National Manual of Assets and Facilities Management

Volume 5, Chapter 9

Security Systems Operations – Offices Procedure

Document No. EOM-ZO0-PR-000042 Rev 001

Document Submittal History:

Revision:	Date:	Reason For Issue
000	28/03/2020	For Use
001	18/08/2021	For Use

THIS NOTICE MUST ACCOMPANY EVERY COPY OF THIS DOCUMENT

IMPORTANT NOTICE

Table of Contents

1.0 PURPOSE

The purpose of this document is to provide guidelines and best practices to the Entity to manage security operations and resources for the protection of facilities. In addition, its purpose extends to provide a range of essential competencies, which security specialists in an Entity should possess to achieve their basic responsibilities.

2.0 SCOPE

The scope of this document is to provide guidelines and practices to the Entity to operate and manage security control systems. Individuals responsible for the security of the Entity should utilize the defined criteria and processes outlined in this document to determine the security level, customization required, and the operations of security control systems for facilities.

In addition, Security Managers should also measure performance, test security initiatives, assign assets in alignment with the Entity mission, strategically manage security-related human resource functions, and budget for resources accordingly.

3.0 TERMS & DEFINITIONS

Term	Description
ANSI	American National Standards Institute
C&E	Cause & Effect
CAFM	Computer-Aided Facility Management
CCTV	Closed-Circuit Television
dB-A	Measure of Noise volume (decibels)
EAP	Employee Assistance Program
ERT	Emergency Response Team
FC	Foot-Candle
HPS	High Pressure Sodium Vapor
HR	Human Resources
HSSE	Health, Safety, Security and Environment
ID	Identity
IEC	International Electro-technical Commission
IES	Illuminating Engineering Society
IOSH	Institution of Occupational Safety and Health
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicators
KSA	Kingdom of Saudi Arabia
LED	Light Emitting Diode
LOTO	Lock Out Tag-Out Procedure
MH	Metal-halide
NFPA	National Fire Protection Association
NIOSH	National Institute for Occupational Safety and Health
O&M	Operation and Maintenance
OEM	Original Equipment Manufacturer
OSHA	Occupational Safety and Health Administration
PAVA	Public Address and Voice Activation
PPE	Personal Protective Equipment
QHSE	Quality, Health, Safety and Environment Management

RFID	Radio-Frequency Identification
SLD	Single Line Diagram
SOP	Standard Operating Procedures
TNA	Training Needs Assessment
UK	United Kingdom
USA	United States of America
VBIED	Vehicle-Borne Improvised Explosive Device

Table 1: Definitions

4.0 REFERENCES

National Manual of Assets & Facilities Management

- ANSI/ISA-18.2-2009
- Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide, USA
- Illuminating Engineering Society (IES) Standards, USA
- ISO/IEC 27001:2005
- ISO/IEC 17799:2005
- National Fire Alarm and Signaling Code Handbook, as per NFPA 72®
- NFPA 110
- NFPA 111
- US Department of Energy – Physical Security Systems Assessment Guide
- US Department of Homeland Security – Catalog of Control Systems Security: Recommendations for Standards Developers
- Surveillance Camera Code of Practice, UK
- The Penal Law on Dissemination and Disclosure of Classified Information and Documents, KSA
- The 2011 ANSI Z535 Safety Sign & Tag Standards, USA
- 2013 American Public Transportation Association, USA
- NIOSH –Workplace Violence
- IOSH –Accident Investigation
- Saudi Aramco Suppliers Safety Management System
- OSHA Personal Protective Equipment
- Volume 10 of the Operation & Maintenance Manual
- Volume 14: Emergency Management
- Serco MELABS – Contract JLC 18-002 Training Management Plan
- National Manual of Assets & Facilities Management, Volume 6
- National Manual of Assets & Facilities Management, Volume 10
- National Manual of Assets & Facilities Management, Volume 14
- Serco MELABS – Contract JLC 18-002 Training Management Plan
- ISO 45001:2018
- United States Department of Energy according to IES Standards, USA
- The Occupational Safety and Health Administration (OSHA); Incorporating the Best Practices According to the 2011 ANSI Z535 Safety Sign & Tag Standards
- US Department of Homeland Security – VBIED Search Procedures
- OSHA, U.S. Department of Labor
- ISO 31000-Risk Management
- OSHA EAP Standard
- Security Specialist Competencies: An Interagency Security Committee Guide
- Data Protection Act, DPA 2018

5.0 RESPONSIBILITIES

Role	Description
System Security Manager / Officer	The person is responsible for the Entities overall security strategy.
Security Manager	Responsible for the daily operation of the security systems.
Security Supervisor	The person responsible for monitoring and reporting occurrences and ensuring operators follow the Standard Operating Procedures (SOP's); additional tasks include the issuing of ID cards when required.
Control Room Staff / CCTV Operators	Responsible for the issuing of ID badges, cards, and security passes. Monitoring access control and intruder detection systems. Backup and reporting of the security system databases and production equipment.
Security Maintenance	Personnel engaged in the maintenance and ongoing repairs to the security system (a 3rd party specialist service provider may supervise maintenance).

6.0 PROCESS

Overview

Appropriate security protocols and measures are critical for the control of access to public facilities that experience high levels of foot traffic (i.e., office facilities, schools and universities, housing, parks and recreation, municipal and healthcare buildings). Facility, security and life safety systems must operate in harmony to achieve the desired level of security. This means that public facilities shall be equipped with integrated security control systems which allow detection of incidents and mitigating threats faster and more effectively. Security control systems include, but are not limited to, the following:

- Data Protection/Passwords & Access
- External Lighting
- Fencing/Gates
- Signs and Tags
- Closed-Circuit Television (CCTV) Surveillance System
- Identification Badges
- Access Control
- Inspection of All Vehicles
- Exterior Doors
- Alarms/Signals
- Announcement System
- Guards/Patrol
- Vehicle Blockers and Rising Bollards
- Rising Barriers
- Tire Spike Systems

6.1 Employee Site Specific Induction & Regulations

All individual department staff and their respective employees are required to attend mandatory on-site safety training. This includes all individual departments and their respective employees. The induction should be comprehensive and include information on facilities, emergency procedures, and the roles of security personnel within their workplace. The induction training should cover the following:

- Key aspects of Occupational Health and Safety
- Residential site-specific requirements
- Entity specific policies and procedures
- Hazard identification
- Key personnel

- Reporting requirements
- Common risks
- Other site-specific information and issues

Workplace Specific Induction Managers, Team Leaders, and Supervisors have the responsibility to ensure that new/transferred employees, visitors, and contractors are inducted within their respective work areas are provided with site-specific information. Site inductions must include the following:

- Scope of work
- HR induction
- Hazards identified and control measures in place
- Health & Safety
- Slips, Trips & Falls
- Access and egress
- Parking areas and traffic routes
- Amenities, such as toilets, lunchrooms, drinking water, and smoking areas
- Safety rules
- Activities where safe work procedures apply
- First aid arrangements and emergency contact details
- Emergency procedures, including the location of the assembly area, emergency exits, fire extinguishers, and emergency contact numbers
- Personal Protective Equipment (PPE)
- Workers' safety responsibilities
- Reporting of hazards, incidents, and near misses

6.1.1 Stakeholder Partnerships

The Internal Customer

Within all organizations, stakeholders and service partner relationships must be effective and productive. Without successful internal customer relationships, the organizational departments will be ineffective in performing their tasks to maximum efficiency, which will ultimately have a direct impact on the end customer. Internal customers are the individuals or departments within organizations who depend on each other for the following:

- Materials
- Information
- Instruction
- Participation
- Assistance

Examples of these within an Entity could include relationships between Contractors, HSSE, Human Resources (HR), and Information Technology (IT). If the departments are not supporting or communicating with each other, this will ultimately create/lead to blockers. Leaders within the organization have a responsibility to identify and support the internal customer best practices and support a 'one team' environment.

6.1.2 Background Checks for Employees/Contractors/Sub-Contractors

The work of security specialists can vary, covering one/several functional areas and may focus on specific subject matter areas. Therefore, security specialists may develop competencies that specialize in one or more functional areas. The following lists the minimum competencies security specialists require:

- Understand the different types of security barriers and the security considerations associated with each one.
- Determine an effective placement of security barriers.
- Understand the objectives and theory of CCTV surveillance systems.

