EXPRO
هيئة كفاءة الإنفاق والمشروعات الحكومية
Expenditure Efficiency & Projects Authority

National Manual of Assets and Facilities Management
Volume 6, Chapter 11

Security Systems Maintenance Plan for Offices

Document No. EOM-ZM0-PL-000039 Rev 000

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

This document, (“Document”) is the exclusive property of Government Expenditure & Projects Efficiency Authority.

This Document should be read in its entirety including the terms of this Important Notice. The government entities may disclose this Document or extracts of this Document to their respective consultants and/or contractors, provided that such disclosure includes this Important Notice.

Any use or reliance on this Document, or extracts thereof, by any party, including government entities and their respective consultants and/or contractors, is at that third party’s sole risk and responsibility. Government Expenditure and Projects Efficiency Authority, to the maximum extent permitted by law, disclaim all liability (including for losses or damages of whatsoever nature claimed on whatsoever basis including negligence or otherwise) to any third party howsoever arising with respect to or in connection with the use of this Document including any liability caused by negligent acts or omissions.

This Document and its contents are valid only for the conditions reported in it and as of the date of this Document.

Table of Contents

1.0 PURPOSE

The purpose of this document is to provide guidelines and practices to the Entity or Facilities Management Company (FMC) for developing and improving security systems maintenance plans within office facilities. The document aims to enhance the functional understanding of the Entity with regards to facility security systems for ensuring safety and security of both physical assets and facility personnel.

2.0 SCOPE

This document provides guidance to those responsible for ensuring that maintenance is carried out in a consistent and reliable manner by focusing on planned activities and reducing costly and disruptive reactive maintenance. The approach embodied herein relies upon proven maintenance strategies, techniques, and practices resulting in enhanced operational efficiency of the facility systems.

A well written maintenance plan shall provide the Entity with a high level of confidence to safely and effectively execute maintenance and repairs in the applicable environments. The objective of this document is to direct maintenance from a standard minimum acceptable quality to a required consistent improved high level quality, through professional technical advice and instruction.

Following key elements are included within the scope, but not limited to:

- Maintenance task planning to optimize security system operations
- Quality Assurance (QA)
- Equipment health and efficiency
- Health, safety and security of stakeholders, and the physical assets

For the purposes of this document, an ‘office’ has been defined as a form of building, portion of a building or space where business activities for organization’s are done such as, but not limited to:

- High rise buildings
- Low rise buildings
- Commercial blocks
- Business centers/hub
- Others

Notwithstanding, the recommendations presented in this document, the final responsibilities for developing the final maintenances management plans/tasks as will be applied to the security systems shall remain with the Entity, FMC, and/or Maintenance Engineer (ME).

3.0 DEFINITIONS

Term	Definition
Basis of Design (BOD)	A mandatory generated pre-construction document based on American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), Leadership in Energy and Environmental Design (LEED), and National Fire Protection Association (NFPA) to prepare Mechanical, Electrical, and Plumbing (MEP) systems manual, and commissioning documents
Cause and Effect	A cause and effect is related to an activity that is dependent upon a prescribed input being met. For instance, the release of external fire door security lock upon fire activation from an associated system. Further details will be contained within a C&E matrix held at site.
Consumable	Physical part of an engineered system, Personal Protective Equipment (PPE), or a cleaning/treatment/preservative liquid/compound whose consumption or use as the part of a maintenance task is necessary and predictable

