

Establish systems for:

- Maintaining comprehensive security records
- Documenting security incidents
- Tracking access logs
- Recording screening activities
- Ensuring records are accessible for inspection

e. Transport Security Plan

For conveying relevant consignments in vessels or vehicles, include:

- Detailed transport security procedures
- Risk management during transit
- Emergency response protocols
- Policies and procedures as required by the Second Schedule

5 The following are some best practices when putting up Security Plans

a. Documentation

- Use clear, precise language
- Include relevant diagrams and maps
- Maintain updated contact lists
- Regular review and updating of procedures

b. Personnel Management

- Clear designation of responsibilities
- Regular training schedules
- Documentation of qualifications
- Procedures for updating authorised personnel list

c. Security Protocols

- Clear escalation procedures
- Emergency response protocols
- Communication systems
- Regular security audits

Security Guidelines Premises Storing/Handling Security Sensitive Materials (SSMs)

S/N	Area of Interest		Description	Recommended Measures
1	Perimeter Security	Perimeter barriers	Perimeter barriers are measures adopted along the boundary of the facility. They are normally the first layer of protection and provide both physical and psychological deterrents to unauthorised entry, thereby deterring or delaying such incidents from occurring. Different objectives for a perimeter barrier include: • Marking an administrative border line of a private area. • Preventing unintended entry of vehicles or people. • Creating a stand-off line for a variety of threats. • Deterring possible intruders. • Preventing or delaying the intrusion of a person. • Preventing the intrusion of a vehicle. • Preventing or delaying an illegal exit from a confined area. • An operative defence line for security guards or police. • A line-of-sight blocking element. • An architectural or landscape feature.	Barriers to humans (such barriers should be at least 2.4m high) • Concrete wall • Brick wall • Welded-mesh • Pedestrian turnstiles fence Barriers to vehicles • Bollards • Drop arm barriers • Vehicular gates • Planters Natural or landscaping barriers • Hedge rows • Rocks • Timber • Water feature
		Monitoring and detection	Monitoring and detection equipment are key components of effective perimeter security. Often, facilities will monitor for security incidents through a	Fence-mounted or open-area sensors • Vibration detection sensors • Video motion detection

			combination of human oversight and one or more electronic sensors or other intrusion detection systems. Typically, when a sensor identifies an event of interest, an alarm notifies the security personnel or assigned staff who will then assess the event directly at the location or remotely through surveillance images. To increase the reliability of a monitoring system, one may elect to deploy multiple interactive, redundant measures at the location of interest.	• Infrared sensors • Acoustic sensors Remote surveillance • Thermal images • Internet Protocol (IP) cameras Human-based monitoring via security sentry or mobile patrol.
		Security lighting	Security lighting increases visibility around perimeters, buildings, and sensitive locations and acts as a deterrent and detection tool. It should therefore be provided at the perimeter to allow security personnel to maintain visual observation during darkness both by direct surveillance and through the CCTV system. Sufficient lighting should be provided to ensure that the perimeter is well-lighted and that there are no blind spots. At a minimum, all access points, the perimeter and restricted areas should be illuminated from sunset to sunrise or during periods of low visibility. In some circumstances, lighting may not be required, but these circumstances must be addressed in the building's security plan. Lighting however, also needs to be	Continuous lighting is the most commonly used form of security lighting systems, consisting of a series of fixed light sources arranged to illuminate a given area on a continuous basis during the hours of darkness with overlapping cones of light. The recommended illumination standards are: • 2 lux for large open areas • 5 lux for surveillance of confined areas • 10 lux for surveillance of vehicle/pedestrian entrances Standby lighting is similar to continuous lighting and meets the same security lighting specifications but is used only in certain

			matched to the operating environment and this should be taken into consideration during planning.	circumstances. When a possible intruder is detected, the security system or guard force can activate the standby lighting system for extra illumination. It can also be deployed at unattended/attended gates for extra lighting. Standby lighting differs from the continuous lighting in that only security personnel or the security system software have control over the system. This lighting system consists of manually operated movable light sources such as searchlights, which can be activated during the hours of darkness to cover specific areas as needed. Moveable lights are normally used to supplement continuous or standby systems. The emergency lighting system may duplicate the other three systems in whole or in part. Its use is normally limited to periods of main power failure or other emergencies. While security lighting should be connected to an uninterruptible power system when possible, emergency lighting should depend on a separate, alternate power source, such as portable generators or batteries.

