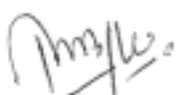


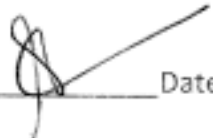




<b>Title</b>	SOP for Control Room Operations & CCTV Footages
<b>Owning Unit(s)</b>	Safety, Security and External Affairs
<b>Appendices (if any)</b>	Not Applicable
<b>Approval and Consent</b>	
<b>Policy Developed by:</b>	
 _____ Raza Zulfiqar Assistant Manager Control Room	 _____ Saqib Arshad Sr. Manager Safety & Control Room Security and External Affairs
<b>Policy Endorsed by:</b>	
 _____ Col Muhammad Anwar Hussain (R) Head of Safety, Security and External Affairs	
Date: <u>25 March 2025</u>	
<b>Approved By:</b>	
 _____ Shahnoor Sultan, Vice-President (Operations and Finance)	
Date: <u>29/3</u>	



## Version History

Version No.	Date	Notes
1.0	03 February 2025	Presentation/Discussion by the panel
2.0	20 February 2025	First Draft Prepared / Presented
3.0	20 March 2025	Second Draft Presented to VP Operations
4.0	25 March 2025	Final Document



## Index

<b>1. Purpose.....</b>	<b>5</b>
<b>2. Scope.....</b>	<b>5</b>
<b>3. Definitions.....</b>	<b>5</b>
<b>4. Elaboration of SOP</b>	
4.1 Restrictions on Camera Use.....	6
Privacy Considerations: Areas where Cameras Cannot Be Used	
4.2 Head of Department (HOD) Responsibilities.....	6
Risk Assessments and Camera Placement, Surveillance Access and Audits	
<b>5. Footage Review SOP .....</b>	<b>6</b>
5.1 Footage Request & Approval Process.....	6-7
5.2 Review Limitations.....	7
5.3 Sharing of Findings with Relevant Authorities.....	7-8
5.4 External Requests .....	8
<b>6. Data Storage Management &amp; Redundancy.....</b>	<b>8</b>
<b>7. Control Room Organizational Chart.....</b>	<b>9</b>
<b>8. Control Room Duties.....</b>	<b>8</b>
8.1 Evidence Preservation.....	9
8.2 Documentation.....	9
8.3 Reporting and Communication.....	9
8.4 Additional Observations.....	9
8.5 Monitoring Responsibilities.....	9
8.5.1 Emergency Situations.....	9
8.5.2 Unauthorized Access & Intrusions.....	9
8.5.3 Unattended Items.....	9
8.5.4 Suspicious Behavior.....	9
8.5.5 Parking Violations.....	9
8.5.6 Guard Placement and Presence.....	9
8.5.7 Premises Misuse.....	10
8.5.8 Fire Alarm Alerts.....	10
8.5.9 Fire Panel Operations .....	10
8.5.10 Pre-Alarm and Fault Reporting .....	10



8.6	Handing Over and Taking Over Shift Responsibilities.....	11
8.6.1	CCTV System .....	11
8.6.2	Access Control System .....	11
8.6.3	Fire Alarm Control Panel .....	11
8.6.4	Public Address System .....	11
8.6.5	Client PCs & Network Switches .....	12
8.6.6	Walk-Through Gates .....	12
8.7	Execution and Maintenance of Equipment.....	11
8.7.1	Equipment Installation and Maintenance .....	11
8.7.2	Daily Functionality Review.....	11
8.7.3	Backup System Connection .....	11
8.7.4	Fault Assessment – Supervisor Responsibility .....	11
8.7.5	Coordination with IT and Procurement.....	12-13
8.7.6	Post-Repair Performance Assessment .....	13
8.7.7	Scheduled Maintenance .....	13
8.7.8	Maintenance Checklist .....	13
8.8	Emergency Response Plan.....	13
8.8.1	Staff Availability & Communication .....	13
8.9	Control Room Responsibilities – Emergency Response Plan.....	14
8.9.1	Proactive Camera Surveillance.....	14
8.9.2	Physical Rounds & Coordination .....	14
8.9.3	Alerting Management Staff .....	14
8.9.4	Safety Monitoring & Incident Reporting .....	14
8.9.5	Monitoring for Safety Hazards.....	15
8.9.6	Fire Alarm and PA System Operations .....	15
8.9.7	Protection of Security Equipment .....	15
8.9.8	Injury or Hazard Response .....	15
8.9.9	Safety Equipment & Resource Management .....	15-16
8.9.10	Equipment Monitoring & Restoration.....	16
8.9.11	Fire Safety Response.....	16
9.	<b>Enforcement and Compliance</b> .....	16
	<b>Annex - Daily Equipment Check Report</b> .....	17



Creating a Standard Operating Procedure (SOP) for a control room is essential to ensure effective monitoring, management, and response to security incidents.

