# VIDEO SURVEILLANCE SYSTEM STANDARD

## FOR BUILDINGS

Version: 2.0

Date: March 2022

**Prepared by:**
Singapore Police Force

**With inputs from:**
Ministry of Home Affairs
Home Team Science and Technology Agency

# Document Version History

| Version | Date | Brief description of amendments and affected contents |
|---|---|---|
| 1.0 | November 2013 | First Issue |
| 2.0 | March 2022 | Second Issue<br><br>1. Added new sections on video analytics, firmware management, critical areas and cybersecurity.<br><br>2. Specific updates relating to security lighting, camera requirements, video compression ratios, storage capacity, system integration, power source and coverage for common areas. |

# Foreword

The Video Surveillance System (VSS) Standard for Buildings is intended to support the adoption of VSS to enhance the overall management of a building's safety and security.

Cameras at strategic locations throughout the building and its perimeter can help building owners to detect anomalies early, respond effectively against possible security threats and crime, and coordinate resources during business contingency. VSS also helps to act as a tool supporting post-incident investigations and providing evidence. However, the VSS does not perform an active role in protective security and should not be designed to serve as the sole protective measure in a specified area, but operate in conjunction with other security measures such as access control, intrusion detection alarm systems, fence intrusion detection systems, security responses etc.

This VSS Standard is a set of recommendations to guide building owners and help provide a consistent approach to the recommended specifications, installation, and operation of VSS across buildings in Singapore.

Given the dynamic nature of VSS industry, this guide focuses on good design and operational considerations, and may not spell out all specific technologies and capabilities within the VSS. As there are many VSS options available in the market, building owners should consider engaging the services of a security consultant when designing a comprehensive VSS.

# Table of Content

# Table of Content

# 1. Introduction

There are four key stages when planning the installation of a VSS: defining the problem, requirements, technical specifications and system commissioning.

a) The first stage 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 address these concerns, or if there are alternative options.

b) The second stage is to define the requirements for the VSS by understanding areas of concern, as well as operational issues and responses, before deciding on the suitable system requirements and identifying any managerial implications.

c) The third stage is to detail down the technical specifications for the VSS to be developed.

d) And finally, the building owner should verify that the deployed VSS meets the operational requirements, and that the performance is fit for purpose after the system has been installed and commissioned.

# 2. Scope

This Standard applies to VSS installations at various types of facilities and buildings including those in the hospitality and retail industries; and government institutions.

# 3. VSS Requirements

## 3.1 Introduction

The purpose of VSS is to capture video images, handle the images, and display them to the operator with adequate information to detect anomalies, support real-time operations and post-incident investigations involving safety and security incidents.

It is important to consider whether each VSS component can meet the operational requirements, the components can function in conjunction with one another, and the VSS, as a whole, is able to meet the operational requirements. These various components, starting with the security lighting system, CCTV cameras, communication linkages, network, image display and recording equipment should be considered as well.

## 3.2 Lighting

### 3.2.1 Overview

Sufficient lighting is necessary for people to see and be seen. From a safety and security perspective, lighting that is strategically placed can improve the effectiveness of VSS and security patrols while acting as good deterrence to reduce the chance of criminal acts occurring in well illuminated area.

Good lighting levels will improve the visibility around the buildings, perimeter lines, and sensitive locations. 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 also be adequately lit so that the VSS can provide a good picture quality.

Security lighting is a security management tool that is applicable in almost all environment within urban developments. Requirements should be identified early so that security illumination could be designed and implemented in the desired areas to obtain the best image quality under all operating conditions.