- Understand the purpose of using video monitoring in security and specify the correct camera type for the appropriate environment/location.
- Understand the basic components of CCTV surveillance systems.
- Understand the different types of cameras and lenses.
- Understand focal length and field of view.
- Understand appropriate implementation and functionalities of pan, tilt, and zoom cameras.
- Understand analog and digital recording pertaining to resolution, bandwidth, and frame rates.
- Understand the causes of video loss and electromagnetic interference.
- Demonstrate a basic understanding of fiber-optic video equipment and media converting devices.
- Demonstrate a basic understanding of the legal considerations associated with video monitoring system applications.
- Understand the advantages of CCTV surveillance system integration with other physical protection system elements.
- Understand the basic elements of an access control system and methodologies to specify a system.
- Understand the basic objectives of an access control system (i.e., permit only authorized individuals to enter/exit, prevent the entry of forbidden items, and enable security assessments and responses regarding irregularities).
- Specify proper entry types for an application based on security needs, physical environment, and organizational culture.
- Understand the basic concepts and challenges involved in implementing anti-tailgating and anti-passback policies.
- Understand the various methods of identity verification and the effectiveness of each type.
- Understand the basic differences between various coded-credential technologies.
- Understand the different types of biometric technologies available.
- Demonstrate a basic understanding of the various lock types and lock components.
- Understand the factors to be considered in establishing access control requirements and accompanying procedures.

6.1.3 Education & Training

All employees should be provided with adequate training to undertake their contractual role. In order to enhance skills and the professional capabilities of an employee, a Training Needs Assessment (TNA) should be conducted to identify the requirements – this will result in the improvement, efficiency, and effectiveness of the employee overall. The purpose of TNA is the following:

- Identify the training needs and ensure that the entire workforce has the necessary knowledge and skills to carry out their activities.
- Enables personnel to reach their full potential.
- Improve efficiency and effectiveness of company activities.
- Analyze and assess training effectiveness.

In-house training records should be maintained by the direct Line Manager, Safety & Assurance Department, or the Contract Coordinator. A completed training attendance sheet should be completed for audit purposes, and a copy of any training should be recorded in the employee's file.

6.2 Security Control Equipment

6.2.1 Data Protection/Passwords & Access

6.2.1.1 Data Protection

Definitions

- Classified Documents shall mean all media types which contain classified information, the disclosure of which causes harm to the State's national or organization's security, interests, policies, or rights, whether produced or received by its agencies.

- Classified Information shall mean information an employee obtains or is privy to by virtue of the office/position. Disclosure of any Classified Documents would undermine the State's national or organization's security, interests, policies, or rights.

Operating Procedures – Policy Perspective

- The Regulations of Classified Documents and Lists issued by the National Center for Documents and Archives shall determine the titles, level of classification, and subject matter of documents in coordination with relevant Entities.
- In the application of the provisions of the Panel Law of Dissemination and Disclosure of Classified Information and Documents, the following shall be considered a public employee:
    - Any person employed by the Government or by any agency of a public standing corporate personality, whether permanently or temporarily.
    - Any person assigned by a Government Entity or any other administrative authority to carry out a certain task.
    - Any person employed by companies or sole proprietorships which manage, operate, or maintain public facilities or provide public services. This includes those employed by companies whose capital is derived or contributed by the State.
    - An arbiter or expert designated by the Government or by any other judicial authority.
- Former/present public employees shall not disseminate or disclose classified information or documents which he/she obtains or is privy to by virtue of the office.
- Classified Documents shall remain within the domains of Government Entities (circulation or the relocation of Classified Documents is strictly prohibited). Such documents may not be printed, reproduced, or photocopied outside the vicinity of Government Entities, except in accordance with controls issued by the National Center for Documents and Archives.

Operating Procedures – Technical Perspective

The following technical guidelines should be considered to attain and enhance information security in the workplace:

- Power and telecommunication line facilities should be placed underground where possible or in an acceptable alternative secure location.
- Network cabling should be protected from unauthorized interception or damage, for example, by using a conduit and avoiding routes through public areas.
- Power cables should be isolated from communication cables to prevent interference.
- Identifiable cable and equipment markings should be used to minimize handling errors, such as accidental patching of wrong network cables.
- Equipment that contains storage media shall be examined to ensure any restricted data and licensed software have been permanently deleted or securely overwritten before disposal.
- Security policies shall be properly applied to off-site equipment considering the high vulnerability to risks of working outside the organization's premises.
- A documented patch list should be utilized to reduce the possibility of errors. For sensitive or critical systems, further controls to consider include:
    - Installation of armored conduit and locked rooms or boxes at inspection and termination points.
    - Use of alternative routings and/or transmission media providing appropriate security.
    - Use of fiber optic cabling.
    - Use of shielded cables to protect information and data traffic.
    - Initiation of technical sweeps and physical inspections for unauthorized devices attached to the cables.
    - Controlled access to patch panels and cable rooms.

6.2.1.2 Passwords & Access

Passwords are a vital element of information security and ensure system protection for the organization's networks and users' accounts. A poorly selected password may cause the Entity's entire network to be compromised. All Entity personnel, including contractors and those with access to the organization's systems, are responsible for taking the appropriate steps as outlined below:

- Immediate change of default passwords of applications, operating systems, or other programs must be completed after installation.
- Responsible management (i.e., IT Management or Security Management shall replace default usernames).
- Based on the criticality levels of systems to be accessed, passwords must be allocated and protected.
- The responsible management shall develop policies and guidelines that specify the complexity level of the password for each criticality level, such as minimum/maximum length, a combination of lower/upper case, numerals, and special characters.
- Security best practices need to be followed in the generation of passwords.
- Passwords should not easily be associated with the user or the organization and must follow appropriate complexity rules.
- Passwords should be transferred to the user via secure media, and the recipient must be verified.
- Login ID and password must not be combined in the same communication.
- The responsible management must ensure that high-level passwords are given to a trusted employee who is available during emergencies.
- Master password logs must be maintained independently from the control system (a notebook should be utilized and secured in a vault or safe).
- Passwords need to be changed frequently and should expire when the user leaves the organization or after a long period of inactivity.
- Double authentication password system (a text message) to ensure security

6.2.2 External Lighting

External lighting is of primary significance in the operation of security systems. Effective exterior lighting allows security personnel in locating and assessing triggered alarm initiations and provides for effective use of CCTV systems. Lights shall have a minimum specified luminescence at ground level for specific areas and emergency lighting backup capabilities. If CCTV is the primary means of assessment, lighting type should not cause glare or bright spots in camera images or footage.

6.2.2.1 Effective Exterior Lighting for Security

Security to consider the following guidelines and the appropriate situations for enhanced effective lighting:

- Horizontal Illuminance: This is the standard for assessing effective lighting primarily because many tasks are horizontal, and the measurements are easy to perform. However, this is less critical for security than other metrics such as vertical illuminance and uniformity.
- Vertical Illuminance: This is critical - one of the main security issues is identifying persons, vehicles, and their movement, which is best done by viewing their vertical surfaces.
- Uniformity/Shadows: This is important - primarily to avoid dark areas where persons or objects may be hidden. Uniformity has also been useful in enhancing video camera effectiveness.
- Glare: Lighting aimed in the wrong direction can cause glare that can adversely affect the ability of occupants and security personnel to identify persons and/or objects.

6.2.2.2 Parking Lighting

- Full-output lighting for most parking facilities is required during core business hours and for crossings, parking vehicles, and pedestrian traffic.
- Most commercial facilities require parking lighting for specific evening hours.
- In compliance with general Illuminating Engineering Society (IES) guidelines, the minimum horizontal illuminance on typical asphalt parking surfaces is 0.2 foot-candles (fc) at any given point.

Operating Procedures

- With the addition to any other time switch or occupancy controls, ensure that all parking facilities lighting is operationally controlled with a photocell or similar to eliminate daytime operation for uncovered parking.
- When a parking facility lighting is scheduled for replacement or when maintenance analysis supports immediate replacement, consider lower wattage lamp and ballast replacements in over-lit areas. Consider Light Emitting Diode (LED) technology as an effective replacement option. LEDs provide possibly more uniform distribution, “whiter” light for better contrast and identification of objects, dim-ability, instant-on capability, and potentially longer useful life.
- Evaluate the use of parking areas and categorize as either:
    - Defined Operating Hours Use
    - Potential Intermittent 24/7 Use
- In Defined Operating Hours Use, parking facilities with known shift hours would apply time switching that will turn off lighting after expected use hours. This could be accomplished by:
    - Time switching all but a few “night-lite” fixtures in the parking facilities.
    - Dimming the parking facilities lighting after expected use hours (LEDs can be dimmed successfully).

For expected intermittent use lighting, consider the use of lighting controlled by occupancy sensors. This would require a change to ‘instant on’ technology such as LED or fluorescent. The sensors would activate part or the entire parking facility, depending on size, when occupants or vehicles approach or enter the area. This could be applied in place of dimming or switching in parking facilities with defined after-hours use.