		Access control	Wherever a perimeter line is planned, points of access for vehicles and pedestrians are required at various points along the line. These points are usually regarded as the weak links of the perimeter as they require a breach in the protective line every time they are opened. Access points control the time and people permitted to enter a building or facility. In addition to controlling passage, access management usually includes the ability to observe and track movement in and out of controlled areas. The entry points through a perimeter line will typically consist of vehicle gates, pedestrian gates, and in some cases, a guard post. The entry points provide places where the required level of vehicle or pedestrian screening and access control can be implemented. The challenge of designing an entry point is to prevent unauthorised access while maximising the flow of authorised access by pedestrians or vehicles.	Position the entry control point to allow adequate visual assessment of approaching vehicles. Allow adequate passage for a vehicle that has been denied access at the security check to exit without having to enter the site or move vehicles in queue. Any vehicle/pedestrian gate on the perimeter line should provide the same level of protection against vehicles and intruders as that provided by the rest of the perimeter line. Entrances should be designed in such a way as to enable access control to be implemented either for unattended entry using an access control system or by guards. Sufficient space should be allocated for proper inspection and for communication (which may be at a distance) between the people entering and those responsible for approving access. Ascertain and verify the purpose of the visit such as checks of government issued photo identification or letters of appointment. Providing company or facility issued photo IDs to individuals permitted

				access to the facility or restricted areas of the facility that identify: • Employees • Regular contractors • Temporary contractors • Visitors
2	General Premise Security	Access Control	This is focused on the identification and securing of cleared personnel who have already been granted permission to enter the facility. The primary component of a successful access control system if knowing who is allowed on-site. Personnel identification measures help a facility quickly determine whether or not an individual is permitted access to a facility or a restricted area.	Providing company-issued photo IDs to individuals permitted access to the facility or restricted areas of the facility that identify different group of personnel • Employees • Regular contractors • Temporary contractors • Visitors An individual should not be allowed access an area other than those permitted. As far as possible, visitors and temporary contractors should be escorted when moving within the facility.
		Monitoring and detection	Monitoring and detection equipment are key components of effective perimeter security. Often, facilities will monitor for security incidents through a combination of human oversight and one or more electronic sensors or other intrusion detection systems. Typically, when a sensor identifies an event of interest, an alarm notifies the security personnel or assigned staff who will then	Open-area sensors • Vibration detection sensors • Video motion detection • Infrared sensors • Acoustic sensors Remote surveillance • CCTV cameras • Thermal images • Internet Protocol (IP) cameras Human-based monitoring

			assess the event directly at the location or remotely through surveillance images. To increase the reliability of a monitoring system, one may elect to deploy multiple interactive, redundant measures at the location of interest.	• Staff to keep a look out for unfamiliar, suspicious characters and suspicious activities within the facility and notify relevant staff upon detection.
		General security policy	Prescribe a company security policy to inculcate a security mindset and enhance security awareness.	Regular training and awareness for new and existing employees. Identify suspicious indicators and report incidents to relevant staff and authorities. Develop SOPs specifying response during contingencies, and hold periodic exercises to ensure staff are familiar
3	Critical Facility Security	Access Control	This is focused on the identification and securing of cleared personnel who have already been granted permission to enter the facility, particularly the critical site/facility. The primary component of a successful access control system if knowing who is allowed on-site. Personnel identification measures help a facility quickly determine whether or not an individual is permitted access to a facility or a restricted area.	Providing company-issued photo IDs to individuals permitted access to the facility or restricted areas of the facility that identify different group of personnel • Employees • Regular contractors • Temporary contractors • Visitors Electronic access control measures • Tap card readers • Biometric readers • Open door detectors (magnetic switches) • Access control management software