## 3.2.2 Design of Security Lighting

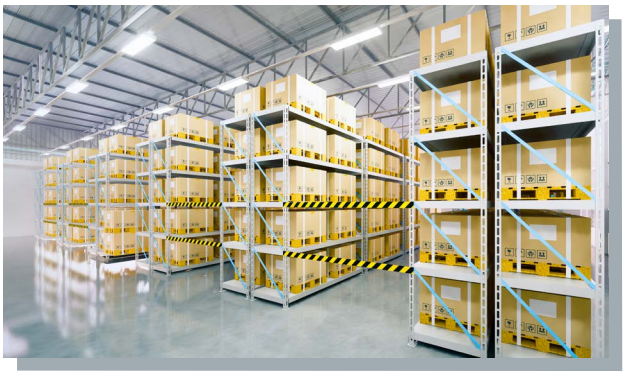
While architectural lighting design for physical infrastructures focuses on aesthetic appeal, ergonomic aspect and energy efficiency, security lightings focus on three key design considerations: glare reduction, selection of light source and preventive measures against tempering and sabotage.

Although adequate lightings around a physical building, perimeter fence and sensitive locations will deter potential intrusion, the lighting should be designed carefully as poorly deployed lightings could result in glare, hinder vision and poor image quality. With the appropriate light fixtures, lightings should be directed downwards to facilitate security operations.

Optimal lighting conditions provides visual comfort for the security guards performing security related activities in the facility and security inspection zones. Good illumination of the facility enables them to perform their visual tasks speedily and accurately.

Security lightings may be subjected to tampering or sabotage, possibly to reduce its effectiveness before an intrusion attempt. Hence, security lightings should either be mounted very high, or protected by vandal resistant materials and designs such as wire mesh or tough polycarbonate casing. Higher risk installations will require a stand-by power supply for their security lightings.

Where possible, lighting fixtures should be located at heights that enable easy maintenance and replacement. The controls of the lighting systems should also be positioned in a secured area, preferably in the security control room.



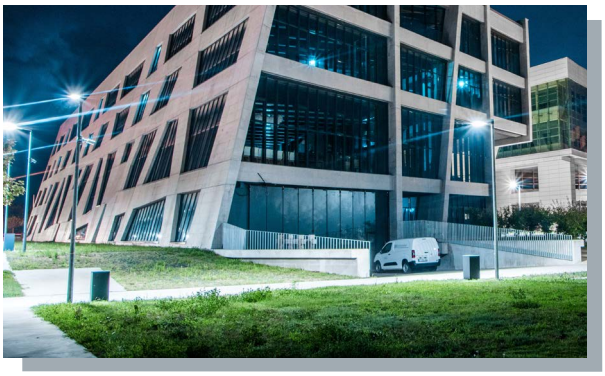


*Figure 1 and 2: Examples of well-lighted environment*

# 3.3 Camera

## 3.3.1 General

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


*Figure 3: Summary of key elements of a CCTV camera*

The cameras should have a minimum resolution of HD 1080p: 1920x1080 pixels (or its equivalent) and true wide dynamic range (WDR) capable of capturing coloured images in challenging imaging conditions, i.e. harsh lighting and darkness.

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.

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

All cameras required to meet “Coverage Requirements” (see Clause 4.2) should be static and the cameras’ field of view (FOV) should not be adjusted by non-authorised users. The FOV should remain clear and unobstructed from obstructions such as temporary/permanent structures, vegetation, and anti-climb features of the perimeter fences.

Network IP-based VSS should comply with prevailing Open Network Video Interface Forum (ONVIF) standards or its equivalent to ensure effective interoperability with IP-based physical security products, i.e. captured CCTV footages could be viewed / processed on compatible platforms.

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

---

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

## 3.3.2 Pan-Tilt-Zoom (PTZ) Cameras

PTZ cameras are cameras capable of remote directional (pan, tilt) and zoom control. This allows the operator to monitor a larger area by remotely directing and focusing the camera view to zoom in on an ongoing incident. PTZ cameras may not be suitable for ingress and egress points as the cameras may be moved away from their intended coverage intentionally or unintentionally.

All PTZ cameras should have an option to allow the user to pre-determine the schedule and locations that he/she wants to monitor (i.e. preset locations), including the setting of a routine pattern and dwell time of preset sequence, 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.