6.2.2.3 Wall-Mount Lighting

Overview:

- The use of wall-mount lighting is intended to provide security and after-dark door access lighting, although this is commonly over-applied.
- The wall-mount lighting over doors is typically needed only for after-dark access to the building. A small amount of lighting is reasonable to maintain door location identification.
    - For roll-up doors, additional lighting may be needed for loading and similar activities.
    - Doors serving as points of exit have special code requirements and restrictions in terms of output and control.

Operating Procedure:

- Consider LED products due to their even distribution, whiter light for enhanced contrast, visual distinction, and potentially longer life than both High-Pressure Sodium Vapor (HPSV) and Metal-halide (MH).
- Re-evaluate the requirement for wall-mount lighting on blank walls and identify security or safety concerns at all facilities. In some cases, fewer lights can be retained, and lower wattages can be incorporated.
- Ensure that all exterior lighting on buildings is controlled with a photocell or similar control to eliminate daytime usage.
- Consider “manual-on timed control” for any additional lighting for activities outside of roll-up doors (loading, unloading, or similar).
    - This would require a separate fixture for the additional wattage or a multiple source fixture.
    - Users would need to manually switch on the lighting and re-activate every hour if required.
    - Longer time settings can be scheduled for locations that have after-hours use.
    - This can be achieved with LED lighting in the form of separate or combination fixtures (similar to a standard incandescent 3-way lamp).

6.2.2.4 Street Lighting

Overview:

- Locations that are higher illuminance than Illuminating Engineering Society (IES) recommendations may provide some opportunities for retrofits. Current recommendations for average horizontal illuminance on typical asphalt road surfaces include:
    - Local road in an area of low pedestrian conflict (typically residential) = 0.4 fc
    - Local road in an area of high pedestrian conflict (typically commercial) = 0.9 fc
    - Collector road in an area of low pedestrian conflict (typically residential) = 0.6 fc
    - Collector road in an area of high pedestrian conflict (typically commercial) = 1.2 fc

Operating Procedures:

- Inspect areas and identify/correct lighting deficiencies, including:
    - Replacing burned-out lamps.
    - Lower wattage lamp and ballast combinations could be retrofitted where suitable to bring light levels to the appropriate amount.
- LED technology shall be considered as a long-term retrofit strategy because of its potential for better uniformity, whiter color, and expected long life.
- Compensatory measures utilized during the failure of lighting systems.
- Procedures to test security-related hardware.
- Procedures to report incorrectly calibrated or inoperable equipment.
- Procedures to record test results.

6.2.3 Fencing/Gates

Overview

Security perimeters are required to control area security and prevent unauthorized access, damage, and interference to the Entity's facilities, equipment, and information.

Examples include, but are not limited to:

- Fences
- Walls
- Controlled Entry Gates
- Staffed Reception Desks

Operating Procedures

- The following are operating procedures to inspect the integrity of interior/exterior security areas and to detect unauthorized access. These include but are not limited to:
    - Based on the results of the risk assessment, security perimeters should be clearly defined, and the siting and strength of each of the boundaries should comply with the security requirements of the assets within the perimeter.
    - Physical barriers should be built where appropriate to prevent unauthorized physical access and environmental contamination.
    - Perimeters of a facility or site containing information processing capabilities should be physically sound (i.e., there should be no gaps in the perimeter or areas where a break-in could potentially occur).
    - The external walls of the site should be of solid construction, and all external doors should be appropriately protected against unauthorized access by control mechanisms (i.e., bars, alarms, and locks).
    - A staffed reception area or other means to control physical access to the site or building should be implemented; access to sites and buildings should be limited to authorized personnel only.
    - Information processing facilities managed by the organization should be physically separated from those managed by third parties.
- Procedures to patrol and inspect vehicle barriers should be instigated to verify integrity.
- The following are procedures to inspect the integrity of activated barriers and to detect tampering. These include but are not limited to:

- All fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance with regional, national, international standards, and the local fire code.
- Suitable intrusion detection systems should be installed for all areas as per national, regional, or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times.

- Procedures should be followed to lock down a facility or area in response to a security condition (i.e., doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level).

6.2.4 Signs and Tags

Overview:

Security signs define access rules to certain areas of a facility or site. Signs also inform and remind people of an organization's expectations for safe and secure behavior. Many security policy notices go unnoticed because they are text-based and fail to stand out. Best practice signs use eye-catching graphical symbols that are noticed and understood at a glance. The following main points shall be considered when establishing security signs:

- Standard format for security messages to bring heightened awareness to important signs.
- The use of graphical symbols to effectively communicate across language barriers.

The following instructions shall act as a helpful guide when designing and operating a security sign system:

Step 1: Existent Security Control Signs Assessment

Conduct a thorough facility walkthrough and record the location and purpose of all existing signs, labels, tags, and markings (i.e., both inside and outside). This exercise is useful in planning and operating a sign system. Such a survey often reveals the following:

- Sign Clutter: This is where multiple signs have been posted in one location. A review of their content may state that some are no longer needed, and others could be combined. The new sign system will solve this problem by eliminating unnecessary signs and combining messages where appropriate.
- Missing/Damaged Signs: If missing or damaged signs are observed, a durability record based on the area is required for each instance.
- Missing Equipment: Signs referring to equipment unaccounted for, would indicate a replacement of the equipment or the removal of the sign.
- Taped Up Messages: Messages are temporarily printed on paper, taped to walls, and doors with the intention of posting a permanent sign in the future. The new sign system will provide the opportunity to update the printed messages, combine them onto one sign when appropriate. This will eliminate the improper look and lack of durability of posting paper notices containing important information.
- Out-of-Date Signs: In accordance with international best practices, every sign component should be aligned with current standards. If observed that the majority of existing signs, labels, and tags fail to use the latest formats, colors, content, and symbols, the new system will rectify these issues by ensuring that the signage adheres to specified standards.
- New Needs: With an awareness of the communication possibilities of new signs, the organization's safety, and security policies can be visually reinforced effectively with properly designed graphic-based safety signs, labels, and tags.

Step 2: Security and Organization Policy Sign Selection

- Security and general policy security signs utilize the signal word 'NOTICE' on a blue background. This provides a unique and uniform format that is easily found among the other signs posted around the facility.
- The sign's symbol and text combined inform people of the security policies and regulations.

Step 3: Viewer Driven Criteria

This is critical to the system's ability to improve security and reduce risk. While installation situations vary, general guidelines that can be applied include:

- Sign Location and Size
  - Place signs visible to the viewer.
  - Place signs in locations that provide people enough time to act accordingly.
  - Place signs where they will not be obstructed from view.
  - Consider readability based on the maximum intended viewing distance.

- Mounting Heights
  - For high-located placement, mount the sign 2 meters (minimum) from ground level.
  - For medium-located placement, place the sign's center 1.14 meters to 1.70 meters from ground level.
  - For low-located placement (e.g., egress path-marking signs), the top of the sign should be placed no more than 0.5 meters from ground level. This is to ensure that signage can be seen readily in emergencies or low visibility conditions.

- Sign Styles
  - Flat, Flag, and Panoramic Signs**:** Use flat signs when the anticipated viewing angle is straight on or less than 60° from the center; utilize panoramic or flag-mounted styles to allow the sign to be seen from an angle.
  - Directional Signs: Signs with a chevron/arrow can be used to help locate objects not immediately visible from a person's position.
  - Other Considerations: Sign size and style should be factored in the anticipated viewing angle and lighting conditions.

The quality of the Safety/Security Sign System is essential, and it is recommended that sign suppliers with proven credentials be selected for the manufacturing process.

6.2.5 CCTV Surveillance System

System Overview, Policies, and Legislations

- The use of a Closed-Circuit Television (CCTV) surveillance system must be for a specified purpose.
- With the use of a CCTV surveillance system, consider the effects on individuals and their privacy. Ensure regular reviews to confirm the use remains justified.
- Transparency is essential in the use of a CCTV surveillance system. Contact points should be made public in the event of complaints or queries related to access to information.
- Responsibility and accountability for all CCTV surveillance system activities, including images and information collected, held, and used, is vitally essential.
- Rules, policies, and procedures must be in place before a CCTV surveillance system is utilized, and these must be communicated to affected individuals for compliance.
- Only required images and information can be stored for the stated purpose of a CCTV surveillance system. Images and information should be deleted once their purposes have been achieved.
- Access to retained images and information should be restricted, and clearly defined rules for access and purpose must be established. The disclosure of images and information should only take place when necessary, or law enforcement purposes.
- Downloading of images or CCTV footage should only be allowed by dedicated users and controlled through password level access. Tracking of removable media should also be considered.
- CCTV operators should consider approved operational, technical, and competency standards relevant to the system and its purpose and work to meet and maintain those standards.
- CCTV observed images and information should be subject to appropriate security measures to safeguard against unauthorized access and use.

