Guidelines for Required Security Measures at Facilities Storing Tier 1 Security Sensitive Materials/Hazardous Materials

This document aims to guide facilities storing Tier 1 Security Sensitive Materials (SSMs) on the required security measures to be implemented to address threats of unauthorised entry, theft, and sabotage of the SSM.

The security measures are primarily segregated into part A, B and C; namely the Perimeter Security (A), General Premises Security (B) and Storage Security (C). Generally, all sections of the measures would apply, with exceptions applied depending on the extent of control that the company has over the security of the premises including that of the perimeter. Circumstances where **only Section C** of the measures apply are when (a) an area is leased and the company has no control over the security measures beyond the leased area and (b) school labs, regardless of whether they are owned or leased.

Note with regards to Tier 1 SSMs regulated by MOH under the Biological Agents and Toxins Act:

a) **Facility** refers to the critical area (or laboratory) where SSM is stored/handled. The facility can be a standalone building, or a critical area resided within a building.
b) **Company** refers the operator of a facility.
c) **Premises** refers to the facility and/or building, together with its land.
d) **General area** refers to the restricted area surrounding the facility/building.

Inspections corresponding to Facility Set-up		
S/No	**Facility Set-up**	**Security Measures that apply**
1	Company owns/leases the entire premises, i.e. the land, the facility and/or the building where the facility is resided; and the company has security control over the perimeter of the premises, the general area, and the facility.	Parts A, B and C
2	Company owns/leases the building and the facility within the building, and the company has security control over the facility and the general area, but not the perimeter of the premises.	Parts B and C
3	Company owns/leases the facility which resides within a building; and the company only has security control over the facility but not the general area and the perimeter of the premises.	Parts C

Prior to the license issuance by the National Authority (NA) regulating the SSM, there will be an inspection to ensure all applicable security measures prescribed in this guideline are implemented on top of the safety requirements by the NA.

Companies may refer to the Guidelines for Enhancing Building Security in Singapore and Video Surveillance System Standard 2022 (found in the open net) for detailed examples and good practices to help building owners incorporate pragmatic security procedures, physical protection concepts and security technology into their building's security plans.

Guidelines for Required Security Measures
at Facilities Storing Tier 1 Security Sensitive Materials/Hazardous Materials

A1) Perimeter Security		
Area of Interest	**Description**	**Mandatory Measures**
A1) Perimeter fencing	Perimeter barriers are measures adopted along the boundary of the premises. They are normally the first layer of protection and provide both physical and psychological deterrents to unauthorised entry. A perimeter line is a physical line, usually following a site boundary, which provides a means of establishing a controlled access area around a building or asset. Physical barriers can be used to define the physical limits of a premises and can help to restrict, channel, or impede access and create a continuous barrier around the site. Physical barriers also serve as a deterrent for anyone planning to penetrate the site. Security measures which form the perimeter line should detect, delay and/or deny access. There are many ways to create a physical barrier including the use of fences, walls, bollards, or planters etc. The selection of barrier elements must take into account the desired level of security based on the threat (e.g. the type of vehicle and approach speed to be protected against). A wide variety of solutions and products are available in the market, which allow premises	**A1.1** There is a perimeter fence/wall surrounding the premises.

	owners to balance cost, physical and architectural considerations. Rationale for perimeter barriers include: • Marking an administrative border line of a private area. • Preventing unintended entry of vehicles or people. • Creating a stand-off distance 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.	
	Fencing along the perimeter or boundary of the premises should be at minimum 2.4m in height. Examples of barriers are as follows: • Concrete wall • Brick wall • Chain-linked fence • Welded-mesh • Pedestrian turnstiles fence	**A 1.2** The fence/wall is minimum of 2.4m in height, including vehicular and pedestrian gates. For existing premises with a fencing/wall lower than 2.4m, companies should increase the perimeter fencing to 2.4m with top guards.

