VIDEO SURVEILLANCE SYSTEM (VSS) STANDARD FOR BUILDINGS

Prepared by: **Singapore Police Force (SPF)**

With inputs from: **Ministry of Home Affairs Headquarters**

- **Joint Operations Department (JOD)**
- **Office of Chief Science and Technology Officer (OCSTO)**
- **InfoComm Technology Division (ICTD)**

Internal Security Department (ISD)

Version: **1.0**

Date: **5 November 2013**

Document Version History

Version	Date	Brief description of amendments and affected pages, paragraph
1.0	November 13	First Issue

Foreword

Video Surveillance System (VSS) is to support and enhance the overall management of a building's security. VSS facilities are an aid to security monitoring, especially of vulnerable or sensitive areas. The physical presence of VSS also provides assurance to the occupants that the building environment is under surveillance.

VSS also helps to act as an investigative tool as a post incident source of evidence, or may deter potential criminals/terrorists if they perceive that their actions being monitored. However, the VSS does not perform an active protective role and should not be designed to serve as the sole protective measure in a specified area, but must work in conjunction with other security measures (e.g. access control, alarm systems, etc.).

This VSS Standard has been developed to provide for a uniform and consistent approach to the recommended specification, installation, operation and performance of VSS across buildings in Singapore. However this VSS Standard is a set of recommendations for building owners and is not mandatory.

Given dynamic VSS market, these standards will not spell out specific technologies and capabilities within the system but relate to general concepts and design considerations that should be taken into account when developing a building's VSS. As there are many VSS options available in the market, it is recommended to employ a professional consultancy when designing VSS.

Table of Contents

1. Introduction

1.1. There are four key stages when planning the installation of a VSS. The first step is to define the problem, be it a security threat, public safety issue or other vulnerability. Consider at this point whether the installation of a VSS is the most appropriate response to these concerns, or if there are alternative options.

1.2. The second step is to define the requirements for the VSS through further defining the areas of concern, understanding operational issues and responses, deciding on the most suitable system requirements and identifying any managerial implications.

1.3. The third step is to detail down the technical specification for the VSS to be developed. And finally, after the system has been installed and commissioned, check is to be conducted to ensure the deployed VSS meets the operational requirements and that the performance is fit for purpose.

2. Scope

2.1. This Standard applies to VSS installations at different types of buildings included those that belong to hospitality and retail industries and government institutions.

3. VSS Requirements

3.1. Introduction

3.1.1. It is important to consider not only whether each VSS component is capable of meeting the operational requirements but also whether the components in conjunction with each other, and the system as a whole are able to meet the operational requirements. The various components, starting with the scene illumination and concluding with the replay and review of recordings, are to be considered.

3.2. Lighting

3.2.1. Introduction

3.2.1.1. Sufficient lighting is necessary for people to see and be seen. From a security point of view, lighting that is strategically placed can increase the effectiveness of VSS and guard work while reducing the chance of criminal acts occurring in the illuminated area. The basic level of lighting should allow the security

deployment (VSS and guards) to identify a human face from a distance of about 10 metres.

3.2.1.2. If the area is intended to be used during the hours of darkness, the lighting should provide adequate visibility for the intended night time operation. Pedestrian walkways, back lanes and access routes open to public areas should have a basic level of lighting. Inset spaces, signs, entrances and exits should be adequately lit so that the VSS coverage would provide a clear picture.

3.2.1.3. Security lighting is employed in order to increase the visibility around perimeter lines, buildings, and sensitive locations. It is a security management tool that is applicable in almost all environments within an urban development. Proper lighting can greatly improve the combined operation of other security systems, particularly VSS and other surveillance measures and therefore it must be designed to compliment these systems.

3.2.2. Design of Security Lighting

3.2.2.1. Lights located in vulnerable locations should be protected against vandalism by means of vandal resistant materials and design.

3.2.2.2. Lighting design should take into account the various current and future obstructions that may cause light to be blocked (e.g. various types of vegetation, such as trees).

3.2.2.3. Design proposal should take into account the possibility of night time outdoor activities and should specify the type, location and intensity of the various lighting elements that will be installed.