PTZ cameras should be able to pan or tilt quickly to capture fast moving targets whenever suspicious activities are detected.

*Figure 4 and 5: Examples of Pan-Tilt-Zoom cameras*

## 3.3.3 Infra-Red Sensitive Cameras

Infrared (IR) sensitive cameras with built-in IR illuminators can improve low light images without adding visible light in poorly lit areas.

As IR cameras would often provide poor colour rendition during the day, the addition of an IR filter for daytime use will improve image quality. It is recommended that ambient light levels be increased in preference to the use of IR cameras.

### 3.3.4 Camera Tamper Protection/ Detection

The camera should be installed in such a way that it is difficult for an intruder to tamper or change the field of view of the camera. This could be achieved by securing cameras at a suitable location or height (minimum height of 2 metres from floor level) and any openings should be properly secured with security fixings. The interconnections, including cabling and antennae, should be secured and not accessible to public.

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

The outdoor cameras should minimally meet the requirement for ingress protection codes IP65[2] if these cameras are exposed to adverse weather conditions.

## 3.4 Image Presentation

### 3.4.1 Display Type

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

The displayed picture in the monitors should be sharply defined, stable with accurate colour reproduction, and should be free of noise, interference, ghosting and pulsing effects at all times. Aspect ratio of the displayed picture should be maintained to minimise any distortion to recorded video.

*2 The ingress protection code (IP Code) IP 65 ratings for CCTV camera enclosures ensures that the enclosures are "dust tight" and water resistant.*

## 3.4.2 Real-Time Surveillance

The VSS live images (video feed) should be monitored by operators in the Security Control Room (SCR), Fire Command Centre (FCC) or other locations (VSS viewing facilities) in the building.

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

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

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

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.

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

To facilitate general surveillance of building's safety and security and incident management, the labelling and numbering of cameras, and the associated recording sequence should be carefully planned to facilitate the rapid retrieval of recorded images.

## 3.4.3 Resolution

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.

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:

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

*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)*

Viewing distance is the greatest distance between the operator and monitor while still perceiving all the details at the specified video resolutions.

| Screen Size (inch) | Resolution of Display (pixel) | Resolution of Video Displayed (pixel) | Viewing Distance (metre) |
|---|---|---|---|
| 20 | 1920 x 1080 | 1080p | 0.79 |
| 32 | 1920 x 1080 | 1080p | 1.27 |
| 42 | 1920 x 1080 | 1080p | 1.67 |

*Table 1 – Resolutions and viewing distances*

## 3.4.4 Number of Camera Images Per Operator

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.

Factors to be considered when determining the number of camera views to be presented to an operator:

a) The risk associated with an event occurring and not being detected,
b) The purpose of the observations,
c) The type of activity and targets within the image,
d) The expected frequency of incidents,
e) How long an operator is likely to view an event,
f) Other tasks carried out by the operator, and
g) The competence level of the operator.

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

## 3.4.5 Video Analytics

Video analytics (VA) is an important tool for detecting unauthorised intrusion in the building and suspicious activities near the perimeter, especially when a single operator is required to monitor many cameras. Common rule-based violations could be programmed for each scene of interest to alert the operator on the security events such as intrusions over a virtual tripwire, suspicious persons or vehicles loitering in a prohibited area, unattended objects, and dealing with an emergency. Building owners could refer to Singapore Standards Technical Reference TR 69:2019 for details on deployment of VA.

# 3.5 Recording

## 3.5.1 Image Compression

The System Integrator or vendor should propose standard codec to achieve optimal compression ratios while ensuring no or little loss of video quality, i.e. do not use special or modified compression algorithms. The following list shows the commonly accepted standard compression formats (non-exhaustive):

a) H.265, “HVEC (ISO/IEC 23008-2 | ITU-T Rec. H.265)”,
b) H.264, “AVC (ISO/IEC 14496-10 | ITU-T Rec. H.264)”, and
c) MPEG-4 part 2, ISO/IEC14496-2.

