مركز المتابعة والتحكم

Monitoring and Control Center

Manual of Standards
For Surveillance Devices

Version 2.0

2023

The Purpose of This Manual

The purpose of the manual of standards for surveillance devices/systems is to be a reliable reference for government agencies, public/private entities, consultants and contractors; to apply the required general specifications, technical specifications and the coverage areas required for the entities that have been specified in this manual. All of which directly contributes to reducing crimes and identifying perpetrators in a way that ensures the maintenance of security and public order of the country.

Terms

Sn	Term	Definition
1	MCC	Monitoring and Control Centre.
2	Public Entities	Government-owned establishments designated for managing public utilities and providing government services.
3	Private Entities	Establishments that are not owned by government agencies and which carry out a commercial or industrial activity, including buildings and residential complexes.
4	Field of View (FOV)	The scene that is captured by the camera and displayed on the monitoring and control screen.
5	Identification Level	The level from which an unknown person is identified for the first time.
6	Recognition Level	The level from which a person is distinguished from another known person.
7	Detection Level	The level from which moving objects are detected.
8	Vehicle View Level	The level from which the type of vehicle and the license plate is clearly visible.
9	Vehicle License Plate Recognition Level	The level from which the vehicle plate data (plate number, source, code, color and category) can be read during day time and night time and stored in a database by using a vehicle plate reader.
10	Single Point of Failure	Refers to one fault or malfunction that can cause an entire system to stop operating.
11	Monitoring and Control Room	The places through which the monitoring and control devices are managed.
12	Monetary and financial institutions (cheques and bonds)	It is the local and foreign institutions operating in the UAE, licensed by the Central Bank in which their business is limited to mediating in the sales or shares purchases, local and foreign bonds, currencies, commodities and mediating in the process of money market.
13	Commercial shops	Commercial shops specified by the concerned authorities.
14	Government authorities	Ministries, federal and local government agencies and departments.
15	Competent authorities	Judicial, police and security authorities.
16	Concerned authorities	The government agencies that are responsible of managing and regulating the use of monitoring and control devices at a country level.

Acronyms

Sn	Acronym	Meaning
1	IP	Internet Protocol.
2	ONVIF	Open Network Video Interface Forum.
3	SNMP	Simple Network Management Protocol.
4	WDR	Wide dynamic range.
5	IR	Infrared.
6	IP66	Ingress Protection 66.
7	LAN	Local Area Network.
8	API	Application programming interface.
9	VMS	Video management systems.
10	RAID	Redundant array of independent disks.

Groupings and Video Storage Duration in Days

SN	Category	Group	Duration
1	Monetary and financial institutions (Bonds, Checks).	A	30 Days
2	Stores/warehouses of precious, hazardous, and medical materials.	A	30 Days
3	Commercial shops specified by the concerned authorities.	A	30 Days
4	Government authorities.	A	30 Days
5	Wedding and events Halls.	A	30 Days
6	Cinemas complex.	A	30 Days
7	Money exchangers.	A	90 Days
8	Government/private, Kindergarten, Nurseries, Schools, Universities and Institutions.	A	90 Days
9	Gold and jewelry shops.	A	90 Days
10	Public Parks.	A	30 Days
11	Entertainment venues and private sport clubs.	B	30 Days
12	Sport clubs and stadiums.	B	30 Days
13	Public and private hospitals, health centers, clinics, pharmacies and blood banks.	B	30 Days
14	Buildings designated for parking.	B	30 Days
15	Residential compounds, buildings and commercial buildings.	B	90 Days
16	Fuel stations.	B	90 Days
17	Museums and exhibition halls.	B	90 Days
18	Labor camps.	B	90 Days
19	Places of worship and religious educational centers.	B	30 Days
20	Holiday homes.	B	30 Days
21	Places of public transport: buses, vehicles, trains, planes, ships, boats, land and sea ports and any other means intended for public transportation.	C	90 Days
22	Hotels, hotel apartments, and places of limited residential.	C	180 Days
23	Shopping malls.	C	180 Days
24	Banks.	C	180 Days
25	Digital data storage and video recording centers.	C	180 Days

Notes:

- The concerned authorities in each emirate have the right to specify the required duration of video storage in days for the categories specified above as they see fit, with a minimum of 30 days.
- The concerned authorities in each emirate have the right to add any other category if they see that the nature of work requires the implementation of this manual.