3.2.2.4. Lighting should be equally spread out, reducing contrast between shadows and lightened areas. It is recommended to use more fixtures with lower wattage rather than few fixtures with higher wattage. This will help to reduce the creation of deep shadows and will help avoid excessive glare.

3.2.2.5. Where possible, lighting fixtures should be located at heights that enable easy maintenance and replacement.

3.2.2.6. The lighting plan should locate areas that may be shadowed and light them up.

3.2.2.7. Lighting at manned entrances must be adequate to identify persons, examine credentials, inspect vehicles entering or departing the facility premises through designated control points, and prevent anyone from entering unobserved into the premises.

3.2.2.8. The lighting illuminating the building's entrance should allow for person identification during hours of darkness and extreme environmental conditions (e.g. heavy downpour).

3.2.2.9. Security posts at entrance points should have a reduced level of interior lighting to enable the security guards to see his surroundings while minimising the adversary's ability to look inside the posts.

3.2.2.10. The controls of the lighting systems should be positioned in a secured area, preferably in the security control room.

3.2.2.11. Lighting should be continuous and should be sufficient to support the VSS coverage. The light sources should be located within a short distance to the object to be monitored.

3.2.2.12. Cones of illumination should overlap to provide coverage in the event of bulb burnout.

3.2.2.13. Lighting should be arranged so as to create minimal shadows and minimal glare.

3.2.2.14. The preferred position for the light is above the camera. The camera should not view the scene through intense beams of light. Where possible, the light source should be a minimum of 2m from the camera.

3.2.2.15. Lighting should be turned on automatically by clock or photoelectric cell.

3.2.2.16. The building should be provided with adequate lighting 24/7 to ensure quality coloured images for facilitating investigation and prosecution are captured.

3.2.2.17. However in the event of low light level and floodlights may be considered as too intrusive, near infrared detection systems that are sensitive to 'light' beyond human vision can be used. These systems tend to produce black and white images at night; during the day their ability to render colour may be poor unless a supplementary infrared filter is part of the camera.

3.2.2.18. In the event of lighting failures, the VSS should be capable of producing images that will enable the evacuation of the building to be effectively managed under emergency lighting conditions.

3.2.2.19. Cameras installed outdoor should ensure that natural lighting (e.g. sun rise, sun set) and artificial lighting (e.g. floodlight, spotlight) do not blind the camera view. If required, polarizing filters may be fitted on the cameras.

3.2.2.20. In the event of lighting failures, cameras of importance should produce good images. These cameras should be installed near emergency lightings, and the

field of view of these cameras shall be adequately covered by additional emergency/ artificial lightings.

3.3. Camera

3.3.1. General

3.3.1.1. The system should consist of multiple colour cameras distributed throughout the building to give comprehensive coverage of all common areas[1].

3.3.1.2. The cameras should have a resolution of HD 1080p: 1920x1080 pixels or its equivalent.

3.3.1.3. The VSS cameras in public areas should be situated where they cannot easily be evaded, damaged or obscured and should be clearly visible to the public.

3.3.1.4. All cameras should provide colour images in order to maximise the scope for crime detection and to enable clear identification of offenders for prosecution.

3.3.1.5. Where headroom is restricted, such that sitting may obstruct public passage, cameras should be mounted in recesses so as to avoid the possibility of injury to customers and to protect the cameras from theft or damage.

3.3.1.6. All cameras required to meet “Core Requirements” (see clause 3.10) should be static and the cameras’ field of view should not be adjusted by non-authorized users.

3.3.1.7. For network IP-based VSS, it is recommended to ensure that compliance to Open Network Video Interface Forum (ONVIF) standards is supported. This is to ensure inter-operability when captured footages need to be viewed / processed on other platforms.

3.3.1.8. Cameras should be suitable for internal or external use (depending on location) and provide the specified quality of picture and view (see clause 3.10) in all weather, environmental conditions and temperatures.