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

Video frame rate is an important CCTV design parameter that affects video transmission, storage, and display. On a day-to-day basis, all recordings should be 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. In addition, the capability to record from selected or designated cameras in real time mode at 25 fps would be useful.

To reduce the storage overhead, the building owner may consider ‘on the fly’ recording method when there are minimum movement in area within specified time period in the building.

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 fps to 6 fps. If the camera is triggered, the recording rate is increased to a faster rate, in the region of 12 fps to 25 fps. The triggers can be external system elements, e.g. motion detection within the camera.

Alternatively, an automated decimation process may also be used. In this method, the footage is recorded at a high frame rate (minimally 25 fps) as the base level. After 31 days of recording, the frame rate is automatically reduced by deleting frames at regular intervals subject to archival requirements. This will allow images of reduced quality to be retained for a longer period of time to support subsequent retrieval(s).

## 3.5.3 Resolution

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

The recorded image should at all times be sharply defined and with accurate colour reproduction under normal lighting. For reduced lighting and emergency lighting conditions, the recorded image should continue to be sharply defined in monochrome.

*Figure 6: Example of coloured HD CCTV images*

## 3.5.4 Storage Capacity

Sufficient image recording capacity should be provided to enable the continuous 24-hour recording of all VSS cameras, and the archival of one full set of recordings for the past 31 days or more.

In addition, sufficient reserve recording media (at least 20%) should be allowed and be hot-swappable enabled.

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.

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

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

| | |
|---|---|
| *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)* |

As most modern IP cameras are equipped with edge redundancy recording capability, such as onboard storage with SD cards, building owners should consider edge storage options to ensure that the video recording will not be interrupted during network equipment failures. The NVR should be configured to automatically retrieve the loss of recording once the network has recovered.

### 3.5.5 Metadata

The image recording equipment should automatically record the camera ID of the camera being recorded, date and time of the recording (synchronised to Global Positioning System (GPS) time). This information should always be displayed on the viewing terminal where it is least likely to obscure or interfere with the image of the main subject. Building owner may record useful metadata generated by advanced VSS.

### 3.5.6 Playback

The recording equipment should have 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.

The video footage should be suitable for immediate playback on media player software bundled within common computer operating systems and/or other commonly used open-source media player software (e.g. VLC Player).

The system should have duplex capability or greater 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.

Each VSS should provide for the playback of any image from any camera recorded from the past 31 days or more in a controlled environment.

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

### 3.5.7 Image Export

Each VSS should have the ability to export any image in any of its cameras from the past 31 days or more.

The image exported should not have any loss of individual frame quality or change of frame rate. There should also be no duplication or loss of frames after the export process. The system should not apply any format conversion or further compression to the exported images to avoid cascaded compression that would reduce the integrity and usefulness of the content.

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

## 3.5.8 Replay of Exported Images

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) so that users can easily view exported video and facilitate investigation work. It should also be capable of exporting still images in *.jpeg (JPEG File Interchange Format).

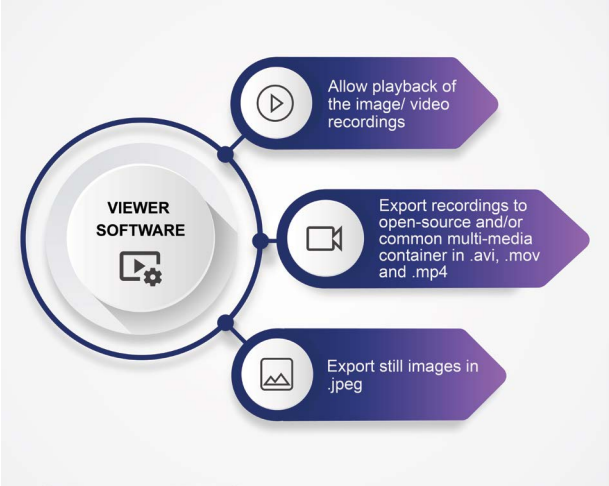



*Figure 7: Functions of System Intergrator viewer software*

## 3.5.9 System Tamper Detection and Protection

Storage facilities, including designated rooms, provided at VSS viewing facility 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. 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.