General and Techinical Specifications

1. General Specifications

SN	Clause	Group (A)	Group (B)	Group (C)
1	Installing high-resolution cameras that cannot meet the minimum required frame rate for recording is not allowed without obtaining prior approval from the concerned authorities.	✓	✓	✓
2	Installing cameras on the roof for example where the field of view exceeding the entity boundaries or exposing private or restricted areas is not allowed without obtaining prior approval from the concerned authorities. The cameras should not have zoom features. Moreover, the cameras or recording system should support the privacy masking feature to hide the unwanted coverage zone.	✓	✓	✓
3	Installing hidden cameras is strictly prohibited.	✓	✓	✓
4	Using wireless cameras is not allowed without obtaining prior approval from the concerned authorities.	✓	✓	✓
5	The entity is required to provide the sufficient light to achieve the identification and vehicle view coverage level.	✓	✓	✓
6	The cameras lens must be varifocal (motorized lens) if the installation of the camera is 4 meters or above.	✓	✓	✓
7	To place a visible sign to notify the visitors and users of the presence of surveillance cameras in Arabic, English and Urdu languages and to be maintained regularly.	✓	✓	✓
8	Entities can use any cloud computing only after obtaining prior approval from the concerned authorities.	✓	✓	✓
9	Powering off the systems, devices, deleting videos or/and images is not allowed without obtaining prior approval from the concerned authorities.	✓	✓	✓
10	The entity is required to use an antivirus software in the recording systems that are running on the Windows operating system; and the software should be enabled and working continuously.	✓	✓	✓
11	The entity is required to install the recording systems in a secure and clean place and away from the possibility of it being tampered.	✓	✓	✓
12	The entity is required to change the default user name and password of the cameras, monitoring devices, software & hardware on a continuous basis.	✓	✓	✓
13	Each operator should have a dedicated user name/password with access granted based on the permissions given to perform their tasks.	✓	✓	✓
14	The account lockout policy should be enabled in case the number of failed log-in attempts to the recording system exceeds 5 attempts.	✓	✓	✓
15	The MAC address filtering should be enabled on the network switches besides disabling the unused ports.	✓	✓	✓

SN	Clause	Group (A)	Group (B)	Group (C)
16	It is prohibited to use operating systems, which are no longer supported by the vendor (e.g. Windows 7).	✓	✓	✓
17	The entity should continuously update the cameras firmware, operating system and antivirus software beside all updates that relate to system security.	✓	✓	✓
18	The entity should provide a firewall according to the specifications if requested by the concerned authorities.	✓	✓	✓
19	Connecting the systems through the internet is not allowed without obtaining prior approval from the concerned authorities.	✓	✓	✓
20	The entity must maintain the public image of the area when installing the monitoring and control devices in accordance to the guidelines and regulations issued by the concerned authorities.	✓	✓	✓
21	The public and private entities must assign a licensed entity to carry out the works of implementing and installing monitoring and control devices, in addition to its maintenance, and providing the concerned authorities maintenance reports when requested.	✓	✓	✓
22	The public and private entities should inform the concerned authorities in the event of technical issue and solve it within one working day. The entity should also inform the concerned authorities if the issue cannot be rectified, stating the reasons.	✓	✓	✓
23	The drawings should be in DWG format.	✓	✓	✓
24	The wires and electrical connections should be hidden or extended inside pipes to prevent vandalism or to make it difficult to tamper with.	✓	✓	✓
25	The electrical connections must be of high quality.	✓	✓	✓
26	The areas and rooms names should be clearly indicated on the drawings (e.g. electricity room, communication room, monitoring and control room, and lobby).	✓	✓	✓
27	The cameras names should be clearly indicated on the final drawings with the installations details of each camera type and should be reflected on the actual system.	✓	✓	✓
28	The camera field of view for each coverage level should be distinguished by the following colors: identification (red), recognition (green), detection (blue).	✓	✓	✓
29	The cables routes between the Integrated Distribution Frame (IDF) and Main Distribution Frame (MDF) rooms should be shown on the drawings including cables conduits and trays.	✓	✓	✓
30	The entity should keep and continuously update the following documents and provide them to the concerned authorities upon request. - The approved as-built drawings. - Systems operating manual. - A document that contains systems configurations details, and IP addresses, usernames and permissions and the passwords.	✓	✓	✓