## 1. Purpose

The primary purpose of this SOP is to regulate the installation, placement, and use of CCTV cameras to monitor and record public areas for safety and security on the university campus. This SOP applies to all university premises and is applicable to faculty, staff, students, visitors, vendors, and contractors. The CCTV system aims to:

- **Safety & Security Surveillance:** Capture footage to provide evidence in case of harm or crime and deter such incidents.
- **Monitor Premises Safety:** Capture footage in the event of stolen or damaged property, providing evidence and deterring property crimes or violations.
- These requirements are essential and legitimate for the conduct of swift monitoring & CCTV surveillance round the clock. The installation of Electronics Security system is to ensure safety & security of campus by surveillance.

## 2. Scope

The procedure is applicable to all staff irrespective of grade and level (permanent/ contractual) deployed at control room. Assistant Manager control room is responsible for conducting their routine conformance check for assurance of necessary compliance against the SOP along with sharing, submission, of any glitch and deficiencies to Sr. Manager control room. Sr. Manager must ensure his random visits to confirm about the level of compliance & disseminate necessary guidelines & remedial measures to minimize the failure.

## 3. Definitions

- **Surveillance Cameras:** Devices used to transmit video signals, visible only to authorized personnel, such as control room staff, relevant managers and HOD.
- **Security Camera Monitoring:** The real-time observation of video footage by authorized university personnel.
- **NVR (Network Video Recorder):** The storage server system used to store CCTV footage continuously 24/7.
- **Control Room Operator (CRO):** Personnel responsible for monitoring surveillance footage, reporting incidents including suspicious act or behaviors, and coordinating with authorities when necessary.

## 4. Elaboration of SOP

- 4.1 **Restrictions:** The use of security cameras, monitoring of cameras, or recording must conform to applicable University standard procedures. Cameras may not be used



where audio and video recordings are prohibited. Further, security cameras shall not be used in areas where there are legitimate personal privacy concerns such as (Lockers Rooms, Restrooms, Shower areas, swimming pool, Changing room and official room).

- **4.2 Head of department:** The Head of Department (HOD) is responsible for integrating technology into the campus security program. This includes conducting technical surveys for camera placement, which is based on risk assessments, safety and security concerns, vulnerabilities and historical crime data. The decision of whether to deploy or relocate security cameras and the specific placement of those cameras falls under the authority of head of department. Only authorized personnel will have access to footage, and regular checks will be conducted to ensure compliance as per standards. To maintain personal privacy in accordance with university values and applicable laws, this SOP establishes procedures and regulates the use of cameras that observe public or common areas.
  - Only control room staff and control room management authorities have access to the video camera recordings.
  - The Assistant Manager of Control Room will audit camera operations, including the recording storage, on a regular basis and should recommend any procedural changes needed to ensure standards and operations conform to this policy.

## 5. Footage Review Policy

### 5.1 Footage Request & Approval Process

#### 5.1.1 Students

- **Approval Requirements:** Footage can only be reviewed or investigated after obtaining approval from the relevant Head of Department (HOD) and endorsement from the Head of Safety, Security & External Affairs.
- **Request Procedure**
  - For **domestic purposes**, students must approach the **Student Life Department** with a copy sent to the HOD of Safety, Security, and External Affairs for approval.
  - For **academic purposes**, students need to obtain approval from the **Registrar's Office/OAP**, with a copy sent to the HOD of Safety, Security, and External Affairs.



- **Detailed Request:** The requesting department or entity must specify the reason for the request, including a detailed description of the incident, time frame, and location of the footage required.

#### 5.1.2 Faculty & Staff

- **Approval Requirements:** Footage can only be reviewed or investigated after obtaining approval from the relevant Head of Department (HOD) and endorsement from the Head of Safety, Security & External Affairs.
- **Request Procedure**
  - For **domestic purposes**, students must approach the **Student Life Department** with a copy sent to the HOD of Safety, Security, and External Affairs for approval.
  - For **academic purposes**, students need to obtain approval from the **Registrar's Office/OAP**, with a copy sent to the HOD of Safety, Security, and External Affairs.
  - **Detailed Request:** The requesting department or entity must specify the reason for the request, including a detailed description of the incident, time frame, and location of the footage required.