Anti-tampering measures should be implemented to prevent unauthorised alterations and protect the integrity of recordings and audit logs, e.g. watermarking, crypto-hashing of video footage and/ or ability to archive video to read-only media.

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

The network must have sufficient bandwidth to support the requirements of the VSS (e.g. maximum number of concurrent feeds for recording, display and video analytical purposes).

Redundancy in the form of automatic failover could be considered for the VSS networks and servers. The failover should be designed to protect against any loss of data during the transition phase. In sensitive and critical areas, alternate CCTV cameras could be connected to different networks to mitigate possible risk of network transmission failures.

## 3.7 Power Source

The power requirements for each component of the VSS should be determined. Power source and its ancillary equipment should be situated in a secured environment. The power cables running in public areas should also be enclosed in metal conduits.

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

Uninterrupted Power Supply (UPS) with at least 30 minutes of backup capacity shall be provided for the VSS such as VMS, NVR systems and viewing terminals. This is to allow the system to continue to operate while the backup power from generator kicks in; and to allow the VMS to properly shut down during prolonged power outage or when the facility does not have a backup power generator, so as to preserve the integrity of video images.

## 3.8 System Integration, Commissioning and Maintenance

### 3.8.1 System Integration

Newly designed CCTV systems have an advantage over existing systems as they can be designed to be integrated with the latest IP security systems such as video analytics, intrusion detection and access control systems.

Integrated security systems could augment security operations by notifying the security officers when security alarm is triggered, providing the location of the alarm on a site plan and displaying the specified camera view for verification purpose.

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.

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

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

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

Any expansion in capacity should be achieved with minimum disruption to the working system.

### 3.8.2 System Commissioning

When the VSS is commissioned and operational, the agreed camera views and image quality for both the monitor view and recorded image should be properly documented and reviewed periodically by the building owner.

### 3.8.3 System Maintenance

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

The building's Security Manager should be responsible for the proper implementation of the VSS to meet the operational requirements. This includes the conduct of regular audits to ensure storage duration, alarms and quality of the VSS' visual and recorded images comply with a set of auditing standards. Any deterioration should be rectified immediately as degradation of VSS performance would result in security gaps.

As smart cameras become more common, it is important to update the firmware of all components within the VSS regularly to minimise application security vulnerabilities.

All system and equipment fault should be rectified within 24 hours, or sooner if the fault results in serious loss of VSS coverage.

Audit trail should be provided to record all physical and network access to the VSS' recorders, e.g. file retrieval transaction performed on the system.

# 4. Coverage of VSS

## 4.1 Fields of View

Fields of view required by the VSS operators 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).