3.3.2. Pan-Tilt-Zoom Cameras

3.3.2.1. As an alternative (or as a supplement) to using fixed-view cameras, it may be beneficial to use a camera with a Pan-Tilt-Zoom (PTZ) capability. This gives the security surveillance operator the ability to cover a wide area but also zoom in to focus on an incident wherever it occurs within the original field of view, providing

[1] These include general access locations such as main entrance lobbies, corridors, taxi stands, pavements, streets within the development’s boundary line.

greater detail and assisting with the identification of the subject. It can also be used to pan across a scene to track a target.

3.3.2.2. All PTZ cameras should have an option to allow the user to pre-determine the locations that he/she wants to monitor (i.e. preset locations), including the setting of a routine pattern, where necessary. The VSS should have a 'default settings' function, which allows the PTZ cameras to auto reset to their original position after pre-determined time duration.

3.3.3. Infra-Red Sensitive Cameras

3.3.3.1. As previously mentioned in Section 3.2.2, some situations may arise when pictures are required at night or in poorly lit areas and hence required an infrared sensitive camera (day/night camera).

3.3.3.2. It should be noted that infrared cameras will often provide poor colour rendition during the day and the addition of an infrared filter for daytime use will improve this. It is recommended that wherever possible ambient light levels are increased in preference to the use of infrared cameras.

3.3.4. Camera tamper protection / detection

3.3.4.1. The camera should be installed in such a way that it is difficult for an intruder to change the field of view of the camera. This should be achieved by installing at a suitable location/ height (minimum height of 2m from floor level) and any openings should be secured by security fixings. Furthermore, the interconnections (e.g. cabling, antennae) should not be accessible and/or able to be torn off.

3.3.5. The cameras should be housed in vandal-resistant and tamper-proof enclosures with non-reflective, shatter-resistant glass viewing ports.

3.4. Image Presentation

3.4.1. Display type

3.4.1.1. All monitors should be capable of displaying colour images and should possess appropriate adjustment controls (such as contrast, brightness, sharpness, and colour).

3.4.1.2. The displayed picture on monitors should at all times be sharply defined, stable, with accurate colour reproduction, and should be free of noise, interference, ghosting and pulsing effects. Aspect ratio of the displayed picture should be maintained with respect to the video source.

3.4.2. Real-time Surveillance

3.4.2.1. The VSS live images (feed) should be able to be monitored by operators in the Fire Command Centre (FCC) or within the VSS viewing facilities.

3.4.2.2. Within the FCC / VSS viewing facility, the operator should be able to select any camera picture for display on any monitor at any time or alternatively to set up a scanning sequence as desired. The dwell time of the scanning sequence should be adjustable.

3.4.2.3. The camera selection control system should allow rapid selection of any camera using minimum manual effort and be consistent across the VSS network.

3.4.2.4. In event of any incidents, each monitor within the FCC / VSS viewing facility should be able to view any camera within the building's VSS. The system should allow multi-view display on VSS monitors.

3.4.2.5. Any one user selecting a live image (feed) should not preclude other users selecting that live image (feed), or any other live images (feed) on the same system.

3.4.2.6. All camera pictures displayed on monitors should include a single superimposition showing the camera ID codes, date and time.

3.4.2.7. The numbering of cameras and the associated recording sequence should be carefully planned in order to facilitate both the rapid and seamless tracking of a targets' movement and the rapid retrieval of recorded images.

3.4.3. Resolution

3.4.3.1. Display resolution should be selected to match and complement the camera resolution and resultant video resolution.

3.4.3.2. The size and resolution of display screens should be considered together with the recommended display sizes. An operator seated at a far distance may not be able to discern the details of a small high resolution monitor.

3.4.3.3. Monitor sizes should be appropriate for the intended viewing distance within the viewing facilities. The viewing distance (VD) can be calculated with the following formula:

$$VD = \frac{DS}{\sqrt{\left(\frac{NHR}{NVR}\right)^2 + 1} \times CVR \times \tan\frac{1}{60}} \times \frac{2.54}{100}$$

Where:

VD: Viewing distance (in metres)
DS: Display's diagonal size (in inches)
NHR: Display's native horizontal resolution (in pixels)
NVR: Display's native vertical resolution (in pixels)
CVR: Vertical resolution of the video being displayed (in pixels)

3.4.3.4. **Table 1** shows a few examples of the distance.