#### 5.2 Review Limitations

- **Time Limit:** Footage requests must be made within **72 hours** of the incident. The time bracket will not be exceeded 24 hours in total.
- **Coverage Area:** Footage can only be reviewed if it pertains to areas that are covered by CCTV surveillance.
- **Exclusions:** Requests to review footage involving **personal belongings** (e.g., EarPods, mobile phones, cosmetics, jewelry, shoes, bottles, and other personal items) will **not** be entertained.
- **CCTV Operator's Role:** The CCTV operator's primary responsibility is to monitor cameras and resolve complaints. Therefore, an additional resource is required for reviewing footage, but only with the **HOD Security's approval**.
- **Urgency:** Only **urgent requests** (duly approved by concerned HOD and HOD Security) will be processed during working hours. Non-urgent requests will be reviewed after **campus hours**.

#### 5.3 Sharing of Findings with Relevant Authorities

- **Restricted Sharing:** Findings from the footage review will only be shared with the **relevant HOD and authorized authorities**.



- **Approval for Sharing:** Footage can only be shared after receiving approval from the **HOD Safety, Security & External Affairs** and **VP Operations**.
- **Viewing Locations:** Management authorities may view the footage at the **Office of Safety and Control Room**.
- **Control Room Lead:** The **Assistant Manager (AM) of Control Room Operations** will lead the CCTV footage evaluation process.
- **Notification to Authorities:** The AM of the Control Room will notify the **HOD, Custodian, or Investigation Committee** via email to arrange a pre-scheduled time to review the footage.
- **Collaboration on Findings:** The findings will be communicated to the relevant authorities after the footage has been collaboratively reviewed for validation.
- **Confidentiality:** Footage is sensitive and private information. It will not be shown or provided to any individual or department without proper authorization.
- **Retention of Footage:** The **Custodian** will inform the HOD of Security regarding the retention of footage in the Control Room records until the observation, incident, inquiry, or investigation is concluded.
- **Data Disposal:** If no further retention is required, footage will be discarded by the Control Room after **three months**.

#### 5.4 External Requests

- **Law Enforcement Requests:** If a law enforcement agency or court requires footage related to **external parameters**, an **official request** on government letterhead, properly signed and stamped, must be obtained. The request must then be approved by the **HOD Safety, Security & External Affairs / Vice President of Finance & Operations** before any action is taken.

### 6. Data Storage Management & Redundancy

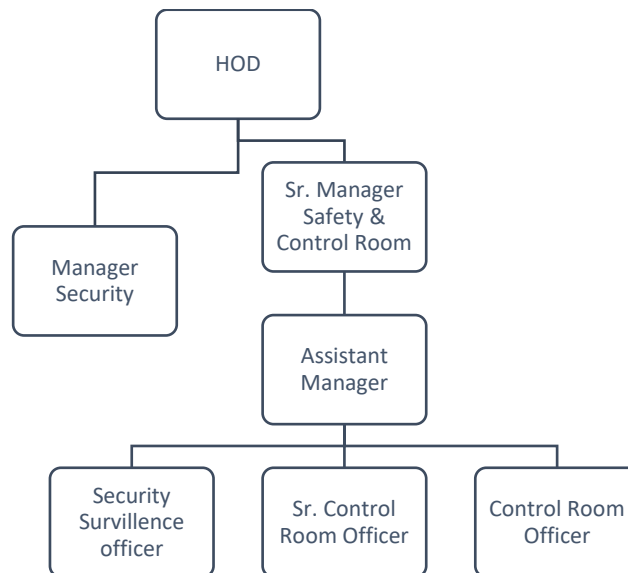
- 6.1 **Primary and Secondary Servers:** Video footage is stored on a primary server with a 25-day retention period. A secondary server serves as a backup, operating on RAID-5 for redundancy.





## 7. Control Room Organizational Chart

An organizational chart for the control room will outline the hierarchy and duties of control room personnel. This chart will ensure clear lines of communication and responsibility.