	For new premises or premises going through major renovation, the baseline is 2.4m (without top guards).
The fence/wall surrounding the premises needs to be installed and maintained periodically. Damages such as corrosion as well as wear and tear should be identified and rectified soonest to prevent tampering leading to intrusion.	**A1.3** The fence/wall is well maintained. (There are no holes or defective areas.)
The base of the fence/wall where it meets the ground needs to be fully sealed, without any gaps so that it mitigates the prevention of digging from the ground level. A minimum footing depth of 300mm is required to delay tunnelling attempts.	**A1.4** There are no gaps in between the base of the fence/wall and the ground. (Gaps will facilitate unauthorised entry via digging below the fence/wall.)
A 2m clearance should be observed from the fence line to the nearest feature such as trees, lamppost, etc which will aid in scaling the fence and accessing into the facility.	**A1.5** There are no objects or structures (e.g. trees, lamppost etc.) within 2m from the exterior of fence/wall that can aid scaling of the fence/wall. *Note: The company can contact the regulatory agency (e.g. NParks for trees) to address the concerns, where necessary.*
The fence/wall should not be designed to have features which aids in having footholds which also assists in scaling.	**A1.6** There are no footholds on the fence/wall that can aid scaling from the exterior.

	Joints and welded seals need to face towards the inner side on the premises so as not to create weakness in the fencing/wall.	**A1.7** The welded points and joints are on the "safe" side, within the premise.
A2) Monitoring and detection	Monitoring and detection equipment are key components of effective perimeter security. Often, premises will be monitored for security incidents through a combination of human oversight and one or more electronic sensors or other intrusion detection systems. Typically, when a sensor detects an event of interest, an alarm will be triggered to notify the security personnel or assigned staff who will then assess the event directly at the location or remotely through surveillance images. Fence Intrusion Detection System Fence intrusion detection systems (FIDS) consist of sensors to detect intruders and a device to sound an alert. These sensors detect intruders by monitoring movement, sound, vibration or other disturbances. Standards for Fence Intrusion Detection Systems The guidelines for fence intrusion detection systems are based on the UFC 4-021-02 and BS 4737-4.3.	**A2.8** A Fence Intrusion Detection System (FIDS) is installed along the fence/wall. Note: To ensure that the intrusion detection equipment (e.g. Vibration detection sensors, Video motion detection, Infrared sensors, Acoustic sensors, etc) is working in tandem with CCTV cameras at surveillance locations.

	Types of Fence Intrusion Detection Systems: • Taut Wires Taut wires are stretched along a fence and will trigger an alarm in the command centre if the wires are cut, pulled or bridged electrically. In some cases, they can also provide a non-lethal electric shock. The taut wires may be installed in a variety of configurations such as on the top, inside or outside of a wall. • Step Detectors Step detectors are used to detect someone stepping on the top of a wall or laying a ladder against it. They usually consist of covered coils running along the top of the wall. When the cover bends from the weight of a person or ladder, the command centre will be alerted. • Infra-Red Active Motion Detectors Infrared active motion sensors screen an area with infrared light. If anyone passes through the screened area, a signal will be sent to the command centre. These detectors can be installed in such a way for it to be completely unobtrusive. • Video Motion Detectors (VMD)	

	VMD is a video surveillance-based system which works by using analytics to identify suspicious behaviour. For example, movement in a prohibited area. While an intruder may see the cameras, he may not know that a motion detector is in use. • Vibration Detectors Vibration detectors are based on wires running through a fence with sensors installed along their length to detect any vibration. An intruder trying to climb the fence will cause an alarm to be triggered in the command centre. • Microwaves Motion Detectors These detectors make an invisible line using microwaves. Crossing the line will send a signal to the command centre. These detectors are usually noticeable. • Infrared Beam Detectors Infrared beams can create an invisible line or lattice that when crossed, triggers an alarm in the command centre. These detectors are usually noticeable.	
	The alarm from the IDS, upon activation should send an alert to two different individuals. An example of the notification may be via a SMS sent	**A2.9** The alarm from the Intrusion Detection System (IDS) should trigger an alert via SMS to at least two

to two staffs. This is in case one of them is occupied and/or unable to respond.	personnel from the company or to a 24h/7 manned (i.e. warm body onsite) security room.
There should be CCTV coverage at all locations of the perimeter of the premises.	**A2.10** The perimeter of the premises is monitored by CCTV cameras. (i.e. The perimeter fencing, and the interior of the premises should be monitored by CCTV cameras.) **A2.11** The specifications of the CCTV cameras and its system comply with the SPF VSS Standard for Building. SPF VSS Standard for Building (extract) (i) The CCTV camera is an Internet Protocol (IP) Camera. (ii) All recordings are made at a minimum of 6 frames per second (fps) (for indoor) or 12 fps (for outdoor monitoring of slow-moving traffic e.g. along driveway) for each and every video image. The CCTV camera has the capability to record from selected or designated cameras in real time mode at 25 fps. *Accepted:* *Indoors – 6 fps* *Outdoors – 12 fps* *Recommended – 25 fps* (iii) The CCTV camera has a resolution of HD 1080p:1920x1080 pixels.