Screen Size	Resolution of Display (in pixels)	Resolution of Video being displayed (in pixels)	Distance (m)
20"	1920 x 1080	1080	0.79
32"	1920 x 1080	1080	1.27

Table 1 – Resolutions

3.4.4. Number of camera images per operator

3.4.4.1. The exact number and presentation of VSS images, and subsequently monitors, required in each station-based VSS viewing facility should be determined by security, crime detection and prevention, and operational requirements.

3.4.4.2. Factors to be consider when agreeing the number of camera views to be presented to an operator may include:

- The risk associated with an event occurring and not being detected;
- The purpose of the observation;
- The type of activity and targets within the image;
- The expected frequency of incidents;
- How long an operator is likely to view an event for;
- Other tasks carried out by the operator; and
- The competence of the operator.

3.4.4.3. Performance evaluations should be periodically undertaken or where there is any significant change to the viewing task or control room setup.

3.5. Recording

3.5.1. Image Compression

3.5.1.1. Special or modified compression algorithms prevent the Police and the Courts having direct access to the recorded images without the use of proprietary software.

3.5.1.2. The System Integrator or vendor should propose standard codec to achieve optimal compression ratios while ensuring no or little loss of image/ video quality. The following is a list of acceptable standard format for compression. This is not an exhaustive list of acceptable formats, the formats below are presented as examples

of what level the compliance of a format should be defined, i.e. stating 'MPEG-4' alone is insufficient.

(i) H.264, "AVC (ISO/IEC 14496-10|ITU-T Rec. H.264)",
(ii) MPEG-4 part 2, ISO/IEC14496-2,
(iii) MPEG-2, ISO/IEC 13818-1;
(iv) H.263, ITU-T Rec H.263.

3.5.1.3. The video container format proposed for the recorded images should be limited to open-source container formats and/or common multi-media container formats such as *.avi (Microsoft), *.mov (Apple QuickTime) and *.mp4 (MPEG).

3.5.2. Frame Rates

3.5.2.1. On a day-to-day basis, all recordings should be made at a minimum of 6 fps (for indoor) or 12 fps (outdoor to monitor slow moving traffic e.g. along driveway) for each and every image. In addition, the capability to record from selected or designated cameras in real time mode at 25 frames per second would be useful.

3.5.2.2. For buildings that have minimum movement, in order to reduce the storage overhead, the building owner may consider using 'on the fly' method for recording.

3.5.2.3. In the 'on the fly' method, the recorded frame rate has two settings. The first being the base frame rate. This is generally low, often in the region of 1 to 6 fps. If the camera is triggered, the recording rate is increased to a faster rate, in the region of 12 to 25fps. The triggers can be external system elements, e.g. motion detection within the camera/VSS.

3.5.2.4. Alternatively, an automated decimation process may also be used. In this method, the footage is recorded at a high frame rate (as recommended in Clause 3.5.2.1) as the base level. After the 28 days of recording, the frame rate is automatically reduced by deleting frames at regular intervals. This will allow images of reduced quality to be retained for longer period of time for any subsequent retrieval requirement.

3.5.3. Resolution

3.5.3.1. The recording equipment should be able to record colour images of sufficient quality to assist in prosecution with the image quality meeting a resolution of HD 1080p: 1920x1080 pixels or its equivalent.

3.5.3.2. The recorded image should at all times be accurate, sharply defined and with accurate colour reproduction under normal lighting. For reduced lighting and emergency lighting conditions, the recorded image should minimally be an accurate and defined reproduction of the scene in monochrome.

3.5.4. Storage Capacity

3.5.4.1. Sufficient image recording capacity should be provided to enable both the continuous 24-hour recording of all VSS cameras, and the archival of at least one full set of 28 days recording and an additional minimum buffer of 10%.

3.5.4.2. In addition, sufficient reserve recording media (at least 20%) should also be kept in reserve to replace those seized by police/security agencies for post incident investigations. The recording media should be hot-swappable enabled.

3.5.4.3. In the event of hard disk failure, the system should be able to support minimally RAID 5 array. When the bad disk is replaced by a new one, the array is rebuilt while the system continues to operate normally.