8. **Control Room Duties:** During their shifts, Control Room Operators (CROs) are responsible for observing and identifying a range of security issues and incidents. They must document these observations accurately for further review. Key duties include:

- 8.1 **Evidence Preservation:** CROs must capture snapshots or other evidence of incidents, ensuring that all details are appropriately labeled and named. This evidence is then preserved for daily inspection by the supervisor and relevant authorities.
- 8.2 **Documentation:** All observations, including unusual activities or security concerns, must be recorded in the log book, with relevant details such as time, location, and nature of the incident.
- 8.3 **Reporting and Communication:** CROs are required to communicate any issues or irregularities observed during their shift. These should be reported to the supervisor or relevant authorities for further evaluation and action.
- 8.4 **Additional Observations:** If CROs notice any issues or incidents that are not listed in the monitoring guidelines, they must ensure these are documented and brought to the attention of the supervisor for further investigation and potential corrective action.



- 8.5 **Monitoring Responsibilities of Control Room Operators (CROs):** Control Room Operators (CROs) are responsible for continuously monitoring the campus CCTV cameras and responding to various security-related incidents. Their duties include:
- 8.5.1 **Emergency Situations:** Report panic or emergency situations, including assaults, protests, disturbances in traffic, terrorism, and suspicious activities, to the line manager, supervisor, and Head of Department (HOD).
  - 8.5.2 **Unauthorized Access & Intrusions:** Monitor and report any unauthorized access or system notifications, including intrusions detected by the cameras.
  - 8.5.3 **Unattended Items:** Notify the Security & Surveillance Officer (SSO) and the person in charge about any unattended or suspicious items, such as bags, electronic devices, or packages.
  - 8.5.4 **Suspicious Behavior:** Immediately report any suspicious activity to the relevant authorities for further investigation.
  - 8.5.5 **Parking Violations:** Notify SSO, Security Officer (SO), and the person in charge of any violations in parking areas, such as incorrect parking or unauthorized vehicles.
  - 8.5.6 **Guard Placement and Presence:** Monitor and report on the position or absence of SSO, SO, and guards at their designated duty points, ensuring proper security staffing throughout the campus.
  - 8.5.7 **Premises Misuse:** Report any misuse of university facilities, such as labs, classrooms, studios, corridors, prayer areas, office premises, or faculty pods, to the relevant authorities.
  - 8.5.8 **Fire Alarm Alerts:** Continuously monitor fire alarms and associated devices to ensure proper operation.
  - 8.5.9 **Fire Panel Operations:** Maintain and manage the addressable fire panel alarm system, ensuring all alarms and devices are functioning correctly.
  - 8.5.10 **Pre-Alarm and Fault Reporting:** In case of a pre-alarm, fire alarm, or any faults detected, record the event in the log book and notify the SSO for physical inspection. During off-hours, CROs will perform a physical round to check for issues.



- 8.6 **Handing Over and Taking Over Shift Responsibilities:** During shift handovers, the incoming Control Room Operator (CRO) is responsible for verifying the functionality of various systems to ensure continuous and efficient security operations. **Daily equipment Check Report Proforma is attached as Annex – A** will be completed by each taking over CRO. The following checks must be performed, and any issues encountered should be immediately rectified, with the supervisor and line manager notified of any discrepancies:

8.6.1 **CCTV System**

- **Live View & Camera Matrix:** Ensure all cameras are operational, and the live feed is accessible.
- **Recording Logs:** Verify that recordings are being stored correctly and check for any discrepancies in recording logs.
- **Camera Angles/Focus:** Ensure cameras are correctly positioned and focused, adjusting as necessary.
- **Timing Discrepancies:** Check the time settings on all cameras and correct any inconsistencies.

8.6.2 **Access Control System**

- **Controllers & Readers:** Confirm that all access control systems, including card readers, are functioning properly.
- **Locks & Emergency Door Releases:** Ensure the electronic locks, push buttons, and emergency door releases are operational.
- **Power Supply & Barriers:** Check the power supply for all access control components, including tripods, turnstiles, heavy-duty barriers, and road blockers.

- 8.6.3 **Fire Alarm Control Panel:** Verify the fire alarm control panel and ensure all input and output devices are functioning correctly.

- 8.6.4 **Public Addressing System Components:** Check the controller, amplifiers, speakers, and desktop microphone to ensure the public addressing system is operational.



8.6.5 **Client PCs & Network Switches:** Ensure that all client PCs and network switches are functioning properly and that connectivity is stable.

8.6.6 **Walk-Through Gates:** Verify the power supply and sensor functionality for walk-through gates, ensuring they are fully operational.

**Note:** Any issues discovered during the handover process should be documented and promptly reported to the assistant manager control room for further action.

8.7 **Execution and Maintenance of Equipment:** Control Room staff are responsible for the proper execution, installation, and ongoing maintenance of various security and monitoring systems on campus. This includes ensuring that all systems are functional and promptly addressing any issues that arise.