	(iv) The CCTV system has a minimum 31 days of archival. (v)The recorded picture quality is not reduced due to the image compression. (vi) the recorded images meet the minimum image height requirements of 'Observation', 'Recognition', 'Identification' and 'Detection' level stated in video surveillance system standard (VSS) for buildings (Annex A). Note: To ask company to send the CCTV specifications to PSWG through the NAs' Points of Contacts (POC).
The security consoles/systems for the cameras should be housed in designated secured rooms accessible for only authorised personnel. The rooms should be capable of keeping the recordings in a secured environment, protected from excessive moisture and dust, with preventive measures against unauthorised access, removal or viewing of the recordings.	**A2.12** (i) The CCTV consoles/systems are housed at secured environment[1], away from moisture and dust. (ii) The CCTV consoles/systems are protected against unauthorised access.

[1] *Secured environment would mean that the location of the recording and storage facilities should be decided based on cyber and physical security risk assessment and be sited within the inner perimeter of the building and away from vehicular access.*

	The keys to access to secured location, where security systems are housed, are to be kept by authorised personnel who operates the CCTV systems, and/or the personnel in-charge of security and/or administrative matters of the CCTV system.	**A2.13** The keys to the room storing the CCTV camera consoles/systems are kept by authorised personnel in a secured receptacle (e.g. in a keypress) within the facility. Authorised person in this case refers to person who is required to/authorised to operate the CCTVs.
	The CCTV system should be monitored 24/7, preferable on site by a warm body. If this is not feasible, the CCTV footages should then be remotely accessible through mobile. If mobile access to footage is used, companies should carry out the required risk assessments to minimize potential security risk (e.g. engaging a professional to ensure that suitable processes and measures are in place to safeguard data security concerns).	**A2.14** The CCTV camera footage is actively monitored. **A2.15** There is comprehensive and continuous CCTV coverage of the perimeter's fence line. Note: There should be 100% coverage of the perimeter including the access points as stated in 4.2.1 of the VSS. (If unsure, to view the CCTV coverage.)

A3) Security lighting	Security lighting increases visibility around perimeters, buildings, as well as sensitive locations and also serves as a deterrent and detection tool. It should therefore be installed 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 premises' security plan. Lighting, however, also needs to be matched to the operating environment and this should be taken into consideration during planning. 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.	**A3.16** The lighting is bright enough to allow the CCTV cameras to capture any movements. Note: For this, to ask the company to playback the recordings from past night (e.g. Playback the footage of what is recorded at 2am). **A3.17** All areas within the premises are well lit during the hours of darkness.
A4) 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	**A4.18** There is a guard post from where access into the premises is regulated for visitors.

	usually regarded as the weak links of the perimeter as they require a breach in the protective line every time they are opened. The control point where access to the facility is facilitated will be the guard post. This location should be always manned (i.e. warm body onsite) and/or whenever there is activity within the facility. Security posts are built when there is a security need to man a static location on the premises' perimeter line or at critical positions for long periods of time. The security post is meant to enhance the ability of the security guard to perform his duties by being well positioned and well equipped regardless of the weather or light conditions. It can also be used to improve his survivability in case of an attack aimed at breaching the perimeter of the premises. Security posts can be designed and built as part of the development or in certain situations, be bought as a ready-made product when only a small booth is required (usually at vehicle entrances). The challenge of designing an entry point is to prevent unauthorised access while maximising the flow of authorised access by pedestrians or vehicles.	Note: 24/7 manned (i.e. warm body onsite) guard posts are ideal. In the event the guard post is unmanned (i.e. inactivity period), the premise must be locked up. If there is any visitor during the unmanned period, staff must escort the visitor from the guard post.