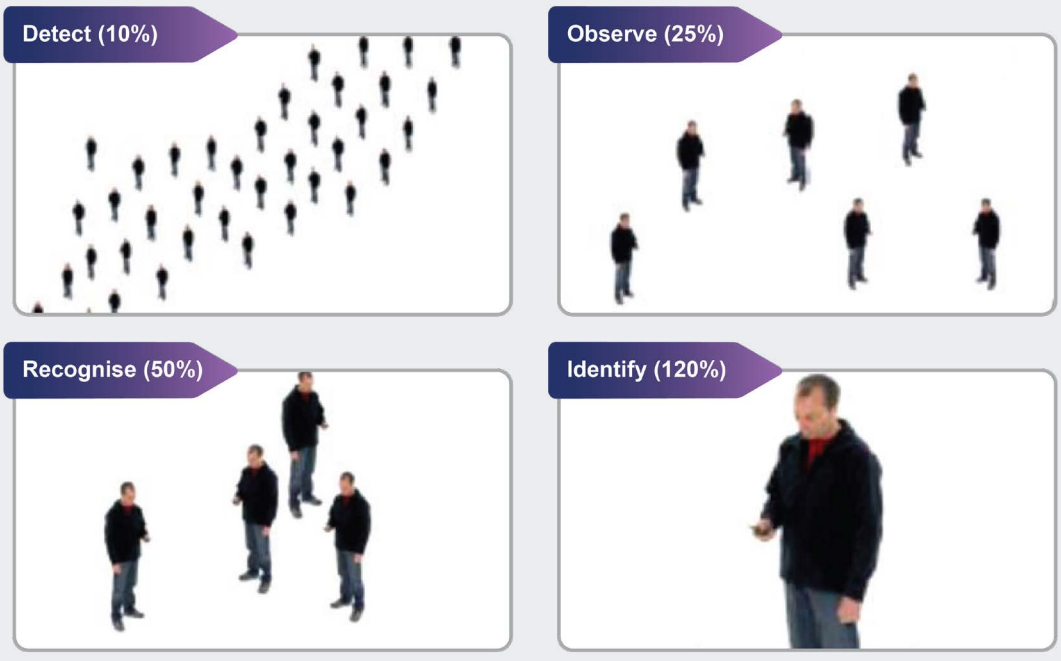



*Figure 8 – Height based 'Level of Detail' for the more commonly used screen heights*

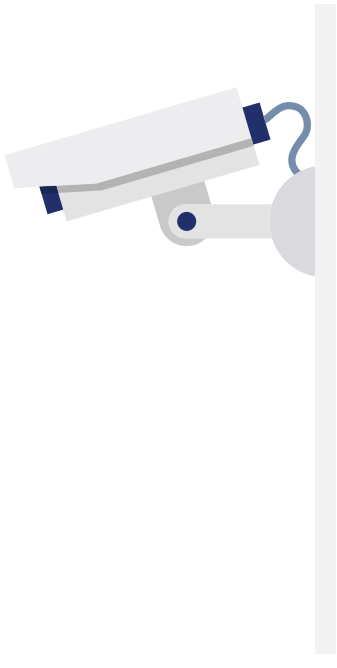
It should be noted at this point that when these guidelines were first developed, the systems all made use of the common fully analogue PAL system with a fixed resolution of 576 lines for video capture and display. Since the influx of digital systems to the VSS market, we have more options to capture,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

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.

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. Table 2 shows the resolutions commonly encountered and Table 3 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 on image quality.

| | 4CIF | PAL | 1080p |
|---|---|---|---|
| **Height** | 576 | 400 | 1080 |
| **Width** | 704 | 720 | 1920 |

*Table 2 – Commonly encountered resolutions (in pixels)*



| Category | 4CIF | PAL | 1080p |
|---|---|---|---|
| **Identify** | 84 | 120 | 45 |
| **Recognise** | 35 | 50 | 20 |
| **Observe** | 20 | 25 | 10 |
| **Detect** | 10 | 10 | 10 |

*Table 3 – Equivalent percentage screen heights for different digital resolutions*

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).

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.

# 4.2 Coverage Requirements

## 4.2.1 Common Areas

Comprehensive coverage throughout common areas is necessary to enable the directing of human traffic flow, the monitoring of potential overcrowding situations, and the detection of undesirable or anti-social behaviour and illegal access into and within the building.

All general access areas such as main entrance lobbies, street areas, pavements, car parks, loading/unloading bays 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.

For hotel premises, common areas coverage should include the lobby, front desk, concierge, entrance/exit points and corridors. For coverage of concierge, see Clause 4.2.4.

For fenced establishments, there should be comprehensive and continuous coverage of the perimeter's fence line.

General coverage of the common areas should meet a minimum image height of 'Observation' level.