SN	Clause	Group (A)	Group (B)	Group (C)
31	The entity should record all maintenance and cleaning works conducted on the systems and the names of whom conducted the work, with the date and time.	✓	✓	✓
32	The indoor and outdoor cameras should be cleaned periodically to ensure clarity of the images all the time.	✓	✓	✓
33	The concerned authorities can choose to add or exclude the need of a surveillance control room in an entity.	✓	✓	
34	Extracting images and/or videos is not allowed without an official letter from the competent authorities granting permission.	✓	✓	✓
35	The public and private entities should provide a record of all persons who extracted or looked at the images or videos specifying the reason after having the written authorization from the competent authorities, with their names, place of work, date and time and to provide the concerned authorities with the records if requested.	✓	✓	✓
36	Access to the surveillance control rooms is restricted to employees, system operators, and authorized visitors only and pictures are prohibited inside the surveillance control room.	✓	✓	✓
37	All data related to the electronic record of entry and exit of employees, system operators, and authorized visitors must be provided only to the surveillance control room/rooms indicating the time and date.	✓	✓	✓
38	A record must be provided in which all the operations that take place in the surveillance control room/rooms are recorded (downloading, withdrawing or transferring the recording material, etc.).	✓	✓	✓
39	The surveillance control room must be equipped with internal and external communication systems.	✓	✓	✓
40	It is forbidden to bring phones and electronic devices equipped with cameras to the surveillance control room/rooms.	✓	✓	✓
41	The surveillance control room/rooms must comply with health and safety requirements.	✓	✓	✓
42	Backup power shall be provided to supply the surveillance control room/rooms in the event of a major power failure for 30 minutes.	✓	✓	✓
43	The location of the surveillance control room/rooms should be isolated from the gathering places of visitors, reception places and crowded corridors.	✓	✓	✓
44	It is prohibited to remove any devices from the surveillance control room/rooms without prior approval from the concerned authorities.	✓	✓	✓
45	It is only permissible to use the drive that contains the encryption feature to transfer data after approval from the concerned authorities.	✓	✓	✓
46	It is prohibited to bring a laptop computer into the surveillance control room/rooms without prior approval from the concerned authorities.	✓	✓	✓
47	The surveillance control room should be equipped with a door access control system.	✓	✓	✓
48	All active parts of the IT network that serve security systems must be installed in secured places. Access to them must be limited to authorized people and to prohibit the active parts from being tampered whether it is in the main distribution frame room or in the integrated distribution frame room.	✓	✓	✓

SN	Clause	Group (A)	Group (B)	Group (C)
49	It is prohibited to update or integrate the devices through the internet in the control room without obtaining prior approval from the concerned authorities.	✓	✓	✓
50	The recording system access password should comply to the below requirements; - Minimum length of 11 characters. - Consists of at least one lowercase and one uppercase letters. - Consists of at least one special character (e.g. #, $, @). - Should be changed frequently or at least every three months by a password not used before.		✓	✓
51	The entity is required to have a surveillance control room; and the concerned authorities have the right to add or exclude this requirement, as needed.			✓
52	The Audit Log/Audit Trail feature should be available and enabled in the surveillance system to monitor users' activities related to changes to the configurations in addition to the logs, it should be kept for the same duration of the video storage as specified for each entity and access should be limited to authorized persons.			✓