8.7.1 **Equipment Installation and Maintenance:** Control Room staff are tasked with the following equipment-related duties:

- **Wiring & Installation:** Manage the installation and wiring of security systems, including CCTV, access control systems, full-height turnstiles, tripod gates, public addressing systems, walk-through gates, and heavy-duty barriers.
- **Complaint Rectification & Maintenance:** Address and resolve any complaints or issues related to the above equipment and ensure their continuous maintenance.

8.7.2 **Daily Functionality Review:** Control Room operations staff are required to conduct daily functionality reviews of all equipment during their respective shifts. Any malfunctions or issues identified must be reported to the Control Room Supervisor or Assistant Manager for further action.

8.7.3 **Backup System Connection:** If a fault is not immediately rectified, on-duty staff are responsible for reconnecting backup systems (including computers, LED TVs, cameras, and access control systems), following instructions from the Supervisor.

8.7.4 **Fault Assessment – Supervisor Responsibility:** The Control Room Supervisor will promptly assess and rectify any faults. If the issue persists, the Supervisor will escalate the matter to the relevant department for further investigation, coordinating with the IT team for resolution.

8.7.5 **Coordination with IT and Procurement - Fault Inspection & Repair:** In cases of hardware failure, the Control Room Supervisor and Assistant Manager will coordinate with the IT and Procurement teams to inspect the faulty



equipment, initiate repairs, and replace necessary parts as quickly as possible to minimize downtime.

- 8.7.6 **Post-Repair Performance Assessment and Feedback:** Once faulty equipment has been repaired or replaced, the on-duty Control Room staff will assess its performance to ensure it is functioning properly. Feedback regarding the performance will be shared with the Supervisor for further evaluation.
- 8.7.7 **Scheduled Maintenance:** The Control Room Supervisor is responsible for organizing semiannual maintenance for all equipment to ensure it remains in good working condition and its service life is maximized. The maintenance will include testing the accuracy and functionality of systems.
- 8.7.8 **Maintenance Checklist:** Upon completion of maintenance activities, a formal Maintenance Checklist will be filled out and endorsed by the Control Room Supervisor. The checklist will then be reviewed by the Assistant Manager to ensure proper documentation and compliance.
- 8.8 **Emergency Response Plan:** The Emergency Response Plan is designed to outline specific tasks and actions for responding to emergencies such as natural disasters, security threats, or other critical incidents. The goal of this plan is to provide clear guidelines and responsibilities for ensuring an effective and coordinated response.
  - 8.8.1 **Staff Availability & Communication**
    - **Duty Schedule Adherence:** All staff must adhere to their assigned duty schedules and be prepared to respond to emergency duties when called upon.
    - **Communication Platforms:**
      - Emergency observations and updates within the security department will be shared through the official **Emergency Safety & Security WhatsApp group**.
      - Observations related to facilities and housekeeping will be communicated through the **Control Room Reporting WhatsApp group**.



8.9 **Control Room Responsibilities – Emergency Response Plan:** Control Room Operators (CROs) play a crucial role in managing emergency situations. Below are the key responsibilities assigned to them during an emergency response:

8.9.1 **Proactive Camera Surveillance:** CROs must remain vigilant during their shifts, ensuring continuous monitoring of all cameras. Every 30 minutes, each camera feed should be reviewed in full view to ensure clarity and identify any potential issues immediately.

8.9.2 **Physical Rounds & Coordination**

- **Initiating Alerts:** CROs must perform physical rounds and contact relevant departments (Facilities, Housekeeping, Admin, Safety & Security) to alert them of any emergency situations.
- **Coordination with RSG QRF Team:** The CRO will also coordinate with the RSG QRF Team, conducting campus rounds in areas like LG/basement parking, boundary areas, and road-side parameters, ensuring appropriate actions are taken on the ground.

8.9.3 **Alerting Management Staff:** The CRO is responsible for contacting key management personnel in the event of a major issue or emergency. These personnel include Col Muhammad Anwar Hussain, Saqib Arshad, Wajid Ali Shah, Rizwan Ahmed, and Raza Zulfiqar. Updates on the situation should be provided until the issue is resolved.

8.9.4 **Safety Monitoring & Incident Reporting**

- **Water Buildup & Drainage:** In the case of water accumulation, the CRO must report it immediately to the Facilities, Housekeeping, Security, SSO, and Fire & Safety teams.
- **Lift Functionality Check:** CROs must monitor lifts for functionality and report any water penetration issues to Facilities immediately.