3.5.4.4. A general equation is provided below to aid in estimating the total amount of storage required:

$$ASR = \left(\frac{Size \times fps \times C \times Hours \times 3{,}600}{1{,}000{,}000}\right) \times T_R$$

Where:

ASR:	Approximate Storage Requirement (in GB)
Size:	Image Size (in kB)
fps:	Frame per Second
C:	Number of cameras in the system
Hours:	Total number of operational hours in a 24 hour period
T_R:	Archival period (in days)

3.5.5. Basic Metadata

3.5.5.1. The image recording equipment should automatically record the camera ID of the camera being recorded and the date and time of the recording (synchronised to Global Positioning System (GPS) time). This information should always be displayed where it is least likely to obscure or interfere with the image of the main subject.

3.5.6. Playback

3.5.6.1. The recording equipment should have the features to include the capabilities of replay and normal play, still field, fast forward, rewind, record, stepping frame, visual search – forward & reverse, speed search and stop. It should also allow fast search by date/time slider and alarm.

3.5.6.2. The video footage should be suitable for immediate playback on media player software bundled within common computer operating systems (e.g. Windows

Media Player 11 and Microsoft) and/or other open-source media player software (e.g. VLC Player).

3.5.6.3. The system should have duplex capability or greater so as to allow simultaneous image recording, image export and playback. The system should be designed to enable the playback of footage without causing interruption to the recording process.

3.5.6.4. Each VSS should provide for the playback of any image from any camera recorded up to 28 days previous and in a controlled environment.

3.5.6.5. During playback, the system should also allow variable time-control for image selection.

3.5.7. Image export

3.5.7.1. Each VSS should have the ability to export any image from any camera up to 28 days previous.

3.5.7.2. The image exported should have no loss of individual frame quality, change of frame rate. There should be no duplication or loss of frames in the export process. The system should not apply any format conversion or further compression to the exported images, as this can reduce the usefulness of the content.

3.5.7.3. Any original metadata and/or authentication signatures should be exported with the images.

3.5.8. Replay of exported images

3.5.8.1. The System Integrator should provide viewer software to allow playback of the image/ video recordings made on the VSS. The viewer software should also be equipped with the capability to export recordings to open-source container and/or common multi-media container formats such as *.avi (Microsoft), *.mov (Apple QuickTime) and *.mp4 (MPEG) to facilitate investigation work. It shall also be capable of exporting still images in *.jpeg (JPEG File Interchange Format).

3.5.9. System tamper protection / detection

3.5.9.1. Storage facilities, including designated rooms, provided at FCC / VSS viewing facility should be capable of keeping the recordings in a secure environment protected from excessive moisture and dust, with preventative measures against unauthorized removal or viewing of the recordings. The location of the recording and storage facilities should be decided on a local risk assessment which takes into account security and crime-related risks, and should be sited in the inner perimeter of the building and away from vehicular access.

3.5.9.2. Anti-tampering measures to ensure court admissibility of recordings and audit logs captured, e.g. watermarking, crypto-hashing of video footage and/or ability to archive video to read-only media to prevent unauthorised alterations should be provided whenever possible.

3.5.9.3. An authentication mechanism is to be proposed by the System Integrator or vendor, to ensure the integrity of all recorded images (recordings) by allowing detection of any alteration or tampering made. This should include the recording of the camera ID and the date and time. It should be a function of the equipment set-up and should not be adjustable by the operator. The System Integrator or vendor should provide the necessary system/software for verifying the integrity of the recorded content.

3.6. Transmission

3.6.1. The network must have sufficient bandwidth to support the requirements of the VSS (e.g. in terms of the maximum number of concurrent feeds).

3.7. System

3.7.1. System Integration

3.7.1.1. If the same proprietor owns adjacent buildings, it is recommended for each building's VSS to include the capability of accessing images from adjacent locations as well.

3.7.1.2. The System Integrator should provide Software Development Kit (SDK) for commands including Select camera, View, Extract, PTZ and Playback.

3.7.1.3. A reserve viewing terminal should be catered for Emergency Response Agencies. This serves to facilitate incident management use.

3.7.1.4. The VSS should be designed and installed with a minimum of 20% spare capacity such that future expansion can be achieved.