2. Technical Specifications

SN	Clause	Group (A)	Group (B)	Group (C)
1	Only fixed type IP cameras should be used.	✓	✓	✓
2	PTZ cameras can be used only after obtaining prior approval from the concerned authorities.	✓	✓	✓
3	The camera resolution should be a minimum of (1920 x 1080) pixels.	✓	✓	✓
4	The minimum camera frame rate should be as the following: - Identification Cameras – 25 frames per second. - Recognition Cameras –12 frames per second. - Detection Cameras –12 frames per second. - Vehicle View Cameras – 25 frames per second.	✓	✓	✓
5	The camera should be equipped with IR and its IR range should match the camera view distance.	✓	✓	✓
6	The camera should support minimum dual streams.	✓	✓	✓
7	The camera and recording system should support the ONVIF Profile S protocol. An alternative protocol can be used after obtaining the concerned authorities' approval.	✓	✓	✓

SN	Clause	Group (A)	Group (B)	Group (C)
8	The camera should support the SNMP v2c/v3 protocol.	✓	✓	✓
9	The camera should support at least the H.264 compression.	✓	✓	✓
10	The camera should have the WDR technology (110 dB) or an alternative technology for a scene containing two parts of unequal lighting (dark and bright part).	✓	✓	✓
11	The camera should have the auto iris technology or an alternative technology in locations where the intensity of the lighting changes continuously.	✓	✓	✓
12	The outdoor cameras should be suitable for the United Arab Emirates climatic conditions and their ingress rating should be minimum IP rating: IP66.	✓	✓	✓
13	For the identification cameras, the angle of incidence of the entrance cameras should not exceed 20 degrees vertical and should not exceed 45 degrees' horizontal.	✓	✓	✓
14	For the identification cameras, the pixel density of the images captured by the entrances cameras should be a minimum 500 pixels per meter, and resolution must be set to minimum (1920x1080). OR The target face shall be the most important part of the image. The size of the target image shall not be less than 120% of the display size on the monitor.	✓	✓	✓
15	For the recognition cameras, the image pixel density for recording should be a minimum 125 pixels per meter. OR The whole body and the surrounding area shall be the most important part of the image. Hence, the size of the target image shall not be less than 50% of the display size on the monitor.	✓	✓	✓
16	For the detection cameras, the image pixel density for recording should be a minimum 30 pixels per meter. OR The whole body and the surrounding area at an average distance shall be the most important part of the image. The size of the target image shall not be less than 10% of the display size on the monitor.	✓	✓	✓
17	For the vehicle view cameras, the image pixel density for recording should be minimum 500 pixels per meter to identify the vehicle type, plate number, source, code, and color. OR The height of the apparent letters and numbers (the target) shall be completely displayed on the screen and shall not be less than 20% of the display size on the monitor.	✓	✓	✓

SN	Clause	Group (A)	Group (B)	Group (C)
18	The camera should be configured on the H.264 codec or on a newer codec technology.	✓	✓	✓
19	The entity should enable the SNMP protocol for all cameras if requested by the concerned authorities.	✓	✓	✓
20	The other settings should be configured to meet the required coverage level (identification, recognition, detection and vehicle view) for recording.	✓	✓	✓
21	Use the recording system that has been approved by the concerned authorities only.	✓	✓	✓
22	The recording system should support all the cameras that are connected to it, and should not affect the required coverage level for both live and recording videos.	✓	✓	✓
23	The recording system used should be approved by the concerned authorities and it should be capable of being integrate with the concerned authorities' systems through API/SDK. The manufacturer/service provider should bear the costs of the systems development.	✓	✓	✓
24	The recording system should be managed through a central management system (CMS) if it has been requested by the concerned authorities.	✓	✓	
25	The recording system should have at least one dedicated LAN port to allow connection with another network.	✓	✓	✓
26	The recording system should support minimum dual streams.	✓	✓	✓
27	The recording system should also support the SNMP v2c/v3 protocol.	✓	✓	✓
28	The recording system should comply with the video codec of the camera.	✓	✓	✓
29	The recording system should have the ability to extract report in (CSV) or (TXT) format.	✓	✓	✓
30	The recording system should be able to extract images and video clips in a format by which they can be played through a free software running on the Windows operating system.	✓	✓	✓
31	The recording system should be able to display the camera name, date, and time on the video stream of each camera.	✓	✓	✓
32	The recording system should support searching by the camera name, date, and time.	✓	✓	✓