	Visitors and contractors gaining access to the premises needs to exchange for a security pass from the guard post, prior to entry into the premises. All personnel and their belongings should be subjected to security checks before entering the premises. To deter and detect perpetrators from entering the premises screening has to be conducted at the entry point. Equipment such as X-Ray machines, Walk-Through Metal Detectors (WTMD), Handheld Explosive Detectors (HHED) "Sniffers", security checking tables and turnstile gates may be deployed to support screening operations. It is recommended to make provision for the additional loading and plan for space, as well as electricity and low voltage infrastructure in the relevant locations for future equipment. It is advisable to physically shield or separate the screening area from the inner lobby. The intent is to isolate the screening area and contain an attack should the perpetrators be discovered at the screening area. It is advisable to plan for a security standing point, room, or booth positioned in such a way as to give security personnel an unobstructed view of the entire entrance area. The purpose of the visit will be established before granting entry. On top of that, checks to	**A4.19** The visitors/contractors are required to produce an ID for verification and issuance of security passes. **A4.20** There are checks conducted on visitors and their belongings. **A4.21** The purpose of the visit is verified. **A4.22** The visitors are escorted from the guard post or counter onwards. **A4.23** The level of protection is the same across all vehicle/pedestrian gates on the perimeter line.

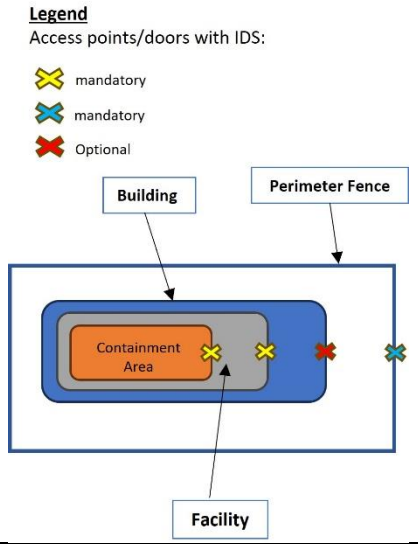
	verify identity of personnel entering the premises will also be determined using government issued photo identification, letter of appointment, etc. All visitors are escorted from the guard post and onwards into the premises, building or facility after they are cleared to enter.	

B) General Premises Security (Restricted Area)		
Area of Interest	**Description**	**Mandatory Measures**
B1) Access Control	This section focused on the identification and securing of cleared personnel who have already been granted permission to enter the premises. The primary component of a successful access control system is knowing who is allowed on-site. Before entering into the premises, all personnel should don the security passes.	**B1.24** The visitors are required to don their security passes when they are within the premises.
	All visitors and temporary contractors should be escorted at all times, after they are allowed entry into the boundary of the premises.	**B1.25** The visitors should be escorted at all times, when within the premises.
	Personnel identification measures help a company to quickly determine whether or not an individual is permitted access to a premises or a restricted area.	**B1.26** Access to restricted/critical areas are clearly demarcated. Examples: (a) Person holding (colour x) pass can only access into (colour x) zone but not others. (b) While colour zoning is good to have, zoning can be implemented by access-controlled passes for different areas.

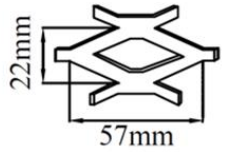
	Identification systems should be installed at access leading to the facility (i.e. storage area or critical area) so that there is proper control of authorised personnel gaining ingress to the area. Some examples of systems are as follows: (a) Access card system (b) Fingerprint verification system (c) Facial recognition Any mechanical lock is a security lock, and keys are to be kept by authorised personnel.	**B1.27** The access leading to the facility (storage/critical area) is controlled. (e.g. There is card reader installed on the doors leading to the facility. Note: To check if mechanical lock is a security lock and keys are being kept by authorised personnel. (To provide photos of the mechanical lockset.)
B2) Monitoring and detection	Monitoring and detection equipment are key components of effective premises security. Often, premises will be monitored 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. The specifications of the CCTV are listed in SPF VSS documents.	**B2.28** The premises within the company are monitored by CCTV cameras. **B2.29** All the doors and access points leading to the facility (storage/critical area) are monitored by CCTV cameras. **B2.30** The specifications of the CCTV cameras and its system comply to the SPF VSS Standard for Buildings. SPF VSS Standard for Building (extract) (i) The CCTV camera is an Internet Protocol (IP) Camera. (ii) All recordings are made at a minimum of 6 frames per second (fps) (for indoor) or 12 fps (for outdoor