				• Access control management stations Manual access control measures • Regulated key access • Sign-in and sign-out procedures
		Monitoring and detection	Monitoring and detection equipment are key components of effective perimeter security. Often, facilities will monitor for security incidents through a combination of human oversight and one or more electronic sensors or other intrusion detection systems. Typically, when a sensor identifies an event of interest, an alarm notifies the security personnel or assigned staff who will then assess the event directly at the location or remotely through surveillance images. To increase the reliability of a monitoring system, one may elect to deploy multiple interactive, redundant measures at the location of interest.	Open-area sensors • Vibration detection sensors • Video motion detection • Infrared sensors • Acoustic sensors Remote surveillance • CCTV cameras • Thermal images • Internet Protocol (IP) cameras Human-based monitoring • Staff to keep a look out for unfamiliar, suspicious characters and suspicious activities within the facility and notify relevant staff upon detection.
		Inventory control and stock keeping	Stock keeping refers to the maintenance of a system, either electronic or manual, of keeping track of the SSMs which are stored/handled/processed in the facility. Such information can include but is not limited to the following: type of SSMs, amount used, amount disposed and location. Information should be readily available.	Lists all the hazardous materials at the covered facility Provides tracking of the quantity and the physical location of each hazardous material Monitors use by authorized personnel

				Tracks disposal and maintains a record of disposed containers Contains purchasing/receiving records for materials management Provision of a locked rack or other tamper-evident, physical means of securing man portable containers of theft/diversion hazardous materials. Examples include: • Chains and locks that cannot be cut or breached with man-powered tools • Entry/motion detectors and alarms for the buildings or rooms where the containers are stored
		Quality Control	Prevent attempts to intentionally disrupt the operations of the facility to cause harm and injuries.	Develop a written procedure to regularly inspect, test, calibrate, repair, and maintain security systems and systems related to security, such as communications and emergency notification equipment. The procedure should identify responsibilities, tasks, their frequencies of occurrence, and the documentation required Perform inspection, testing, and maintenance tasks on a regular basis and in accordance with the manufacturer's instructions

				Include all security equipment, such as gates, cameras, lights, alarms, and keypad entry systems, in the routine inspection and maintenance Employ appropriate security measures when performing maintenance, as well as in response to non-routine outages, equipment failures and malfunctions Document non-routine incidents and promptly report them to the Security Officer in charge Have procedures to verify the identity and each occurrence of contractor personnel who perform inspection, testing, and maintenance of security equipment

CCTV Specification

a) CCTV cameras covering all entrances and exits directly leading to/from the approved storage area and the interior of the approved storage area where the stocks are stored.
b) Ensure that all the conditions below are met:
   i. each CCTV camera is positioned and angled in such a way that it can capture the face of every person entering or exiting through that doorway, or depositing, removing or handling any SSM in the approved storage area;
   ii. there is a clear line of sight from the CCTV cameras to the locations they are covering; and
   iii. the CCTV cameras' line of sight shall not be obstructed in any way.
c) All CCTV cameras and recording system(s) meet or exceed the following specifications:
   i. records colour images at the resolution of HD 1080p: 1920x1080 pixels or its equivalent;
   ii. records at 12 frames per second;
   iii. supports the exporting of CCTV camera recordings via a USB port in open-source formats such as *.avi (Microsoft), *.mov (Apple QuickTime), *.mp4 (MPEG), or such format as approved by the Licensing Officer in writing;
   iv. is switched on and in a recording mode at all times; and
   v. is able to store all CCTV camera recordings for at least 31 days from the date of recording.

d) All CCTV cameras and recording system(s) remain in good working condition at all times.