SN	Clause	Group (A)	Group (B)	Group (C)
33	The recording system should resume working and recording automatically whenever a restart occurs due to power interruption or any other malfunction.	✓	✓	✓
34	Entities are permitted to set the recording upon motion detection, as long as the system records before the motion is detected by 10 seconds.	✓	✓	
35	The recording system date and time should match the real date and time continuously.	✓	✓	✓
36	The recording system should be configured to overwrite the video that exceeds the specified storage period for each entity based on the first in first out method.	✓	✓	✓
37	The stored video/images should not occupy a storage space of more than 80% of the total storage capacity.	✓	✓	✓
38	The entity should provide redundant power supplies for the monitoring and control system with minimum 30 minutes operating time. The redundant power supplies should support the SNMP v2c/v3 protocol. The SNMP protocol is excluded for entities that have a recording system that is not running on Windows operating system.	✓	✓	✓
39	The redundant power supplies should have the safe shutdown feature for systems running on Windows operating system.	✓	✓	✓
40	The recording system should have an independent and secured electrical circuit; the maximum load of each circuit should not exceed 80% of the total electric circuit capacity.	✓	✓	✓
41	The entity should provide monitoring screens of size minimum 21 inches and to be compatible with the resolution of the installed cameras.	✓	✓	✓
42	Monitoring screens should be designed for continuous operations (24/7) – (365 days).	✓	✓	✓
43	Monitoring screens should be designed for monitoring purposes.	✓	✓	✓
44	The network switches should support the SNMP v2c/v3 protocol.		✓	✓
45	The network switches should have the MAC address filtering feature.		✓	✓
46	The recording system should be managed through a video management system (VMS) that supports multicast streams and the operating system should be Windows.			✓
47	The recording system should have the ability to integrate with video analytics systems.			✓
48	The system must be set to continuous recording (24/7).			✓

SN	Clause	Group (A)	Group (B)	Group (C)
49	The recording system should automatically and continuously be synchronized with a time source to ensure a real-time connectivity.			✓
50	All the system log (notifications/SNMP) must be viewed through a software to show all system errors, this will allow the operator to report about any malfunction.			✓
51	The surveillance devices should not have a single point of failure.			✓
52	The surveillance system failover/failback time should not be more than two minutes.			✓
53	Core switches should be layer three and stackable.			✓
54	Storage should be configured to at least "RAID 5" and the hard drives should be enterprise with a minimum rotation rate of 7200 rotation per minute (RPM).			✓

Areas and Level of Coverage

1. Areas and Level of Coverage (General)

The public and private establishments (A, B, C) must adhere to covering the public places specified below.

- Levels of coverage and places of coverage are determined by the concerned authorities, the below places and levels of coverage can be used to their benefit.

Identification Level	
1	The entrances and exits of the facility and the emergency exits.
2	Control rooms and equipment rooms for monitoring and control devices.
Recognition Level	
3	Entrances of main utility rooms entrances (electrical, elevators, mechanical and communication rooms).
4	Cash handling areas, selling, and purchasing points.
5	Places of cash funds/cabinets.
6	Entrances of public toilets from the outside.
7	Lobbies, receptions and waiting areas.
8	Areas of drop off and pick up of visitors from vehicles.

9	Emergency assembly areas.
10	Lift lobbies, inside lifts and stairs (escalators and fixed stairs).
11	Emergency exit staircases (alternately between every two floors).
12	Corridors.
13	Goods loading and unloading areas.
14	Male and female public praying areas.
15	All main kitchens, dining and canteen areas.
Detection Level	
16	Perimeter of the building from the outside.
17	Landscape areas.
18	Basement and outdoor parking areas.
Vehicle View Level	
19	Entrances of passengers drop-off and pickup areas.
20	Entrances and exits of vehicles.

