

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

S/N	Area of Interest		Description	Recommended Measures
1	Perimeter Security	Perimeter barriers	<p>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.</p> <p>Different objectives for a perimeter barriers include:</p> <ul style="list-style-type: none"> • 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. 	<p>Barriers to humans (such barriers should be at least 2.4m high)</p> <ul style="list-style-type: none"> • Concrete wall • Brick wall • Chain-linked fence • Welded-mesh • Pedestrian turnstiles fence <p>Barriers to vehicles</p> <ul style="list-style-type: none"> • Bollards • Drop arm barriers • Vehicular gates • Planters <p>Natural or landscaping barriers</p> <ul style="list-style-type: none"> • Hedge rows • Rocks • Timber • Water feature
		Monitoring and	Monitoring and detection equipment	Fence-mounted or open-area sensors

		<p>detection</p>	<p>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.</p> <p>To increase the reliability of a monitoring system, one may elect to deploy multiple interactive, redundant measures at the location of interest.</p>	<ul style="list-style-type: none"> • Vibration detection sensors • Video motion detection • Infrared sensors • Acoustic sensors <p>Remote surveillance</p> <ul style="list-style-type: none"> • CCTV cameras (4 CIF, 6 frames/sec for indoor and 12 frame/sec for outdoors, 28 days archival with 10% buffer) • Thermal images • Internet Protocol (IP) cameras <p>Human-based monitoring via security sentry or mobile patrol.</p>
		<p>Security lighting</p>	<p>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.</p> <p>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</p>	<p>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.</p> <p>The recommended illumination standards are:</p> <ul style="list-style-type: none"> • 2 lux for large open areas • 5 lux for surveillance of confined areas • 10 lux for surveillance of vehicle/pedestrian entrances <p>Standby lighting is similar to continuous lighting and meets the same security lighting specifications, but is used only in certain circumstances. When a possible intruder is</p>

			<p>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 matched to the operating environment and this should be taken into consideration during planning.</p>	<p>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.</p> <p>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.</p> <p>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.</p>
		<p>Access control</p>	<p>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</p>	<p>Position the entry control point to allow adequate visual assessment of approaching vehicles.</p> <p>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.</p>

			<p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Ascertain and verify the purpose of the visit such as checks of government issued photo identification or letters of appointment.</p> <p>Providing company or facility issued photo IDs to individuals permitted access to the facility or restricted areas of the facility that identify:</p> <ul style="list-style-type: none"> • Employees • Regular contractors • Temporary contractors • Visitors
2	General Premise Security	Access Control	<p>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</p>	<p>Providing company-issued photo IDs to individuals permitted access to the facility or restricted areas of the facility that identify different group of personnel</p> <ul style="list-style-type: none"> • Employees

		<p>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.</p>	<ul style="list-style-type: none"> • Regular contractors • Temporary contractors • Visitors <p>An individual should not be allowed access an area other than those permitted.</p> <p>As far as possible, visitors and temporary contractors should be escorted when moving within the facility.</p>
	Monitoring and detection	<p>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.</p> <p>To increase the reliability of a monitoring system, one may elect to deploy multiple interactive, redundant measures at the location of interest.</p>	<p>Open-area sensors</p> <ul style="list-style-type: none"> • Vibration detection sensors • Video motion detection • Infrared sensors • Acoustic sensors <p>Remote surveillance</p> <ul style="list-style-type: none"> • CCTV cameras • Thermal images • Internet Protocol (IP) cameras <p>Human-based monitoring</p> <ul style="list-style-type: none"> • 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	<p>Prescribe a company security policy to inculcate a security mindset and enhance security awareness.</p>	<p>Regular training and awareness for new and existing employees.</p> <p>Identify suspicious indicators and report incidents to relevant staff and authorities.</p>

				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 is 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.	<p>Providing company-issued photo IDs to individuals permitted access to the facility or restricted areas of the facility that identify different group of personnel</p> <ul style="list-style-type: none"> • Employees • Regular contractors • Temporary contractors • Visitors <p>Electronic access control measures</p> <ul style="list-style-type: none"> • Tap card readers • Biometric readers • Open door detectors (magnetic switches) • Access control management software • Access control management stations <p>Manual access control measures</p> <ul style="list-style-type: none"> • 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	<p>Open-area sensors</p> <ul style="list-style-type: none"> • Vibration detection sensors • Video motion detection • Infrared sensors • Acoustic sensors <p>Remote surveillance</p> <ul style="list-style-type: none"> • CCTV cameras • Thermal images

		<p>security personnel or assigned staff who will then assess the event directly at the location or remotely through surveillance images.</p> <p>To increase the reliability of a monitoring system, one may elect to deploy multiple interactive, redundant measures at the location of interest.</p>	<ul style="list-style-type: none"> Internet Protocol (IP) cameras <p>Human-based monitoring</p> <ul style="list-style-type: none"> 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	<p>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.</p>	<p>Lists all the hazardous materials at the covered facility</p> <p>Provides tracking of the quantity and the physical location of each hazardous material</p> <p>Monitors use by authorized personnel</p> <p>Tracks disposal and maintains a record of disposed containers</p> <p>Contains purchasing/receiving records for materials management</p> <p>Provision of a locked rack or other tamper-evident, physical means of securing man portable containers of theft/diversion hazardous materials. Examples include:</p> <ul style="list-style-type: none"> 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	<p>Prevent attempts to intentionally disrupt the operations of the facility to</p>	<p>Develop a written procedure to regularly inspect, test, calibrate, repair, and maintain</p>

			<p>cause harm and injuries.</p>	<p>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</p> <p>Perform inspection, testing, and maintenance tasks on a regular basis and in accordance with the manufacturer’s instructions</p> <p>Include all security equipment, such as gates, cameras, lights, alarms, and keypad entry systems, in the routine inspection and maintenance</p> <p>Employ appropriate security measures when performing maintenance, as well as in response to non-routine outages, equipment failures and malfunctions</p> <p>Document non-routine incidents and promptly report them to the Security Officer in charge</p> <p>Have procedures to verify the identity and each occurrence of contractor personnel who perform inspection, testing, and maintenance of security equipment</p>
--	--	--	---------------------------------	---