- Control room access for the viewing of live images should be restricted to authorized personnel only.

Operating Procedures

- Procedures to assess alarms.
- Procedures to track intruders using CCTV with pan-tilt-zoom features.
- Procedures to periodically verify the operability of CCTV systems that are not continuously displayed (i.e., call-up, or sequenced monitors).

6.2.6 Identification Badges

Identification badges are to ensure that only authorized personnel enter, occupy, or leave a secured facility and to indicate the limitations placed on access to classified matters. All employees, contractors, third party users, and all visitors should be required to wear some form of visible identification. Security personnel should be notified immediately if they encounter unescorted visitors and anyone not wearing visible identification.

The facility's security management usually manages identification badging systems. There may be instances where individual departments manage badging functions. Larger facilities may have a dedicated department/group that solely administers identification badging.

Operating Procedures

- Badge Accountability Procedures
  - Ensure that records include the date of issue, description, and the serial number of badges, organization, destruction date, and name of the holder.

- Storage of Unissued Identification Badges Procedures
  - Ensure that facilities sufficiently protect unissued identification badges against loss or unauthorized use.
  - Ensure that unissued identification badges are properly controlled, stored, and secured in locked drawers, the badge office, or the reception area.
  - Ensure proper storage of coded identification badges to eliminate the potential threat of uncontrolled access.

- Badge Recovery and Access Termination
  - Ensure prompt recovery of identification badges of terminated employees before their departure from the site and to prevent the likelihood of misconduct by dissatisfied employees.
  - Ensure that long-term visitors and temporary employees follow termination procedures when leaving the site and confirm the recovery of identification badges.
  - Security/Assessors should investigate any monetary concealments to prevent individuals, vendors, or a contracting company from retaining expired badges.
  - Security/Assessors should review methods of badge recovery and assess all locations such as dropbox repositories, protective force checkpoints, and badge office storage containers to ensure that badges are adequately protected throughout the recovery process.

- Identification Badge Destruction
  - Confirm the destruction of unwanted identification badges and ensure reconstruction to be unachievable.
  - Security/Assessors should analyze the badge destruction equipment and observe the disposal process to ensure its effectiveness.

- Identification Badge Photo Update
  - Ensure all employees have new photographs with their current appearance.

- Security officials are responsible for ensuring badge photos are current. The officials have a further responsibility to report any employee exhibiting a significant change in his/her facial appearance to the badging authority.

- Handling of Lost Identification Badges
  - When badges are reported as lost, all personnel responsible for controlling secure areas must be informed to prevent the potential use of the lost badge to attain unauthorized access.
  - Ensure proper implementation of procedures for the timely deletion of lost badges from the automated access control system and for notifying the relevant organization regarding cases involving lost badges.
  - Security officials should identify misplaced badges at portals by reviewing the lost or stolen badge register. Deficiencies in this activity can lead to unauthorized access.

- Understanding of Policies & Procedures for All Issued Badges
  - Policy and procedure training programs will be provided for the various types of badges (i.e., permanent employee, contractor, temporary visitor, and foreign nationals).

- Protection of Field Device Network
  - Ensure consistent levels of protection to the network of devices utilized in the badge creation process.
  - Ensure and protect transmission lines leading in and out of security areas.
  - Ensure locating the interconnecting equipment and cabling in a security area as this will prevent remote access to the systems.

6.2.7 Access Control

Secure areas shall be protected using suitable access control systems to prevent access to unauthorized personnel. Therefore, Entity security management must implement the following security control and operating procedures:

- Identification control for publicly accessible areas.
- Physical access devices shall be utilized for controlling entry to facilities.
- Develop and maintain access control lists of personnel that require authorized access to specific facilities.
- Verification of individual access authorizations before granting access to a facility.
- Issuance of proper authorization credentials as per Entity needs (i.e., badges, identification cards, or biometric authentication).
- Ensure annual review, removal, and approval of the access list and authorization credentials.
- Securing keys, combinations, and other physical access devices.
- Ensure a defined schedule for the change of combinations and replacement of keys in the event of personnel transfers, loss of keys, or terminations.
- Ensure control and verification of physical access to information systems distribution and transmission lines of communications within facilities.
- Safeguard control of physical access to information system devices to prevent unauthorized personnel from observing and attaining information (i.e., computers, monitors, or printers).
- Loading dock personnel will perform activities within designated areas, and access to other secure areas of the building will be restricted.
- External loading dock doors should be secured when internal doors are opened.
- All deliveries situated in the loading dock should be inspected for potential threats before transport to secure areas within the organization.
- Incoming items should be registered in accordance with asset management procedures upon entry to the site.
- Incoming and outgoing shipments should be segregated when possible.
- The date, time of entry, and departure of visitors should be recorded, and they should be supervised unless access has been previously approved. Visitors should only be granted access for specific, authorized purposes and must be informed on the security requirements and the emergency procedures of the area.

- Access to areas where sensitive information is processed or stored should be controlled and restricted to authorized personnel only. Authentication controls (e.g., access control card plus PIN) should be used to authorize and validate all access, and an audit trail of all access should be securely maintained.
- Third-party support service personnel should be granted restricted access to secure areas. Access to sensitive information processing facilities should be authorized and monitored.
- Ensure regular reviews for access rights to secure areas (i.e., and revocation and revisions).
- Specialist equipment should be fitted with Radio-Frequency Identification (RFID) security devices linked with the access control system. This ensures they are not removed from the site without prior approvals (i.e., laptops containing secure data or specialist software).
- Upon system commissioning, consideration should be given to compiling group functions for the issuance of access cards and the review of access rights to certain roles. Restrictions to personnel will be based upon their specific function and/or times of attendance (i.e., IT staff/Technicians access to secure areas such as Electrical or Communication rooms).

6.2.7.1 Inspection of All Vehicles

Operating Procedures

- Wear a high visibility jacket when conducting inspections.
- Refrain from wearing loose or hanging jewelry.
- Personnel should ensure that they are visible to traffic.
- Establish eye contact with the driver before approaching their vehicle.
- Personnel should be confident when questioning individuals and inspecting vehicles.
- Be aware of all current situations:
    - Threats to your organization
    - National terror advisories
    - Available local support
- Personnel to maintain cultural awareness.
- Establish a thorough inspection technique and ensure areas are thoroughly examined.
- Personnel to request the driver to switch off the engine.
- Before inspection of the vehicle, ensure the engine is off, and the emergency brake is engaged.
- Smoking is prohibited while conducting inspections.
- Use caution when inspecting engines, exhausts, radiators, and other vehicle components.
- For added protection, the use of gloves are recommended.
- Never reach into vehicle fan blades.
- Do not perform a search that exceeds the scope of your authority.
- Do not touch or move objects of concern.
- Report any suspicious items and decline access until guidance is acquired.

6.2.8 Exterior Doors

- Security exterior doors typically serve as a facility's general entrance and exit doors or as service entrances for facility operations personnel.
- Facility exterior doors are often the weakest part of the structure because of their service requirements and functional components.
- The number of open exterior doors shall be kept to a minimum as per business requirements to reduce the number of vulnerabilities to a facility's envelope.
- Exterior doors must provide a level of protection that is equal to or better than the level of protection provided by a facility's walls, floors, and ceilings.
- Door systems shall withstand a certain amount of pressure from the following: direct force impact, frame spreading, explosion, and/or vandalism.
- Exterior doors may be embedded with well-connected louvers and glazing as part of a balanced design approach.
- Solid wooden cores may be installed on the exterior doors, and/or a steel plate may be attached over the front to delay penetration times.
- Exterior doors should be securely attached to a structure using a metal frame that is grouted with cement.

- Exterior doors should also be mounted to open outward - away from an interior space.
- Under blast conditions, outward opening doors will sit in their frames from the force of the detonation. This prevents exterior doors from entering the facility as flying debris during an explosive event.
- Where intruder detection devices are fitted, these must be checked as part of the Maintenance Plan.
- Where doors are connected to the Access Control Room, the 'hold-open' feature should be enabled. Security control can monitor and initiate investigations when limits are exceeded.
- Emergency exit doors must be linked to the Fire Alarm System and should be tested weekly/monthly to ensure they operate upon activation.