3.7.1.5. Any additional capacity should be achieved with minimum disruption to the working system.

3.7.2. Signage

3.7.2.1. Notices strategically located around the building should be provided to inform the public that the VSS is being continuously monitored and recorded.

3.8. Power Source

3.8.1. Power source should be situated in a secured environment. Power cables running in public areas should be enclosed in metal conduits.

3.8.2. The VSS should feature an alert system for loss of power or image due to technical failure.

3.8.3. Uninterrupted Power Supply (UPS) with at least 30 minutes of backup capacity is to be provided for the VSS.

3.9. System Validation

3.9.1. System Commissioning

3.9.1.1. Upon successful hand-over of a fit for purpose system, a soft and hard copy of each of the agreed camera views and image quality (both monitor view and the recorded image) should be taken and reviewed by the building's Security Manager, to ensure that the field of view and image quality from each camera fit the building's security requirements.

3.9.2. System Maintenance

3.9.3. The VSS should be supported by a maintenance regime that ensures that the operational requirements defined in this standard are consistently met and the availability of all parts of the system is maximized. System availability should be set at 95% over a 12 month time frame.

3.9.4. The quality of the visual and the recorded images should be monitored and compared to a set of auditing standards, implemented by the building's Security Manager. Any deterioration should be rectified immediately.

3.9.5. All system fault rectifications should be rectified within 24 hours; or sooner if the faults results in serious loss of VSS coverage.

3.9.6. The building's Security Manager should also be responsible for auditing the correct implementation of the VSS to meet the operational requirements and identify any improvements (if necessary).

3.9.7. Audit trail should be provided to record all access to the recorders including every file retrieval transaction performed on the system.

3.10. Coverage of the VSS – Core Requirements

3.10.1. Common Areas

3.10.1.1. Comprehensive coverage throughout common areas is necessary to enable the monitoring of the flow of people, the identification and mitigation of potential overcrowding situations and the identification of undesirable, illegal or anti-social behaviour.

3.10.1.2. All general access areas such as main entrance lobbies, street areas, pavements, car parks and vehicle boarding and alighting points such as taxi stands and bus stops within the development's boundaries, should be equipped with sufficient cameras to provide a comprehensive coverage of the area.

3.10.1.3. For hotel premises, common areas coverage should include the lobby, front desk, concierge, entrance/exit points and corridors. For coverage of concierge, see clause 3.10.4.

3.10.1.4. General coverage of the common areas should meet a minimum image height of 'Observation' level (see guidelines as outlined in clause 5.1).

3.10.1.5. The positions of the cameras should be carefully planned and located to provide the comprehensive coverage with the minimum number of cameras. Account should be taken of the effect that periods of maximum human density may have on the achievement of the operational requirement.

3.10.2. Entrances & Exits

3.10.2.1. There should be sufficient cameras to provide comprehensive coverage of all external public access doors, emergency exits and vehicle entrances/exits (e.g. at the gantry points of car parks). The cameras should be mounted at a suitable height (e.g. where they cannot be evaded, damaged or obscured) – looking towards, rather than down at the doorway or driver.

3.10.2.2. Frontal view of people entering/exiting the building's premises via main entrances/exits, should meet a minimum image height of 'Identification' level (see guidelines as outline in clause 5.1).

3.10.2.3. Frontal view of people entering /exiting the building's premises via entry/exit points along passageways, walkway or MRT stations, should meet a minimum image height of 'Observation' level.

3.10.2.4. There should be coverage of the frontal views in both directions of every emergency exit. The entrances to the emergency exit escape routes should also be

covered by cameras in the public areas. General views of these emergency exits should meet a minimum image height of 'Observation' level.

3.10.2.5. Cameras deployed at the vehicle entrances/exits (e.g. at the gantry points of car parks) should capture the number plates of the vehicles entering/exiting the car park and loading/unloading bay and should be identified by the number plate identification.

3.10.3. Lifts / Staircases

3.10.3.1. For lifts which act as alternate entry and exit points to the building, frontal view of the lift doors for people entering the building and general views of the associated lift lobby areas are to be monitored at a minimum image height of 'Observation' level (see guidelines as outline in clause 5.1).