2. Areas and Level of Coverages (Based on Activity of the Entity)

The public and private establishments (A, B, C) must adhere to the coverage areas as specified for each category, which has been determined according to the nature of activity in the entity as shown below:

- **Monetary and financial institutions (bonds, cheques)**

Recognition Level		
1	Open office spaces for staff.	Optional
2	Safe/Vault Rooms.	Mandatory
3	Customer service locations.	Mandatory

- **Stores/warehouses of precious, hazardous, and medical materials**

Recognition Level		
1	Full coverage from the inside of the stores/warehouses for precious materials, hazardous materials and medical materials and its perimeter.	Mandatory

- **Commercial shops specified by the concerned authorities**

Recognition Level		
1	Inside the liquor storage area.	Mandatory

- Government entities

Recognition Level		
1	Customer service areas.	Mandatory
2	Private praying areas.	Optional
3	Archive of important documents.	Mandatory
4	Main conference rooms.	Mandatory

- Cinemas

Recognition Level		
1	Full coverage of ticket counter areas.	Mandatory
2	Audience seats (halls).	Mandatory

- Public and private schools, universities, institutes, kindergartens and nurseries

Recognition Level		
1	Kindergarten classrooms.	Mandatory
2	Sleeping areas/rooms in kindergartens and nurseries.	Mandatory
3	Classrooms in schools, institutes and universities.	Mandatory
4	Classrooms for people of determination.	Mandatory
5	Main theaters/galleries.	Mandatory
6	Indoor and outdoor playing areas and public swimming pools.	Mandatory
7	Library.	Mandatory

- Gold and jewelry shops

Recognition Level		
1	Display and sale tables for gold and jewelry stores.	Mandatory

- Public parks

Recognition Level		
1	Full coverage of ticket counter areas.	Mandatory
2	All playing areas.	Mandatory
Detection Level		
3	General coverage of the park.	Mandatory
4	Garden perimeter and vehicle parking areas.	Mandatory

- Entertainment venues and private sport clubs

Recognition Level		
1	Full coverage of ticket counter areas.	Mandatory
2	Food and beverages selling points.	Mandatory
Detection Level		
3	Indoor and outdoor playing areas and public swimming pools.	Mandatory

- Sport clubs and stadiums

Identification Level		
1	Entrances of audience stands of sports entities.	Mandatory
2	Entrances to the stadium.	Mandatory
3	All stairs leading to audience stands.	Mandatory
4	Audience seating area in sports entities (250 pixels per meter).	Mandatory
5	Baggage scanner area (250 pixels per meter). The field of view of the camera must be set on both the entry and exit of the baggage scanner.	Mandatory
Recognition Level		
6	General view of audience seats (PTZ).	Mandatory
7	Food and beverages selling points.	Mandatory
8	TV broadcasting area.	Mandatory
9	Full coverage of ticket counter areas.	Mandatory
10	Press conference areas.	Mandatory
11	Seating areas for coaching staff and substitute players.	Mandatory
Detection Level		
12	Indoor and outdoor playing areas and public swimming pools.	Mandatory

- **Public and private hospitals, health centers, clinics, pharmacies and blood banks**

Recognition Level		
1	Inside the laboratory, pharmacy, blood banks and drug warehouse.	Mandatory
2	Entrance of operating rooms, intensive care rooms and x-ray rooms.	Mandatory
3	Medical archive rooms, administrative archive rooms and important documents rooms.	Mandatory
4	Ambulance drop off area.	Mandatory
5	Indoor and outdoor playing areas and public swimming pools.	Mandatory

- **Buildings designated for parking**

Detection Level		
1	Inside the building to cover vehicle parking area.	Mandatory

- **Residential compounds, buildings and commercial buildings**

Recognition Level		
1	Corridors of all floors.	Mandatory
Detection Level		
2	Public places available to the public in residential compounds, buildings and commercial buildings.	Mandatory
3	Indoor and outdoor playing areas and public swimming pools.	Mandatory
4	Internal roads of residential compounds.	Mandatory