6.2.9 Alarms/Signals

- Alarm response procedures.
- Alarm shelving, including documentation.
- Refresher training for operators, including documentation.

Alarms/Signal Management System shall be utilized to detect unauthorized entry and/or bring attention to secure areas that require protection. The procedures to meet these requirements are documented in approved site security plans. A diverse range of alarm systems is available for surveillance and detection use. For example:

- Exterior Perimeter Sensors
- Interior Sensors
- Perimeter CCTV
- Interior CCTV
- Alarm Processing and Display
- Infant and Special Care Baby Protection system
- Seismic and Pressure Sensors
- Operating Procedure:
    - Procedures to assess intrusion alarms.
    - Procedures to assess tamper and line-supervision alarms.
    - Procedures to respond to alarms, including response time.
    - Response procedures for when multiple alarms occur simultaneously.
    - Procedures to record/log alarms.
    - Procedures to patrol perimeters, security areas and to inspect systems to ensure that protection is not degraded (i.e., Inspect and confirm that no ladders or equipment can be used to bridge/jump exterior sensors in isolation zones and that no equipment is blocking interior sensors).
    - Compensatory procedures during the failure of an alarm system or components.
    - Procedures to position alarms in access mode and return them to service mode.
    - Ensure provisions are made for testing the functionality of the alarm as part of the scheduled maintenance plan.

6.2.10 Announcement System

All announcement systems used to communicate emergency directions or messages shall ensure the information provided meets the following criteria:

- The announcement shall be in real-time and not depend on pre-recorded statements.
- Announcements shall be informative in content to enable personnel to respond more efficiently.
- The announcement shall provide the following:
    - Information on the hazard and danger.
    - Guidelines on actions to be taken by personnel.
    - Location of the risk or hazard.
    - The source of the warning (i.e., the identity of the governing authority).
    - Announcements shall be specific, consistent, clear, audible, and accurate.

- Announcements shall be relegated to specific zones to address groups only affected by the situation.
- The announcement system may be integrated with Life Safety Systems, such as Public Address and Voice Activation (PAVA).
- The announcement shall be intrusive to gain and retain attention.
- A periodic inspection should be scheduled as part of the maintenance plan. Sound levels should reach the minimum dBA (A-weighted decibels) requirement, and any defects are reported and repaired promptly.

6.2.11 Guards/Patrols

Refer to National Manual of Assets and Facilities Management Volume 5, Chapter 9, Document (EOM-ZO0-PR-000100) Manned Security Procedure

7.0 START-UP PROCEDURE

7.1.1 System Specific Instructions

Refer to 7.1.4 Operating Instructions (O&M Manual)

7.1.2 Security & Data Protection

The Entity is to consider its policy upon the use of data obtained from the access cards and the storage of this data. In addition, CCTV footage and images should only be accessed by authorized personnel appointed by the Entity. Further information in the formation of the policy may be obtained within the guidance of the Data Protection Act, DPA 2018.

7.1.3 Quality, Health, Safety and Environment Management (QHSE) Policy

7.1.3.1 Risk Assessment

Several hazards can cause harm in the workplace, and a consistent and comprehensive approach can identify threats and mitigate risks. The Health Safety Security and Environment (HSSE) operators must recognize the ability to identify hazards, assess risk, and determine risk controls is the foundation of the HSSE Management System. It is imperative that personnel assigned responsibilities are qualified, experienced, and have prior knowledge of HSSE requirements.

Potential threats may be physical or health-related, and a comprehensive risk assessment should identify hazards in both categories. Examples of physical hazards include moving objects, fluctuating temperatures, high-intensity lighting, rolling or pinching objects, electrical connections, and sharp edges. Examples of health hazards include overexposure to harmful clouds of dust, chemicals, or radiation.

Risk assessments must be consultative, and the results should be communicated to all affected personnel. The objectives of the risk assessment process must be reviewed to ensure that the reduction targets established within the safety system are being applied.

The risk assessment should begin with a walkthrough survey of the facility to develop a list of potential hazards in the following categories:

- Impact
- Penetration
- Compression (Rollover)
- Chemical
- Heat/Cold
- Harmful Dust
- Light (Optical) Radiation
- Biologic

The basic layout of the facility should be documented, and a review of any history of occupational illnesses or injuries must be recorded and considered. Factors to observe during the walkthrough survey include:

- Sources of electricity.
- Sources of motion, such as machinery, could potentially result in an impact between personnel and equipment.
- Sources of high temperatures that could potentially result in burns, eye injuries, or fire.
- Types of chemicals used in the workplace.
- Sources of harmful dust.
- Sources of light radiation, such as welding, brazing, cutting, furnaces, heat treating, and high-intensity lights.
- The potential for falling objects.
- Sharp objects that could poke, cut, stab, or puncture.
- Biological hazards or other potentially infectious substances.

Documentation of the risk assessment is required through a written certification that includes the following information:

- Part 1: Hazard Identification
  - Identify Hazard
  - Location
  - Processes
  - Hazard Categories
  - Assessor Name, Signature, and Date

- Part 2: Risk Assessment & Risk Control
  - Area/Activity/Job/Task
  - Responsible Person/Date
  - Assessment Completed By /Job Title
  - Assessment Date
  - Hazard Number
  - Hazard Description
  - Consequence
  - Hazard Timing
  - Personnel at risk from the hazard
  - Current Control Measures
  - Risk Assessment
  - Acceptable Risk
  - Additional Control Measures (If any)

The workplace should be periodically reassessed for any changes in conditions, equipment, or operating procedures that could affect occupational hazards. This periodic reassessment should also include a review of injury and illness records to identify any trends or areas of concern and taking appropriate corrective action. The suitability of existing Personal Protective Equipment (PPE), including an evaluation of its condition and age, should be included in the reassessment.

7.1.3.2 Method Statement

Periodic and reactive maintenance should only be undertaken by competent personnel that are familiar with the system and are approved by the relevant authorities. Regular maintenance activities should be undertaken safely. Barriers should be in place and documented on a site-specific Risk & Method Statement. Details to compile a method statement are contained within Volume 10 of the Operation and Maintenance (O&M) Manual.

7.1.3.3 PPE & Tools List

Hazards exist in countless different forms: sharp edges, falling objects, flying sparks, chemicals, noise, and other potentially dangerous situations. Employers have the responsibility to protect their employees from

workplace threats. This is achievable by utilizing the data from the walkthrough survey during a risk assessment of the facility and developing a list of potential hazards.

Controlling a hazard at its source is the best way to protect employees. Depending on the hazard or workplace conditions, it is highly recommended to use engineering or work practice controls to manage or eliminate hazards. For example:

- Building a barrier between the hazard and the employees is an engineering control.
- Changing how employees perform their work is a work practice control.

When the walkthrough survey is complete, the employer should organize and analyze the data and determine the proper types of Personal Protective Equipment (PPE) required at the worksite. The employer should become aware of the different types of PPE available and the levels of protection offered. Select PPE that will provide a level of protection greater than the minimum required for employees. Examples of PPE include such items as:

- Gloves
- Foot and Eye Protection
- Protective Hearing Devices (Earplugs and Ear defenders)
- Hard Hats
- Respirators
- Full Body Protective Suits

The following points listed below provide guidelines on selecting and utilizing PPE equipment and tools:

- All PPE clothing, tools, and equipment should be of safe design and construction.
- All PPE clothing, tools, and equipment should be maintained.
- Employers should take into consideration the fit and comfort of PPE when selecting appropriate items for their workplace.
- Most protective equipment is available in multiple sizes, and care should be taken to select the appropriate size for each employee.
- If several different types of PPE are worn together, ensure they are compatible.
- Improper fitting PPE can increase the difference between being safely covered and dangerously exposed. It may not provide the level of protection desired and may discourage employee use.

7.1.3.4 Lockout/Tag-Out (LOTO) Procedure

LOTO procedures are essential for all employees to prevent unexpected initiation of machinery and equipment or the release of hazardous energy during service or maintenance activities.

This procedure applies to all employees, including affected contractors who assign, authorize, or perform work on equipment that has an energy source that could be activated or released during service or maintenance activities.

The LOTO procedure serves as an essential element in identifying and managing energized sources. Ignoring this procedure could result in serious injuries or significant harm.

Equipment that has the potential of being energized, activated, or operated during service or maintenance activities shall be assessed before the commencement of work to ensure that all sources of energy and potential hazards are properly identified and secured, in accordance with the instructions established by this procedure. Relevant departments are responsible for implementing the requirements of this procedure, including, but not limited to:

- Perform assessments and develop written operating procedures that document specific procedural steps for performing LOTO.
- Maintain an inventory of equipment and the specific Standard Operating Procedures (SOP).
- Provide LOTO devices (tags, locks, and/or any other hardware) for isolating, securing, or blocking machines or equipment.