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.

*Figure 9 and 10: Examples of common areas (lobby and carpark)*

## 4.2.2 Entrances and Exits

There should be sufficient cameras to provide comprehensive coverage of all external public access doors, emergency exits and vehicle entrances/exits (e.g. turnstile gates, gantry points of car parks, etc.). 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.

Frontal view of people entering/exiting the building's premises via main entrances/exits, should meet a minimum image height of 'Identification' level.

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.

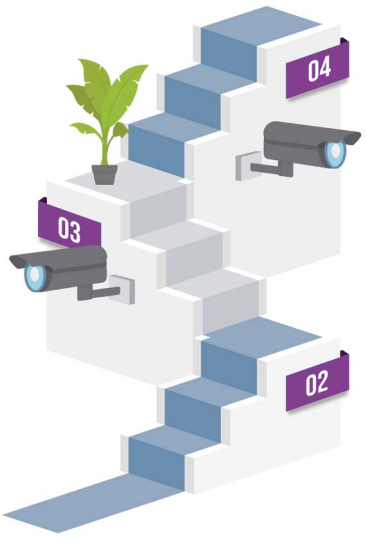
There should be coverage of the frontal views in both directions of every emergency exit. The entrances to the emergency exit escape routes should also be covered by cameras in the public areas. General views of these emergency exits should meet a minimum image height of 'Observation' level.

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.

## 4.2.3 Lifts/ Staircases

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.

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.




## 4.2.4 Counters

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.

### 4.2.5 Sensitive Rooms

Coverage of the external areas outside the door of the sensitive rooms[3] is to be provided. General views of the external access area of the doors should meet a minimum image height of 'Observation' level.

For each door fitted with an intrusion alarm, the activation of the alarm should 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.

### 4.2.6 Critical Areas

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

Coverage of the internal areas housing the critical assets[4] such as critical operational equipment or systems is to be provided. General views of the critical assets should meet a minimum height of 'Observation' level.

### 4.2.7 Summary of Coverage Requirements

Building owners may refer to Annex A for the summary of the coverage requirements covered under Clause 4.2.

---

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

*4 Critical asset refers to critical system, equipment or processes which, if damaged or destroyed, may have a debilitating impact on the functioning of the premises, e.g. single point of failure.*

# 5. Other Considerations

## 5.1 Training of VSS Operators

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

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

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 operators are familiar with the SOPs.

## 5.2 Signages

The Personal Data Protection Act (PDPA) requires organisations to inform individuals of the purposes for which their personal data will be collected, used or disclosed in order to obtain their consent. Building owners should thus provide notifications in order to fulfil their obligation to obtain consent for the collection, use or disclosure of CCTV footage.

Notices should be strategically placed at prominent location or points of entry of a building to inform the individual that the VSS is in operations.

For more details on PDPA, building owners may refer to PDPC Advisory Guidelines on PDPA.

## 5.3 Cybersecurity

Building owners should consider engaging the services of a cybersecurity specialist to understand the potential cybersecurity risks and effective schemes to prevent unauthorised access, interference, or disabling of the VSS.

Building owners may refer to IMDA Internet of Things (IoT) Cyber Security Guide and the General Cybersecurity Guidelines for IP Video Surveillance Systems in Annex B for recommendations to safeguard the VSS.

# 6. References


1. CPNI Security Lighting Guidelines for Security Manager (Feb 2015)
2. IMDA Internet of Things (IoT) Cyber Security Guide (Version 1, 2020)
3. PDPC Advisory Guidelines on PDPA (Rev 31 Aug 2018)
4. Technical Reference for Video Analytics within Video Surveillance System, Parts 1 and 2, TR 69: 2019
5. CCTV Operational Requirements Manual – Home Office Scientific Development Branch (Version 5.0, dated Apr 2009)
6. IES Security Lighting for People, Property, and Critical Infrastructure, IES G-1-16: 2016
7. IEC Video Surveillance Systems for use in security applications, IEC 62676: 2014