		monitoring of slow-moving traffic e.g. along driveway) for each and every video image. The CCTV camera has the capability to record from selected or designated cameras in real time mode at 25 fps. *Accepted:* *Indoors – 6 fps* *Outdoors – 12 fps* *Recommended – 25 fps* (iii) The CCTV camera has a resolution of HD 1080p:1920x1080 pixels. (iv) The CCTV system has a minimum 31 days of archival. (v)The recorded picture quality is not reduced due to the image compression. (vi) the recorded images meet the minimum image height requirements of 'Observation', 'Recognition', 'Identification' and 'Detection' level stated in video surveillance system standard (VSS) for buildings Annex A. Note: To ask premises to send the CCTV specifications to PSWG through the NAs' POC.
	The security consoles/systems for the cameras should be housed in designated secured rooms accessible by only authorised personnel. The	**B2.31** (i) The CCTV consoles/systems are housed at secured environment, away from moisture and dust. Examples of

recordings should be kept in a secured environment, protected from excessive moisture and dust, with preventive measures against unauthorised access, removal or viewing of the recordings.	such environment will be the Guard house, security and control room etc. (ii) The CCTV consoles/systems are protected against unauthorised access.
The CCTV camera footage is actively monitored. Actively monitored means having access to CCTV live footages either at site 24/7 or having mobile access to the footages despite the location of the viewer. If mobile access to footage is the preferred option, companies should carry out the required risk assessment to minimize potential security risk (e.g. engaging a professional to ensure that suitable processes and measures are in place to safeguard data security concerns).	**B2.32** The CCTV camera footage is actively monitored.
Monitoring and detection equipment are key components of effective premises security. Often, facilities will be monitored 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.	**B2.33** IDS is installed on the doors and access points located immediately before the entrance (i.e. door) to the facility (storage/critical area). Some examples of IDS are: (a) Vibration detection sensors (b) Video motion detection (c) Infrared sensors (d) Acoustic sensors

		
	The alarm from the IDS, upon activation should send alert to two different individuals. An example of the notification may be via SMS to these two staffs. This is in case one of them is occupied and/or unable to respond.	**B2.34** The alarm from the IDS is sent to at least two separate personnel or to a 24/7 manned (i.e. warm body onsite) security room. (e.g. trigger an alert via SMS to the company's staff/security room).
B3) General security policy	Develop SOPs to identify suspicious indicators, incident reporting and response during contingencies. As a baseline guide, stakeholders can refer to the resources on SGSecure on suspicious indicators.	**B3.35** There is a set of Standard Operating Procedures (SOP) in place to identify suspicious indicators and report incidents to relevant staff and authorities. **B3.36** There is a SOP in place for contingency response and staff are familiar with it.

Part C - Storage Security		
Area of Interest	**Description**	**Mandatory Measures**
C1) Access Control	This is section focused on the identification and securing of cleared personnel who are authorised to enter the facility (storage/critical area). Example of access to the storage areas: (a) Electronic access measures • Tap card readers. • Biometric readers • Electronic Keypress • Open door detectors (magnetic switches) • Access control management software • Access control management stations (b) Manual access control measures with sign in and sign out procedures. • Regulated lock and key access.	**C1.37** The access into facility (storage/critical area) is controlled. (e.g. by card reader or lock and key with a sign in logbook). Note: To check if mechanical lock is a security lock and keys are kept by authorised personnel. **C1.38** Only authorised personnel are allowed access into the facility and there must be a system to ensure such access is updated regularly.
	Walls and partitions of the facility (storage/critical area) should be made up of solid materials and extended to true ceiling to prevent unauthorised access. Walls and partitions should offer	**C1.39** (i) The walls of the facility (storage/critical area) are made up of solid material (e.g. concrete/steel/bricks) and shall be extended to the true ceiling. Otherwise,