    - Lock Out Device: Mechanism that utilizes a positive means, such as a lock, key type, to hold an energy-isolating device in a safe position and prevents the accidental initiation of a machine or equipment. This meets the requirements of the LOTO procedures.
    - Tag-Out Device: Warning mechanism which can be fastened securely to an energy-isolating device. This would indicate that the energy-isolating device and the equipment being controlled may not be operated until the tag-out device is removed. This should be in accordance with the requirements of an established LOTO procedure.
- Ensure LOTO training is completed for all authorized employees before they commence work with equipment.
- The supervising department shall continually monitor employee performance and compliance with this procedure and shall rectify any deviations or inadequacies observed.
  Departments must ensure that machinery design is capable of accepting a LOTO device during equipment replacement, repair, renovation, modification, or installation.
- Supervising departments shall conduct an annual review of their energy control program and document any updates.

LOTO Application Checklist

- Prepare for shutdown
    - Notify affected workers.
    - Review procedures.
    - Identify all energy sources.
    - Ensure all isolating devices will accept LOTO devices.
    - Gather the necessary tools and equipment.
    - Identify any supporting equipment or systems that must also be shutdown
- Shutdown equipment by normal methods.

Note: Use an orderly shutdown to avoid additional hazards.

- Isolate or block all energy sources for the equipment.
- Apply lockout locks and tags to each energy-isolating device and ensure the activity is conducted safely.
    - Release all stored energy.
    - Release, restrain, block, disconnect, or ensure the safety of residual stored energy.
    - When possible, use energy drains (pressurized lines, free-wheeling shafts, and active ground).
    - If energy re-accumulates during the shutdown procedure, continually verify and monitor a safe energy level until lockout/tag-out is removed.
- Physically verify energy isolation by operating controls or measuring the energy state (use a meter to verify zero energy per NFPA 70E Article 120, Operation of Startup Controls).
- If the worksite has been left unattended, repeat the above, and verify the integrity of locks and tags against tampering before continuing work.
- Perform work.

LOTO Removal Checklist

- Inspect the work area to ensure that non-essential items have been removed and the work has been completed.
- Ensure that the work area is clear of personnel.
- Remove LOTO devices.
- Inform affected employees that the work has been completed and that locks and tags have been removed.
- Wherever necessary, place security guards in the vicinity of remotely initiated equipment to ensure personnel or vehicles do not come into contact upon their reinstatement (i.e., rising bollards for vehicles in pedestrian traffic areas).
- Restore equipment to service.

7.1.4 Operating Instructions

Best practice approaches recommend operators to have an Operations and Maintenance (O&M) manual in-hand when starting-up, operating, or shutting-down systems. Official O&M manuals are produced by the system's Original Equipment Manufacturer (OEM), this provides all comprehensive instructions and specific guidelines for safe start-up, operation, and shutdown techniques. O&M manuals guide operators on how to perform adequate maintenance planning and implementation for all relevant categories. The submission is a composite document that provides warranty information, final programming, schedules, calibration settings, and manufacturer or distributor information for each control device.

7.1.5 Start-up Checklist

Security control systems are complex; therefore, system-specific start up procedures must be followed to mitigate any potential issues. The OEM manual must be adhered to when developing the startup checklist. A comprehensive methodology shall be in place for the system which must be followed in regards to the below:

- Access Control System
- CCTV
- Bollards/Barriers
- External Lighting
- Helipad Lighting System

7.1.6 Pre-Energization Test Results

Competent individuals should verify test results before the pre-energization of any electromechanical system. The pre-assessment plan shall be developed, reviewed, and approved by the Operations Team to prevent any potential of overloading, faults, breakdowns, harm to people and systems, or property. Procedures must be developed in conjunction with operations, the safety of personnel, customers, contractors, and stakeholders.

7.1.7 Line Diagram / System Architecture

Line Diagrams, System Architecture, and Single Line Diagrams (SLD) are a reference tool for the Operations Management Team to diagnose system faults and failures. They shall always be stored either as hard copies or in system software to direct operations effectively. It is advisable to have copies placed near the equipment to aid a technician's knowledge and also provide a fault-finding structure. Any alteration during fault diagnosis or modification due to changes in facilities layout shall be updated as red lines within the documentation and copies must be made available to the Operations Management Team. Please refer to site-specific SLD and Manufacturers Operations Manual. An example of a typical system architecture diagram is given below:

Examples of a typical system architecture diagram are given below:

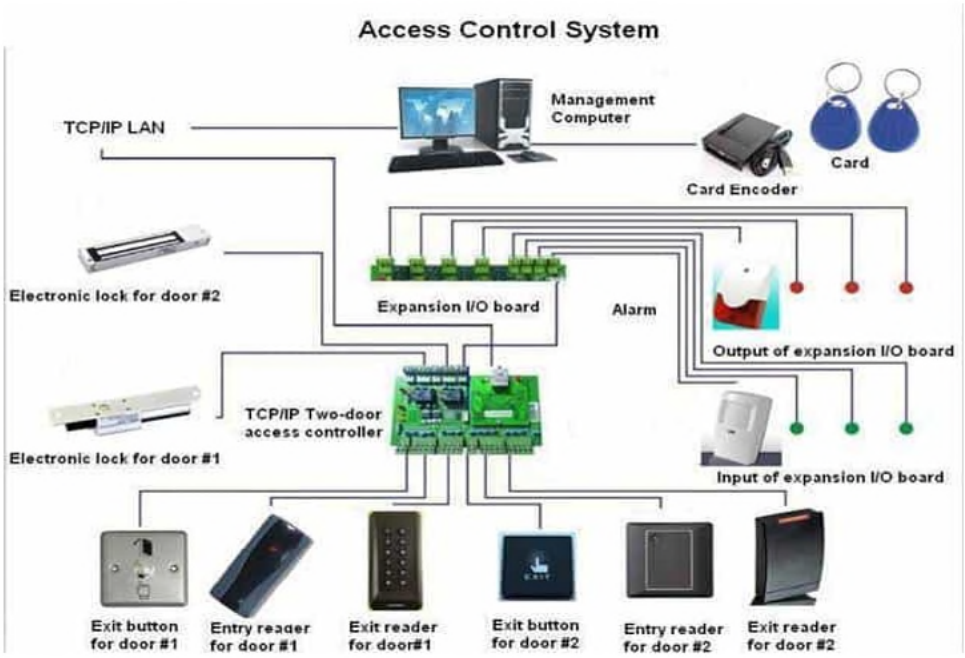

Figure 1: Access Control System Architecture

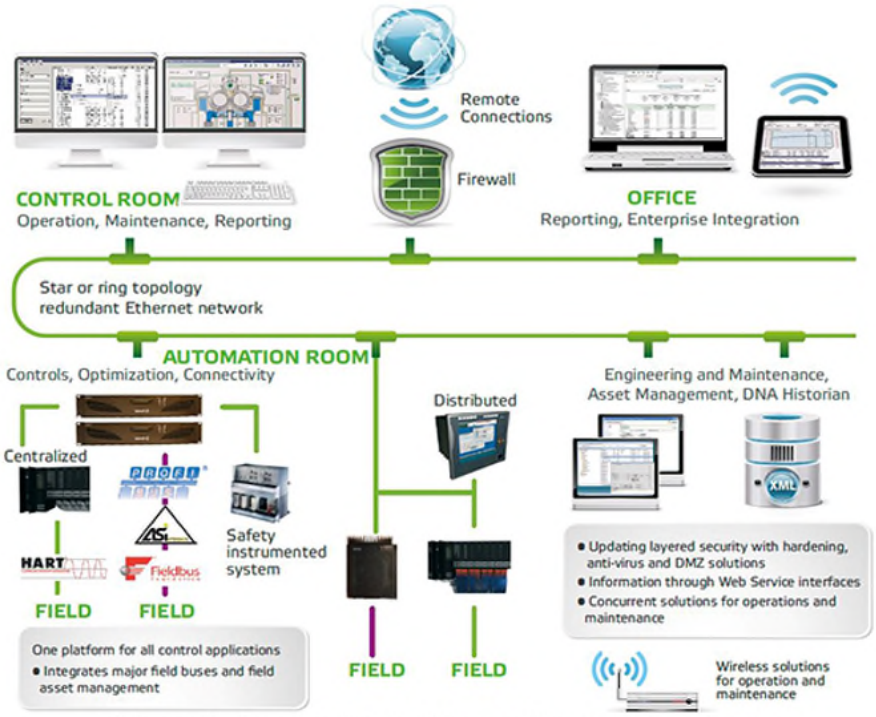

Figure 2: Access Control Human Machine Interface

7.1.8 Systems Pre-Energization Check List

The Entity's O&M team must systematically perform the critical task of inspecting electrical equipment before energization. The design and construction of data centers usually consist of complex systems. The benefit to the end-user is the electrical equipment that makes up the power distribution system will function within set parameters. Consider the following as part of the O&M checklist:

- Ensure the electrical equipment is constructed and assembled functioning within specified parameters.
- Ensure all electrical connections are cleaned, installed, and tightened per the manufacturer's specifications.
- Ensure all the sectional shipping split connections between sections are effectively and properly terminated.
- Verify the present state of all insulation levels before energizing the electrical equipment in conjunction with the manufacturer's specifications.
- Verify deterioration levels of insulated components, materials, or properties due to damage during shipment, mishandling, storage, or operation.
- Identify any deteriorated/damaged components, parts, or equipment that require replacement or repair.
- Ensure all electrical terminations have been torqued to values as prescribed by the electrical equipment manufacturer.
- Ensure the grounding system for the building or facility has been inspected and tested.