3.10.3.2. For staircases which act as alternate entry and exit points to the building, frontal view of people entering the building and general views of the associated staircase areas are to be monitored at a minimum image height of 'Observation' level (see guidelines as outline in clause 5.1).

3.10.4. Counters

3.10.4.1. For locations that involve security checks or registration before people are granted permission to proceed further into the building like checkpoints and ticket issuance counters, frontal view of people should meet a minimum image height of 'Recognition' level (see guidelines as outline in clause 5.1).

3.10.5. Sensitive Rooms[2]

3.10.5.1. Coverage of the external area outside the door of the sensitive rooms is to be provided. General views of the external access area of the doors should meet a minimum image height of 'Observation' level (see guidelines as outline in clause 5.1).

3.10.5.2. For each door fitted with an intrusion alarm, upon activation of the alarm, it would trigger the display of the image of the relevant camera(s) automatically on the designated VSS viewing facility monitor. General views of the doors should meet a minimum image height of 'Identification' level.

3.10.6. Critical Areas

3.10.6.1. Coverage of the external area outside the access doors to critical areas such as air intake vents and rooftops is to be provided. General views of the external

[2] Sensitive rooms can be defined as rooms that house important or critical equipment for the recording of CCTV images, e.g. NVRs.

access area of the doors should meet a minimum height of 'Observation' level while general views of the doors should meet a minimum image height of "Identification' level.

3.10.7. Summary of Core Requirements

3.10.7.1. The below table communicates target image height requirements to a height of 2m from floor level. **Table 2** is a summary of the requirements from "Core Requirements" (clause 3.10).

Location	Defined Areas	Detect	Observe	Recognise	Identify
Common Areas	Extensive Coverage of Common Areas (e.g. main entrance lobby).		√		
	Street Areas within Building's Boundaries (including pavements, walkways).		√		
	Vehicle boarding and alighting points (including taxi stand & bus stop).		√		
	Car Park – Parking areas.		√		
Entrances & Exits	Frontal view of people entering the building's premises via main entrances / exits.				√
	Vehicle description and number plate to be captured at vehicle entrances / exits / loading and unloading bay.				√
	Entrances / Exits (along passageways, walkways & MRT stations) leading to the concourse area.		√		
	Both directions of Emergency Exits		√		
Lifts	Frontal view of the lift doors for people entering the building premises		√		
	General views of the associated lift lobby areas.		√		
Staircases	Frontal view of people entering the building premises		√		
	General views of the associated staircase lobby areas.		√		
Counters	Frontal view of people registering at counter			√	
Sensitive Areas	External view of access for enclosed area		√		
	Intrusion-alarm triggered image viewing on security monitors when enclosed area is breached				√
	100% coverage of open areas		√		

Critical Areas	External view of access to critical areas		√		
	Frontal view of people entering the critical areas				√

Table 2 – Summary of Recommendations for Key Areas

4. Training of VSS Operating Staff

4.1. The VSS operating staff should undergo the appropriate training as stipulated by the building's Security Manager. They should be taught what to look out for and be able to react when a potential incident occurs, to monitor the event accurately and not lose information that could be pertinent to any future investigations.

4.2. The shift patterns adopted for the VSS operating staff should include sufficient breaks to ensure health and productivity of the staff.

4.3. It would also be beneficial to have Standard Operating Procedures (SOPs) in place for reference and to conduct regular refreshers to ensure that the VSS operating staff are familiar with the SOPs.

5. Supporting Information

5.1. Categories of Fields of View

5.1.1. Fields of view required by the VSS operating staff are described by four categories of view as follows:

(a) **Detect**: A figure occupies at least 10% of the available screen height and the scene portrayed is not unduly cluttered. Following an alert an observer can, after a search, ascertain with a high degree of certainty whether or not a person is visible in the pictures displayed to him (or more than 40mm per pixel);

(b) **Observe**: A figure should occupy between 25% and 30% of the screen height. At this scale, some characteristic details of the individual, such as distinctive clothing, can be seen, whilst the view remains sufficiently wide to allow some activity surrounding an incident to be monitored (or more than 16mm per pixel);

(c) **Recognise**: When the figure occupies at least 50% of screen height, viewers can say with a high degree of certainty whether or not an individual shown is the same as someone they have seen before (or more than 8mm per pixel);

(d) **Identify**: With the figure now occupying at least 120% of screen height, picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt (or more than 4mm per pixel).