	resistance and able to provide evidence of unauthorised entries into the facility (storage/critical area). Otherwise, the gap should be closed with expanded wire mesh to be extended to the true ceiling. Openings such as ventilation shafts, windows, etc, at the facility (storage /critical area) should be secured using fixtures such as grills to prevent entry of people or foreign objects. It is common to protect windows against forced entry by adding steel grilles. Although it may not be aesthetically pleasing, they are a cost-effective solution that provides protection when the window is open. The grille including its connection details should be designed in accordance with the forced entry standards.	the gap should be closed with 5mm expanded wire mesh with aperture size of maximum height about 22mm and maximum length 57mm) to be extended to the true ceiling. (ii) There are no unsecured openings (i.e. windows/door panels) at the facility (storage/critical area). (e.g. openings should be secured with grilles and wire mesh). Note: Any opening of more than 620 cm2 in area and over 150mm in its smallest dimension needs to be secured with either 5mm expanded metal mesh of aperture size maximum height 22mm and maximum length 57mm; or rigid steel bars of 13mm diameter extending across the shorter dimension of the opening with maximum 150mm spacing. EXPANDED METAL MESH 
	The facility (storage/critical area) should be made up of a true ceiling to prevent attempts of forced entry and be secured in a manner that precludes removal without leaving evidence of tampering.	**C1.40** The ceiling of the facility (storage/critical area) is made up of a true ceiling (a solid, unmoveable, layer of material). Note: A false ceiling leading to true ceiling is acceptable.

	When the walls do not extend to the true ceiling and a false ceiling is created, the false ceiling should be reinforced with 18 gauge expanded metal mesh to serve as the true ceiling.	When the walls do not extend to the true ceiling and a false ceiling is created, the walls should be extended to the true ceiling with expanded wire mesh (See above).
C2) Monitoring and Detection ***For facility which have no control of perimeter security/general premises, they must adopt either Option 1: S/no 41 to 46(a) and 47 to 49 or Option 2: S/no 46 [including both (a) and (b)] to 49***	Monitoring and detection equipment are key components of effective facility (storage/critical area) security. Often, facilities will be monitored for security incidents through a combination of human oversight and one or more electronic sensors or other intrusion detection systems. Typically, when a sensor at the door to the facility (storage/critical area) detects an event of interest, an alarm will be triggered to notify the security personnel or assigned staff who will then assess the event directly at the location or remotely through surveillance images. The specifications of the CCTV are listed in SPF VSS documents. The alarm from the IDS at the facility (storage/critical area) upon activation should send alert to two different individuals. An example of the notification may be through SMS to these two staffs. This is in case one of them is occupied and/or unable to respond.	**C2.41** IDS is installed at the door(s) to the facility (storage/critical area). **C2.42** The alarm from the IDS is sent to at least 2 separate personnel or to a 24/7 manned (i.e. warm body onsite) security room. (e.g. trigger an alert via SMS to the company's staff/security room). **C2.43** The door(s) to the facility (storage/critical area) is monitored by CCTV cameras. **C2.44** The facility (storage/critical area) is monitored by CCTV cameras. **C2.45** There is comprehensive and continuous CCTV coverage at the exterior area and facing the door of the facility (storage/critical area). **C2.46**

	For a leased facility (i.e. only leasing the storage room with no control over the fence line and area leading up to the storage room), the CCTV cameras are to be equipped with video analytics which detects motion around the perimeter and areas facing the doors to the storage room for detection of unauthorised movements/activities. Any alert should be sent to at least 2 separate personnel. (e.g. trigger an alert via SMS to the company's staff).	There is comprehensive and continuous CCTV coverage directly at facility (storage/critical area) (e.g. storage cabinet like freezers.). Note: (a) There should be 100% CCTV coverage of SSM storage as stated in 4.2 of the SPF VSS Standard for Buildings. (If unsure, to view the CCTV footage). (b) For a leased facility (i.e. only leasing the storage room with no control over the fence line and area leading up to the storage room), the CCTV cameras are to be equipped with video analytics which detects motion around the perimeter and facing the doors to the storage room for detection of unauthorised movements/activities. Any alert should be sent to at least 2 separate personnel. (e.g. trigger an alert via SMS to the company's staff).
	The specifications of the CCTV are listed in SPF VSS documents.	**C2.47** The specifications of the CCTV cameras and its system comply to the SPF VSS Standard for Buildings. SPF VSS Standard for Building (extract) (i) The CCTV camera is an Internet Protocol (IP) Camera. (ii) All recordings are made at a minimum of 6 frames per second (fps) (for indoor) or 12 fps (for outdoor monitoring of slow-moving traffic e.g. along driveway) for each and every video image. The CCTV camera has