7.1.9 Post-Energization Check List

While energizing any electromechanical system, it is recommended that activities must be performed by a qualified electrical/mechanical technician. A site-specific SOP must be followed for safe energization of the asset, and for the safety of the people.

Pre-assessments and comprehensive plans must be developed, reviewed, and approved by the Operations Management Team before energizing security systems.

Contingency plans shall be in place should there be any disruption to normal operational activities.

7.1.10 Post-Energization Test Results

A standard process must be in place to record and validate the energization test results by a competent person. All stakeholders involved in operations should be made aware of the status of systems confirming that systems are safely energized and available for operations. This shall be communicated formally to all parties involved either by emails or publications, any comments or observations shall be managed through correct published process or procedure.

7.1.11 Cause & Effect (C&E) Matrix Checks

A Cause & Effect (C&E) Matrix shall be made available to the Operations Team. Any changes found within the existing C&E matrix must comply with building operational standards - the site Operations Team must be informed of any amendments to the C&E matrix. Systems integrated with fire alarms or programed with any other special control systems should be reflected within the C&E matrix. A mandatory testing regime shall be developed along with integration checks, which will be performed at intervals – this will be in accordance with the NFPA standards.

Any deviations found shall be documented and communicated to all parties. A revised program shall be developed, reviewed, tested, approved by system specialists, and witnessed by the Operations Team. Non-conformities shall be reflected in all documents and amended at the next formal review sessions.

7.1.12 Approved Person Sign Off

All documents associated with security systems shall be reviewed and approved by nominated individuals or an approved authority.

8.0 SHUTDOWN PROCEDURE

8.1.1 Security & Data Protection

Refer to 7.1.2 Security and Data Protection

8.1.2 Operating Instructions (O&M Manual)

Refer to 7.1.4 Operating Instructions (O&M Manual)

8.1.3 Shutdown Checklist

Step 1: Shutdown Preparation

Seek authorized person's approval before shutting down equipment

- Understand equipment hazards.
- Notify other workers of the shutdown.

Step 2: Shutdown Equipment

- Use the normal shutdown procedures.
- Turn all switches to OFF.

Step 3: Energy Sources Isolation

- Use energy isolation devices in accordance with established procedures to prevent transmission or release of energy.

Step 4: Application of Locks & Tags

Apply locks and tags to:

- Valves
- Breakers/Electrical Disconnects
- Mechanical Blocks

Step 5: Release or Block of all Stored Energy

- Discharge capacitors
- Block/Disconnect lines
- Block or release springs
- Block elevated parts
- Relieve system pressure
- Drain fluids
- Vent gases
- Allow the system to cool (or use PPE).
- Apply any additional locks and tags as needed.

Step 6: Verification of Equipment Isolation

- Check that other workers are clear of potential hazards.
- Check that locking devices are secure.
- Attempt normal startup.
- Return control to OFF/Neutral.

Step 7: Performance of the Task

- Perform service or maintenance.

Step 8: Lockout Release

- Ensure machinery is properly assembled and all tools removed.
- Ensure that employees are outside of danger zones and are notified that devices are being removed.
- Remove LOTO devices.

Note: LOTO devices must be removed by authorized employees.

8.1.4 System Specific Instructions

Refer to 7.1.4 Operating Instructions

8.1.5 Critical Systems Protection

Refer to 7.1.4 Operating Instructions for system protection as per OEM instructions

8.1.6 QHSE Policy

Refer to 7.1.3 QHSE Policy

8.1.6.1 Risk Assessment

Refer to 7.1.3.1 Risk Assessment

8.1.6.2 Method Statement

Refer to 7.1.3.2 Method Statement

8.1.6.3 PPE & Tools List

Refer to 7.1.3.3 PPE and Tools List

8.1.6.4 LOTO Procedure

Refer to 7.1.3.4 LOTO Procedure

8.1.7 De-Energization Permit (AP Approved)

Shutdown procedure requires that active systems should de-energized for personnel safety. Best practice standards state this is the preferred method for protecting employees from electrical hazards. The employer is permitted to allow employees to work on or near exposed active parts only:

- If the employer can demonstrate that de-energizing introduces additional or increased hazards, or
- If the employer can demonstrate that de-energizing is infeasible due to equipment design or operational limitations.
- If the employer does not de-energize under permitted conditions, then suitable safe work practices for the conditions under which the work is to be performed shall be included in the written procedures and strictly enforced.

The following work approaches are based on best practice standards:

- Strictly, only qualified individuals shall be allowed to work on energized parts or equipment.

- A circuit that cannot be de-energized using the procedures outlined must be treated as energized.
- De-energized parts are required to be locked and tagged.
- If a tag is used without a lock, it shall be supplemented by at least one additional safety measure that provides a level of safety equivalent to that obtained using a lock. Examples of additional safety measures include the removal of an isolating circuit element, blocking of a controlling switch, or opening of an extra disconnecting device.

A lock may be placed without a tag only under the following conditions:

- Only one circuit or piece of equipment is de-energized.
- The lockout period does not extend beyond the work shift
- Employees exposed to the hazards associated with reenergizing the circuit or equipment must be qualified for the procedure.
- Verification of De-energization (Mandatory):
    - A qualified individual must perform the verification.
    - The qualified individual shall activate the equipment operating controls or verify that the equipment cannot be restarted.
    - The test equipment shall be used to ensure that electrical parts and circuit elements have been de-energized.
    - Testing instruments and equipment shall be visually inspected for external defects or damage before being used to determine de-energization.
    - For circuits over 600 volts, nominal - testing equipment shall be checked for proper operation immediately before after inspections.

8.1.8 Line Diagram

Refer to 7.1.7 Line Diagram/System Architecture

8.1.9 Cause & Effect Matrix Checks

Refer to 7.1.11 Cause & Effect (C&E) Matrix Checks

8.1.10 Systems De-Energization Check List

A system-specific checklist shall be developed and approved before de-energization by the Operations Team. Once the de-energization has occurred, the responsible person shall carry a checklist and ensure that the expected operational impact has been limited accordingly. Any deviation from the checklist should immediately be communicated to the Operations Team.

8.1.11 Post De-Energization Test Results

In order to practice a safe system of operation, it is essential to verify inactive results. Any deviation from the plan shall be communicated immediately to Operations Team – this is to ensure awareness of possible changes and the impact to the original operational plan.

8.1.12 Approved Person Sign Off

Refer to 7.1.12 Approved Person Sign Off

9.0 SYSTEM MONITORING/DAILY ROUNDS PROCEDURE

9.1.1 Fault Reporting

If an operator has a request for a repair, there shall be a formal fault report form or hotline. Fault reports will have different categories based on criticality and priority:

- Priority Fault Reports categorized as minor/low will usually be checked during specific working hours. Faults reported after stipulated working hours or the weekend will not be reviewed until the next working day.
- Priority Fault Reports categorized as critical/high (i.e., a power failure, danger to life, or potential damage to property) shall be reported immediately by telephone.

9.1.2 Walk-Around Inspections

When conducting a walk-around inspection, encourage operators to refer to each equipment's O&M Manual for diagrams and information. Experienced operators are often familiar with the equipment and can identify issues based on experience and routine use. Consider the following inspection criteria:

- Inspect the machine at the start and end of a shift.
- Ensure the inspection is conducted in the same direction.
- Any differences in the state of the machine must be reported. It is the operator's responsibility to monitor the machine and document the details to the shift report.