Term	Definition
Criticality	Typically, a 4-5 level ranking system that categorizes the importance of the component, asset, or maintenance task. Refer to the National Manual of Assets and Facilities Management (NMA & FM) Volume 2 – Asset Management
Data Point Schedule	A table format which shall show the monitoring and control points for the equipment and system. Points such as control and monitoring as I/O points (Input and Output point to and from the controller)
Frequency (FQ)	Refers to a cyclic time period (e.g., weekly, monthly, quarterly)
Maintenance Levels	The complexity of maintenance activity. For example, level 1: reset, level 2: predictive maintenance, level 3: monthly related to the skillset/competence level, and experience of the operative. Sometimes referred to as task level
Maintenance Program/Schedule	Refers to the time basis of the delivery activity
Monitor/Head end Personal Computer (PC)	See engineering equipment's, systems' status for monitoring and control the operations
Permit to Work (PTW)	A safety management and work control documented system, adopted by most organizations for management of work activities
Point of Work Risk Assessment (POWRA)	A short checklist that operatives refer to at the 'location of' and immediately before carrying out a task
Quality Assurance (QA)	Method by which to assess that quality standards are being met
Quality Control (QC)	Quality standards to be attained
Run to Failure (RTF)	A maintenance strategy where the asset is deliberately not maintained but allowed to run until it fails
Test	Verifying by means of observation or measurement that the system meets the expected and/or acceptable requirements
Threshold	Numerical value of a parameter at which a decision is made
Abbreviations	
ACS	Access Control System
AHJ	Authorities Having Jurisdiction
AP	Authorized Person
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BOM	Bill of Materials
BS	British Standard
CCTV	Closed-Circuit Television
CIBSE	Chartered Institute of Building Services and Engineers
CMMS	Computerized Maintenance Management System
CO_2	Carbon dioxide
CO	Carbon monoxide
CPU	Central Processing Unit
DIS	Door Intercom System
DVR	Digital Video Recorder
ELV	Extra Low Voltage
EN	European Norms
ESS	Electronic Security Systems
FDD	Fault Detection and Diagnostics
FM	Facilities Management
GUI	Graphical User Interface
HSSE	Health, Safety, Security, and Environment
I/O	Input and Output
ID	Identity
IDS	Intruder Detection System
IP	Internet Protocol

Term	Definition
IT	Information Technology
JHA	Job Hazard Analysis
LEED	Leadership in Energy and Environment Design
LOTO	Lock Out Tag Out
LV	Low Voltage
ME	Maintenance Engineer
MEP	Mechanical, Electrical, and Plumbing
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NMA & FM	National Manual of Assets and Facilities Management
O&M	Operations and Maintenance
OEM	Original Equipment Manufacturer
PAT	Portable Appliance Test
PAVA	Public Address and Voice Alarm
PC	Personal Computer
PIR	Passive Infrared
POE	Power Over Ethernet
PPE	Personal Protective Equipment
PM	Planned Maintenance
PTZ	Pan, Tilt, and Zoom
RAMS	Risk Assessments and Method Statements
RFID	Radio-Frequency Identification
SC	Statutory Compliance
SE	Specialist Engineer
SFG	Services and Facilities Group
SOO	Sequence of Operation
SOP	Standard Operating Procedure
UPS	Uninterruptible Power Supply

Table 1: Definitions

4.0 REFERENCES

- American Society of Refrigeration and Air Conditioning (ASHRAE 13) – Specifying Building Automation Systems
- Chartered Institution of Building Services Engineers (CIBSE M) – Maintenance Engineering and Management
- National Fire Protection Association (NFPA 101) – Life Safety Code
- National Fire Protection Association (NFPA 72) – National Fire Alarm and Signaling code
- National Fire Protection Association (NFPA 730) – Guide for Premises Security
- National Manual of Assets and Facilities Management – Maintenance Procedure Writers Guide (EOM-ZW0-GL-000002)
- National Manual of Assets and Facilities Management – Extra Low Voltage (ELV) Systems Integration Guideline (EPM-KE0-GL-000007)
- National Manual of Assets and Facilities Management Volume 2 – Asset Management
- National Manual of Assets and Facilities Management Volume 4 – Financial Planning
- National Manual of Assets and Facilities Management Volume 6 Chapter 3 – Description and Definitions (EOM-ZM0-PR-000002)
- National Manual of Assets and Facilities Management Volume 6 Chapter 3 – Preventative and Predictive Maintenance Program Procedure (EOM-ZM0-PR-000003)
- National Manual of Assets and Facilities Management Volume 7 Chapter 2 – Work Control
- National Manual of Assets and Facilities Management Volume 10 – Health, Safety, Security, and Environment (HSSE)
- National Manual of Assets and Facilities Management Volume 11 – Quality
- National Manual of Assets and Facilities Management Volume 12 – Risk Management

- Standard Maintenance Specification for Building Services (SFG 20)