- **Fuel stations**

Identification Level		
1	Entrances and exits of convenience stores.	Mandatory
Recognition Level		
2	At main tanks refueling points (petrol, diesel and gas).	Mandatory
3	The inside of the convenience store.	Mandatory
LPR Cameras		
4	Entrances and exits of fuel stations.	Mandatory

- **Museums and exhibition halls**

Recognition Level		
1	Full coverage of ticket counter areas.	Mandatory
2	Indoor and outdoor venues/galleries and exhibition areas.	Mandatory
3	Baggage scanner area (250 pixels per meter). The field of view of the camera must be set on both the entry and exit of the baggage scanner.	Mandatory

- **Labor Camps**

Recognition Level		
1	Indoor and outdoor playing areas.	Mandatory

- **Places of worship and religious educational centers.**

Recognition Level		
1	Indoor and outdoor praying areas for women and men.	Mandatory
2	The entrances to ablution places from the outside.	Mandatory
3	The entrances to the minarets from the outside.	Mandatory
4	Classrooms for women, men and children.	Optional

- **Holiday Homes**

Recognition Level		
1	Vehicle parking for homes, villas and farms.	Mandatory
Vehicle View Level		
2	Vehicle entry area and the main gate of houses, villas and farms.	Mandatory

- **Places of public transport: buses, vehicles, trains, planes, ships, boats, land and sea ports and any other means intended for public transportation**

Identification Level		
1	All entrances from the outside. (250 pixels per meter)	Mandatory
2	Passengers entry and exit gates.	Mandatory
3	All entrances from the runway to the airport campus.	Mandatory
4	Passengers entrances and exits of boats pavements.	Mandatory

5	Baggage scanner area (250 pixels per meter). The field of view of the camera must be set to the entry and exit of the baggage scanner.	Mandatory
Recognition Level		
6	Surrounding areas of baggage and luggage inspection scanners.	Mandatory
7	All ports for passenger registration, inspection and registration of luggage and baggage.	Mandatory
8	Full coverage of stores/warehouses for precious materials, hazardous materials and medical materials and their surroundings.	Mandatory
9	All prayer rooms.	Mandatory
10	Full coverage of ticket counter areas.	Mandatory
11	Main tank supply points and fuel, diesel and gas supply points.	Mandatory
12	Detention area.	Mandatory
13	Passenger waiting area.	Mandatory
14	Inside retail stores.	Mandatory
15	Staff resting area and locker rooms.	Mandatory
16	Smoking area.	Mandatory
17	Aircraft isolation area.	Mandatory
18	Aircraft maintenance area.	Mandatory
19	Baggage claim area.	Mandatory
20	All service rooms from inside and outside.	Mandatory
21	At the railway track area (intersection, rig crossing, under bridge, over bridge, under pass).	Mandatory
22	Fence of the public transport entities.	Mandatory
23	Boat/Marina pavements.	Mandatory
Detection Level		
24	Marina/boat dock.	Mandatory

- **Hotels, hotel apartments, and places of limited residential**

Identification Level		
1	Passengers entrances and exits of boats docks.	Mandatory
Recognition Level		
2	General outdoor coverage of the villas/chalets of hotels, hotel apartments and serviced residences.	Mandatory
3	Boat/Marina pavements.	Mandatory
Detection Level		
4	Indoor and outdoor playing areas and public swimming pools.	Mandatory

- **Banks**

Recognition Level		
1	Safe/Vault Rooms.	Mandatory
2	Branch manager office.	Optional
3	Staff offices in open spaces.	Optional

- **Digital data storage and video recording centers**

Recognition Level		
1	The entire coverage of the data center and video recording center.	Mandatory

Additional Requirements

Automated License Plate Reader System

It is a system capable of automatically detecting and reading the plate number, source, color and category.