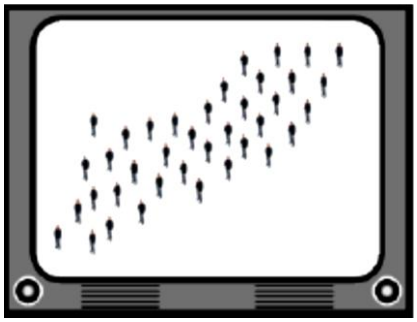
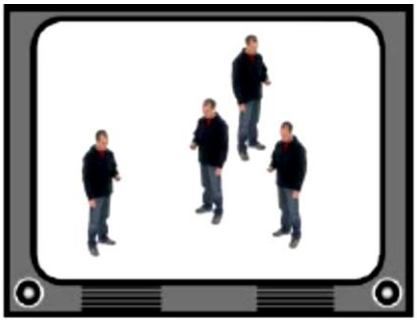
Detect	Observe
	
10%	25%
Recognise	Identify
	
50%	120%

Figure 1 – Height based 'Level of Detail' for the more commonly used screen heights

5.1.2. It should be noted at this point that when these guidelines were first developed, the systems all made use of the common fully analogue PAL system with a fixed resolution of 576 lines for video capture and display. Since the influx of digital systems to the VSS market, there is now variability in the capture, recording and display resolution.

5.1.3. So a 'Recognise' requirement can no longer be simply equated to a 50% screen height. For instance, through the use of megapixel cameras and high resolution displays it is now possible to provide the same image resolution as before using a much smaller physical percentage of the screen.

5.1.4. Conversion tables have therefore been devised to show how the traditional percentage screen height criteria for a PAL system will look under a range of non-PAL resolutions.

5.1.5. **Table 3** shows the resolutions commonly encountered and **Table 4** shows the equivalent screen heights needed to maintain the required resolution. These figures should be used only as a guideline to the proportion of the screen filled by the target as other factors such as lighting and angle of view, will also have an influence.

Table 3 – Commonly encountered resolutions

	PAL	1080p	720p	WSVGA	SVGA	4CIF	VGA	2CIF	CIF	QCIF
Height	400	1080	720	600	600	576	480	288	288	144
Width	720	1920	1280	1024	800	704	640	704	352	176

Table 4 – Equivalent percentage screen heights for different digital resolutions

Category	PAL	1080p	720p	WSVGA	SVGA	4CIF	VGA	2CIF	CIF	QCIF
Identify	120	45	67	80	80	84	100	167	167	334
Recognise	50	20	30	35	35	35	45	70	70	150
Observe	25	10	15	20	20	20	25	35	35	70
Detect	10	10	10	10	10	10	10	15	15	30

5.1.6. It should be noted that the resolution being compared reflects the lowest resolution in the chain and not necessarily the display screen resolution. The person imaged is of average height (1.64m to 1.76m).

5.1.7. It is important to examine the recorded picture quality to ensure that the picture quality is not reduced due to the image compression technology as the compression process will lead to a loss in picture detail.

6. References

Video Surveillance System (VSS) – Standard for Mass Rapid Transit (MRT) Stations (Version 3.0, dated 2006)

CCTV Guidelines for Police Establishment (Version 4.0, dated Sept 2010)

CCTV Operational Requirements Manual – Home Office Scientific Development Branch (Version 5.0, dated Apr 2009)

7. Abbreviations

FCC	-	Fire Command Centre
fps	-	Frames per second
GPS	-	Global Positioning System
NVR	-	Network Video Recorder
OR	-	Operational Requirements
PTZ	-	Pan-Tilt-Zoom
SDK	-	Software Development Kit
SOP	-	Standard Operating Procedure

UPS	-	Uninterrupted Power Supply
VSS	-	Video Surveillance System