	the capability to record from selected or designated cameras in real time mode at 25 fps. *Accepted:* *Indoors – 6 fps* *Outdoors – 12 fps* *Recommended – 25 fps* (iii) The CCTV camera has a resolution of HD 1080p:1920x1080 pixels. (iv) The CCTV system has a minimum 31 days of archival. (v) The recorded picture quality is not reduced due to the image compression. (vi) the recorded images meet the minimum image height requirements of 'Observation', 'Recognition', 'Identification' and 'Detection' level stated in video surveillance system standard (VSS) for buildings Annex A. Note: To ask premises to send the CCTV specifications to PSWG through the NAs' POC.
The security consoles/systems for the cameras should be housed in designated secured rooms accessible by only authorised personnel. The recordings should be kept in a secured environment from excessive moisture and dust,	**C2.48** (i) The CCTV consoles/systems are housed at secured environment, away from moisture and dust. (ii) The CCTV consoles/systems are protected against unauthorised access.

	with preventive measures against unauthorised access, removal or viewing of the recordings.	
	The CCTV camera footage is actively monitored, i.e. live footages accessible on site on 24/7 basis or having mobile access to the footages if the viewer is at another location. If mobile access to footage is the preferred option, companies should carry out the required risk assessment to minimize potential security risk (e.g. engaging a professional to ensure that suitable processes and measures are in place to safeguard data security concerns).	**C2.49** The CCTV camera footage is actively monitored.
C3) Inventory Control	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.	**C3.50** The SSMs are kept in secured cabinets, e.g. freezers. **C3.51** The keys/access to the cabinets (or freezers) are managed securely. (e.g. within an electronic keypress) **C3.52**

	The access rights to the SSMs are to be managed securely, e.g., given to personnel on the need basis, documented or monitored. The keys to the room/cabinets storing SSM should be securely managed. An example will be with the use of an electronic keypress. Locations where the SSMs are kept should be secured all times, and access rights to the SSMs are to be given to the personnel on the need basis and to be documented or monitored to prevent misuse. The movement and utilisation of the SSMs should be monitored closely and properly recorded. Audit of SSMs inventory must be done regularly to ensure there is proper check and balance. If facilities are unable to conduct audit(s) once every 3 months and an annual inventory stock-take to ensure 100% accountability of SSMs, they must provide justifications and/or details of the processes in place for tracking SSM stocks, such as ensuring the integrity of seals on boxes. To prevent unauthorised access there must be proper disposal of security sensitive material, as advised by the NA.	The access rights to the SSMs are managed securely. (e.g. given to personnel on the need basis, documented or monitored) **C3.53** There is proper inventory recording of the SSM. (e.g. via record management system, where additions and usage are recorded clearly) **C3.54** Inventory audits are conducted quarterly for the SSMs, with a 100% accountability check (stock-taking) of the SSMs at least once a year. **C3.55** The expired and unsafe to use/store SSMs are disposed securely. (i.e. through an authorised/licensed disposal company as mandated by the NA). Note: The concerns here would be whether unauthorised personnel can obtain the materials from the disposal. To check with the NA POC if the disposal procedure has met their requirements.

C4) Quality Control and Processes	A designated person should be in-charge to manage any security incident (e.g. house breaking) that occur with the facility. He/she should always be contactable when there is a need to update any post incident matters to the authorities. In case of any occurrence of incidents involving safety and security, the police should be alerted immediately through the 999 hotline. The security measures should be at the same level of compliance throughout the day. There should not be an instance where the security measures are lowered during certain timings, e.g. at night due to inactivity. There should be regular maintenance of security systems, such as the VSS and Card Access System, to ensure that they are working at all times. Appropriate security measures should be employed when performing maintenance as the system may not be able to detect any incident during such times. Such measures should also be employed in response to non-routine outages, equipment failures and malfunctions, as these may be signs of adversary tampering with the security system.	**C4.56** There is a designated person who will manage any security incident (e.g. house breaking) that occur with the facility. **C4.57** There was no security related incident involving the SSM. **C4.58** The level of security measures is maintained at all times. **C4.59** There is maintenance conducted for the security system (e.g. CCTV cameras and Card Access System) to ensure that the systems are working. **C4.60** The staff are trained on their roles during a security incident (e.g. house breaking, theft of SSM).

	The staffs within the company should be trained on their roles during a security incident (e.g. house breaking, theft of SSM) and be vigilant to recall key details necessary for follow-up Police investigations.	