9.1.3 Maintenance

Maintenance activities on the operation of the system should only be undertaken by staff that is trained, qualified, and approved. Ineffective maintenance could potentially lead to access restrictions, delays, or damage. Maintenance should be performed during off-peak periods to reduce disruption. Consideration should be given to alternative arrangements during maintenance. For instance, additional security personnel for the inspection of user credentials, recording personnel or granting access to sensitive areas.

9.1.4 Scheduled Maintenance

Scheduled maintenance of the system should be coordinated with Facility Management and site security staff. If required, security staff should be assigned to supervise the maintenance activity. If specialist contractors are required, this should be scheduled through the Site Maintenance Management Platform, Computer-Aided Facility Management (CAFM), or the Computerized Maintenance Management System (CMMS). Temporary passwords or access cards issued for planned/corrective maintenance activities are to be returned, de-activated, and/or destroyed.

Details of maintenance activities are outlined within Volume 6: Maintenance Management of the O&M Manual.

9.1.5 System Testing

System testing should be undertaken by qualified personnel who have approved access from the Entity Security Officer. Testing should be undertaken periodically as per the requirements within Volume 6: National Assets and Facilities Management Manual. All testing must align with the specifications of the system, and any deviations are to be recorded and notified to the Security Officer.

Temporary passwords or issuance of access cards for testing/commissioning are to be returned, de-activated, and/or destroyed on completion of activities.

10.0 EMERGENCY RESPONSE ACTIONS

10.1.1 Threat Response/Workplace Violence Training

Threats to organizations can be classified within Risk Management:

- Risk Management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events.

- Workplace/occupational violence usually refers to physical abuse or threats, and this creates a risk to the health and safety of an employee(s). The National Institute for Occupational Safety and Health (NIOSH) defines personal relationships, customer/client, and criminal intent all as categories of violence in the workplace. These categories are further segmented into the following three levels:

    - Level 1: Displays early warning signs of violence.
    - Level 2: Slightly more violent.
    - Level 3: Significantly violent.

Many workplaces have initiated programs and protocols to protect their employees. The Occupational Health Act of 1970 states that employers must provide an environment in which employees are free of harm or harmful conditions.

Organizations should employ security staff with relevant training to effectively deal with threats and workplace violence.

10.1.2 Emergency Services Plan

The Emergency Services Plan shall be in writing and cover specific actions. Employers must ensure employee safety from fire and various other emergencies. The following elements shall be included in the formation of the plan:

- Emergency escape procedures and emergency escape route assignments.
- Procedures to be followed by employees who remain to operate critical operations during emergencies.
- Procedures to account for all employees after emergency evacuation has been completed.
- Rescue and medical duty procedures to be performed by employees.
- Procedures for reporting fires and other emergencies.
- Contact information of relevant individuals/departments to provide information or explanation of responsibilities.

Alarm System:

- The employer shall install an alarm system that complies with best-practice standards.
- The alarm system will be equipped with a distinctive signal and sound feature that will vary depending on the type of emergency.

Evacuation:

The employer shall establish an Emergency Action Plan that includes the types of evacuation in emergencies.

Training:

Before implementing the Emergency Action Plan, the employer shall provide nominated individuals training in the safe evacuation of employees.

The employer shall review the Emergency Action Plan with each employee at the following times:

- Initially, when the plan is developed.
- When the employee's responsibilities or designated actions under the plan change.
- Annual review.

10.1.3 Bomb Threat/Terrorist/Fire/Explosion/Chemical Threat Procedures

The Kingdom of Saudi Arabia - Ministry of Interior, General Directorate of Civil Defense and Safety should be contacted – telephone: 998.

Refer to local site-specific guidelines regarding emergencies.

Refer to Volume 14: Emergency Management

10.1.4 Evacuation Plans/Emergency Preparedness/Incident Command (Inside/Outside Company)

Within Entity emergency evacuation/preparedness & incident command procedures, the following factors should be considered:

- Emergency Management: Defined as an active process to prevent, prepare, and respond to emergencies. Furthermore, to maintain continuity and effectively recover from a situation that threatens life, property, operations information, or the environment.
- Business Continuity: A process that ensures organizational steps are taken to identify the impacts of potential losses. Continuity can be implemented by the recovery strategy plans.
- Crisis Management: Defined as the ability of an Entity to manage effectively incidents that are likely to impact public, security, strategic, reputational, or financial factors.

Refer to Volume 14: Emergency Management Response Team

10.1.5 Emergency Response Team

An Emergency Response Team (ERT) is a group of employees who prepare for and respond to any emergency incident in the workplace (i.e., a natural disaster or an interruption of business operations). ERTs are common in both private and public service organizations. As a best practice, it is recommended Entities consider utilizing ERTs to assist during an emergency, and all personnel involved be given adequate training on an annual basis.

10.1.6 Critical Systems Protection

Security systems must be protected from any unauthorized access. Only authorized personnel can access restricted data (i.e., access entries, history logs, time stamps, video records, and attendance history). Security systems shall be programmed to have different user's level access for data protection. Any unauthorized entries could potentially harm system operations, and data can be compromised. In addition, software/firmware and applications must be updated on regular intervals according to the original equipment manufacturer (OEM) guidelines.

10.1.7 Investigation

Following any incident or accident, an investigation must be undertaken by the appropriately qualified individual, department, or governing body.

What is an incident, and why should it be investigated?

The term "incident" is defined as an occurrence, condition, or situation arising in the course of work that has resulted in or could have resulted in injuries, illnesses, damage to health, or fatalities.

The term "accident" is also commonly used or can be defined as an unplanned event that interrupts the completion of an activity, and that may (or may not) include injury to a person or property damage. The term "incident" can refer to an unexpected event that has not caused injury or damage at that specific time but involved a potential for it. "Near miss" or "dangerous occurrence" are terms for an event that could have caused harm but did not.

Note: The term incident is used in some situations to cover both an "accident" and "incident." It is argued that the word "accident" implies that the event was related to fate or chance. When the principal cause is determined, it is usually found that many events were predictable and could have been prevented if the right actions were taken - making the event not one of fate or chance (thus, the word incident is used). For simplicity, the term incident will be used to mean all the above events.

This information is intended to be a general guide for employers, supervisors, health and safety committee members, or members of an incident investigation team. When incidents are investigated, the emphasis should be concentrated on finding the root cause of the incident so it may be documented, and future incidents can be prevented. The purpose is to find facts that can lead to corrective actions, not to find fault.

Reasons to investigate a minor or serious workplace incident include:

- To establish the cause of incidents and to prevent similar incidents in the future.
- To fulfill any legal requirements.
- To determine the cost of an incident.
- To determine compliance with applicable regulations (i.e., occupational, health, and safety or criminal).

10.1.8 Critiquing Session

It is recommended that tabletop discussions be conducted post-incident with emergency services to outline lessons learned and the effective way to improve emergency response planning procedures.

10.1.9 Employee Assistance

An Employee Assistance Program (EAP) is a support program that assists employees with personal problems or work-related issues that may impact their job performance (i.e., traumatic events, health, mental and emotional well-being). EAPs generally offer free and confidential assessments, short-term counseling, referrals, and follow-up services for employees and their family members. EAP counselors also work in a consultative role with managers and supervisors to address employee and organizational challenges and needs.

10.1.10 Debriefing

A site debriefing should be undertaken immediately for employees who have been directly involved in a traumatic situation. Debriefing allows staff to have the time to process the event and work through any negative emotions. Individual counseling sessions provide a secure environment for discourse and a venue to assess the personal impact of a traumatic event.

10.1.11 Post-Incident: Briefing/Discussion

An integral part of any organization’s learning and development is to conduct a post-incident debriefing. This process should be embedded as part of the organization's principles in learning and development. The briefing discussion sessions should promote a culture of transparency and open dialogue. Lessons learned can be discussed, analyzed, and incorporated into the organization's continuous improvement plan. The debriefing process looks for answers to the following three questions:

- How well prepared were we?
- How well did we perform?
- What can be done to future proof ourselves?

10.1.12 Grab Packs for Attending Civil Defense

Consideration should be given to the provision of a grab bag containing information such as an available list of emergency contacts, buildings floor plans and access/evacuation details, fire hydrant locations, first aid kit, and any other essential items required that could assist Civil Defense during an emergency. Nominate an individual with the responsibility for the grab pack in the event of an emergency. Grab packs should be reviewed periodically to ensure contents are up-to-date (i.e., change of layout, system modifications, or upgrades). Additionally, the plans should be used for periodic testing and training of staff to ensure that they are suitable and relevant. Any deficiencies should be reviewed and where necessary amended at the next formal review session.