8.9.5 **Monitoring for Safety Hazards**

- **Hazardous Conditions:** Special attention must be given to monitoring safety hazards such as slipping, tripping, electrocution, short circuits, or falls. CROs are responsible for overseeing the safety of ground teams working under hazardous conditions (e.g., during rain or other environmental hazards).



- **Drain Hole Monitoring:** If drain holes are open, they must be monitored through available cameras to ensure emergency cones are placed by the housekeeping team to avoid accidents.

#### 8.9.6 Fire Alarm and PA System Operations

- **Fire Alarm Monitoring:** In the event of a fire alarm or potential fault, the CRO should ensure the operation of fire alarms and address any issues related to rain or other causes.
- **Public Announcement (PA) System:** The CRO is responsible for activating the PA system when required for emergency announcements.

#### 8.9.7 Protection of Security Equipment

- **Protecting Equipment from Water Damage:** CROs should ensure that under-vehicle cameras, road blockers, and other surveillance equipment are protected from water damage by using covers such as tarps or sandbags.
- **Equipment Removal:** If any equipment is at risk of being damaged by rainwater (e.g., gym readers, swimming pool equipment), it should be promptly removed with the coordination of office staff for manual locking if needed.

#### 8.9.1 Injury or Hazard Response

- **Immediate Rescue & Medical Support:** In case of injury, the CRO must ensure immediate rescue and, if necessary, request assistance from the QRF team. The Control Room should promptly inform Safety & Security management, and if required, contact an ambulance.
- **Injury Assessment:** The injured person's condition will be assessed by the QRF, CRO, and SSO staff. During office hours, the injured person will be taken to the wellness medical room, and after hours, the relevant department manager will handle further action, including hospital transportation if necessary.

#### 8.9.9 Safety Equipment & Resource Management

- **PPE Availability:** Personal Protective Equipment (PPE) will be available in the control room for staff use in case of emergency.
- **Issuance of Equipment:** The Control Room will issue any necessary equipment (e.g., walkie-talkies, emergency lights) from their stock to external departments as required. Proper documentation of the



equipment issued will be maintained, and returned items will be recorded with details of the person returning them.

#### 8.9.10 **Equipment Monitoring & Restoration**

- **CCTV Camera Offline Management:** In case any CCTV camera goes offline, the CRO must ensure that it is restored to operation as soon as possible while maintaining staff safety during the process.
- **Power Outages:** Any prolonged power outage will be immediately reported to the department management and addressed accordingly.

8.9.11 **Fire Safety Response:** In case of fire, the CRO is responsible for taking immediate action to extinguish the fire if possible. The Security team, Control Room, and Facilities team should be notified for further handling of the incident.

### 9. **Enforcement and Compliance.**

All staff, faculty, students, and visitors are expected to comply with this SOP. Any violations will be addressed according to university regulations, with potential legal and disciplinary actions taken as needed.





**Annex – A**

**Daily Equipment Check Report:**

<b>SHIFT:</b>											
<b>DATE:</b>											
<b>CRO:</b>											
S NO.	Item Description	Qty	Status		Fault Observed		Unfunctional	Functional	Total Delay Time	Reported to	Location Of Fault
			Ops	Non- Ops	Rectified	Pending					
	NVR	-	-	-	-	-	-	-	-	-	-
	Cameras	-	-	-	-	-	-	-	-	-	-
	Workstation	-	-	-	-	-	-	-	-	-	-
	LCD	-	-	-	-	-	-	-	-	-	-
	ACS Controller	-	-	-	-	-	-	-	-	-	-
	ACS Reader	-	-	-	-	-	-	-	-	-	-
	Push Button	-	-	-	-	-	-	-	-	-	-
	EM Lock	-	-	-	-	-	-	-	-	-	-
	Tripod Turnstile	-	-	-	-	-	-	-	-	-	-
	FH Turnstile	-	-	-	-	-	-	-	-	-	-
	FACP	-	-	-	-	-	-	-	-	-	-
	FACP Devices	-	-	-	-	-	-	-	-	-	-
	PAS Controller	-	-	-	-	-	-	-	-	-	-
	PAS Amplifier	-	-	-	-	-	-	-	-	-	-
	Speakers	-	-	-	-	-	-	-	-	-	-
	Barriers	-	-	-	-	-	-	-	-	-	-
	UVIS	-	-	-	-	-	-	-	-	-	-
	Walk thru Gates	-	-	-	-	-	-	-	-	-	-