1. General and Technical Specifications

SN	Clause
1	Only fixed type IP cameras should be used.
2	The camera should support the ONVIF Profile S protocol. An alternative protocol can be used after obtaining the concerned authorities approval.
3	The outdoor cameras should be suitable for the United Arab Emirates climatic conditions and their ingress rating should be not lower than IP rating: IP66.
4	The camera should be configured to minimum (1600 X 1200) pixels.
5	The camera frame rate should be configured to minimum 20 frames per second.
6	The recording system used should be approved by the concerned authorities and it should be capable of being integrate with the concerned authorities' systems through API/SDK. The manufacturer/service provider should bear the costs of the systems development.
7	The accuracy of vehicle detection should be a minimum of 99% and the accuracy of license plates recognition should be a minimum of 95% during day and night time for Gulf Cooperation Council plates.
8	The manufacturer/service provider should add the new license plates and develop the vehicle plate reader to achieve the required recognition accuracy of (95%) within (90) days. Additionally, the entity should bear the costs of the systems development.
9	The vehicle plate reader should have a software through which an overview image of the vehicle is displayed to identify its type besides the plate image as illustrated in the figure below.
10	The software should supports searching by the camera name, camera location, plate number, source, code, color, category, date and time in addition to the ability to extract reports that contain the vehicles overview images, plates images and data in (CSV) format.
11	The vehicle plate reader should generate the below alerts and display them on the software with the ability to configure the severity of the last four alerts to medium and high. Alerts: - The camera stopped working. - The image-processing unit stopped working. - The system is not detecting vehicles data. - Failed to send vehicle images and data in case of a network failure. - Malfunction in the watchdog or a similar solution. - The image storage space increases to a value equivalent to the pre-configured percentage.

	- The memory utilization rate of the image-processing unit increased to a pre-configured percentage. - The memory utilization rate of the recognition engine increased to a pre-configured percentage. - The recognition accuracy of the license plates decreased to a value below the pre-configured percentage.
12	The vehicle plate reader should resume working whenever a restart occurs due to power interruption or any other malfunction. Additionally, it should automatically send the images and data once the system restoration is complete.
13	Powering off the systems, devices, deleting videos or/and images is not allowed without obtaining prior approval from the concerned authorities.
14	The operating system of the recording system should be Windows.
15	The recording system and network switches should support the SNMP v2c/v3 protocol.
16	The network switches should have the MAC address filtering feature.
17	The vehicle plate reader should automatically and continuously be synchronized with a time source to ensure a real-time connectivity.
18	The recording system should be configured to overwrite the video that exceeds the specified storage period for each entity based on the first in first out method.
19	The entity should provide redundant power supplies for the vehicle plate reader system with minimum 30 minutes operating time, and the redundant power supplies should support the SNMP v2c/v3 protocol.
20	The redundant power supplies should have the safe shutdown feature for systems running on Windows operating system.
21	The pictures taken by the vehicle plate reader should be stored in the JPEG format.
22	The stored video/images should not occupy a storage space of more than 80% of the total storage capacity.
23	Entities can use any cloud computing only after obtaining prior approval from the concerned authorities.
24	The license plate reader system should have their dedicated devices with the possibility to share network switches.
25	It is prohibited to use operating systems, which are no longer supported by the vendor (e.g. Windows 7).
26	The entity should record all maintenance activities conducted on the systems including the names of those who conducted the exercise, the date and time.

Disclaimer

1	This document belongs to Monitoring and Control Centre. MCC reserves the right to modify it at any time without prior notice.
2	The concerned authorities bear no liability on incidents resulting from failure to adhere to these standards or faults resulting from technical or manufacturing flaws or vulnerabilities.
3	The concerned authorities have the right to request to add or make changes on the monitoring and control devices in entities like adding places of coverages or/and increasing the number of cameras or/and any other changes. The entity shall bear all costs that may occur.
4	The Arabic language is the approved language in the interpretation and implementation of this manual, and in the event that a difference is established between the English text and the Arabic text contained in this manual, the Arabic text shall be used and shall be authentic and shall be considered for any interpretation of its phrases.