# 7. List of Abbreviations

| | | |
|---|---|---|
| CCTV | - | Close Circuit Television |
| FCC | - | Fire Command Centre |
| fps | - | Frames per second |
| GPS | - | Global Positioning System |
| IMDA | - | Infocomm Media Development Authority |
| NVR | - | Network Video Recorder |
| OR | - | Operational Requirements |
| PDPA | - | Personal Data Protection Act |
| PDPC | - | Personal Data Protection Commission |
| PTZ | - | Pan-Tilt-Zoom |
| SDK | - | Software Development Kit |
| SOP | - | Standard Operating Procedure |
| UPS | - | Uninterrupted Power Supply |
| VMS | - | Video Management System |

## ANNEX A: Summary of Coverage Requirements

Table 4 shows the summary of the coverage requirements under Clause 4.2 that stipulates the target image height requirements on the viewing terminals.

| Location | Defined Areas | Detect | Observe | Recognise | Identify |
|---|---|---|---|---|---|
| **Common Areas** | Extensive Coverage of Common Areas (e.g. inner fence line, 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 | | | | √ |
| | Internal view of room housing critical assets | | √ | | |

*Table 4 - Recommendations for Key Areas*

## ANNEX B: General Cybersecurity Guidelines (IP Video Surveillance System)

| S/No | Guidelines | Details | Areas of Applicability | | |
|---|---|---|---|---|---|
| | | | Camera | NVR | VMS |
| 1 | Product shall be promptly updated with the latest firmware/ software updates/ security patches | Regular firmware and OS updates (every month) | √ | √ | √ |
| | | Unsupported product shall be replaced | √ | √ | √ |
| 2 | Strong Password | Change default passwords | √ | √ | √ |
| | | Use complex password of 12-character length, with combination of at least 3 out of the 4 following groups: uppercase, lowercase, special characters and numbers | √ | √ | √ |
| | | Change password regularly (every 6 to 12 months) | √ | √ | √ |
| | | Passwords are not displayed in clear | √ | √ | √ |
| 3 | Account Management | Unique account for individual | √ | √ | √ |
| | | Timely removal of unnecessary accounts | √ | √ | √ |
| | | CCTV operators shall only have read-only access | √ | √ | √ |
| 4 | Session Security | Use HTTPS/TLS where possible | √ | √ | √ |
| 5 | Cryptography | Use strong cryptographic algorithms. | √ | √ | √ |
| 6 | Hardware Root-of-Trust | Use equipment that implements hardware root-of-trust where possible | √ | √ | √ |
| 7 | Device and System Hardening | Use Surveillance Product Hardening Guides | √ | √ | √ |
| | | Operating System Hardening Guides (e.g. refer to “Centre for Internet Security”) | | | √ |
| 8 | Network Access Control | Segregation from Internet (physical, via firewall to restrict access to only authorised Internet destinations) | √ | √ | √ |
| | | Secure remote access using VPN and MFA | √ | √ | √ |
| | | Network switch port authentication (MAC address whitelist, 802.1x) | √ | √ | √ |
| 9 | Event logging | Log all user access and administrator activities | | √ | √ |
| | | Regular log review for anomaly | | √ | √ |
| 10 | Anti-Malware | Use up to date anti-malware versions | | √ | √ |
| 11 | Clock synchronisation | Configure to retrieve time from a single NTP source | √ | √ | √ |
| 12 | Physical Access Control | Use secure hosting facility | | √ | √ |
| | | Use secure rack where possible | | √ | √ |
| | | Protect power and network cables/connectors using conduits | √ | √ | √ |
| 13 | Resilience | Perform regular backup | | √ | √ |
| | | Perform Business Continuity and Disaster Recovery exercises where possible | √ | √ | √ |

*NVR- Network Video Recorder*
*VMS- Video Management System*