5.0 RESPONSIBILITIES

Only trained and competent individuals shall be appointed by management to perform maintenance tasks on security systems. Proper training and certifications of the individuals responsible for the maintenance tasks shall be verified, and routine audits be completed. A Training Needs Assessment (TNA) shall be conducted to identify existing or any new requirements. The purpose of TNA is the following:

- To identify the training needs and ensure that maintenance workforce is competent to carry out their activities.
- Enable individuals to reach their full potential
- Improve efficiency and effectiveness of company activities
- Analyze and assess training effectiveness
- Ensure that Original Equipment Manufacturer (OEM) maintenance guidelines are in practice
- Ensure that compliance is met

In house training records shall be maintained by the training department, safety and assurance department, or a contract coordinator, depending on the structure of the organization. A training attendance sheet shall be completed for audit purposes, along with a summary of the training provided. It is common to have the securities department subcontracted as it is a specialized service with responsibilities to ensure safety of occupants and facility.

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.

5.1 Levels of Operation

Interaction with the security systems may take place at all levels of the system and, at each level; there may be different requirements for different operator classes.

Role	Description
Entity	Governmental Entity having jurisdiction over parks and recreation facilities
Entity Representative {Facilities Operating Client (FOC)}	Entity representative having overall management of the facility
System Security Manager / Officer	The person responsible for the Entity facility's overall security strategy
Security Manager	The local appointed representative for the day to day operation of the security systems in place
Security Supervisor	The person responsible for monitoring and reporting occurrences and ensuring operators follow the Standard Operating Procedures (SOPs) for activities e.g., Issuance of ID cards
Control Room Staff & CCTV Operators	Duties of these personnel include, but not limited to: • Issuance of ID badges, cards and security passes • Monitoring of access control and intruder detection systems • Reporting and backup of the security system databases and production equipment
Security Maintenance	Personnel engaged in the maintenance and ongoing repairs of the security systems under the control and supervision of site staff. This may be a third party specialist service provider company

Table 2: Roles & Responsibilities

6.0 PROCESS

6.1 Security Systems

The following are security systems found within office facilities:

- Electronic access control
- Closed Circuit Television (CCTV) cameras
- Monitors and recording devices
- Motion detectors
- Intruder alarms
- Infrared and vibration detection
- Communication systems
- Others

Security systems are instrumental in monitoring events occurring in the facility perimeter or system network and analyzing them for any possible breaches and/or security threats in accordance with the Entity's security protocol and safety guidelines.

The capabilities of security systems are broadly categorized as information gathering, logging, detection, and prevention. The typical components of a security system are as follows:

- **Sensor or Agent:** Sensors and agents monitor and analyze activity. The sensors employ monitor networks, including network based, and wireless incorporating network behavior analysis technologies. The agents are typically used for host based technologies
- **Management Server:** A management server is a centralized device that receives and manages information from the sensors or agents and manages them. Sophisticated management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same Internet Protocol (IP) address, is known as correlation. Management servers are available as both appliance and software only products. In larger deployments, there are often multiple management servers, and in some cases, even two tiers of management servers may be used
- **Database Server:** A database server is a repository for event information recorded by sensors, agents, and/or management servers
- **Console:** A console is a program that provides an interface for the interface users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are solely employed for security administration, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some consoles provide both administration and monitoring capabilities

The building blocks of a facility security system include the following:

- **Access Control Systems (ACS):** The ACSs aim to authorize, record, and control the movement of personnel and assets in accordance with the facility security protocols. ACSs execute the frontline provision of granting access or imposing restriction depending upon the level of authorization
- **Video Surveillance:** The video surveillance systems aim to provide visual display and recording of the designated points at which the cameras are installed for visual inspection. These systems aid the operators to pre-emptively take action for preventing any security breaches or securing the facility from any sort of threat
- **Environmental Protection Systems:** The environment protection systems aim to monitor and control the predetermined environmental parameters such as Carbon monoxide (CO), Carbon dioxide (CO_2) levels, water flow rate, and toxicity level to secure the facility or the surrounding environment from any emanating biohazard
- **Additional Security Systems:** There may also be the following security devices used to help protect occupants:
    - Outdoor lighting with controlled luminescence to assist video surveillance

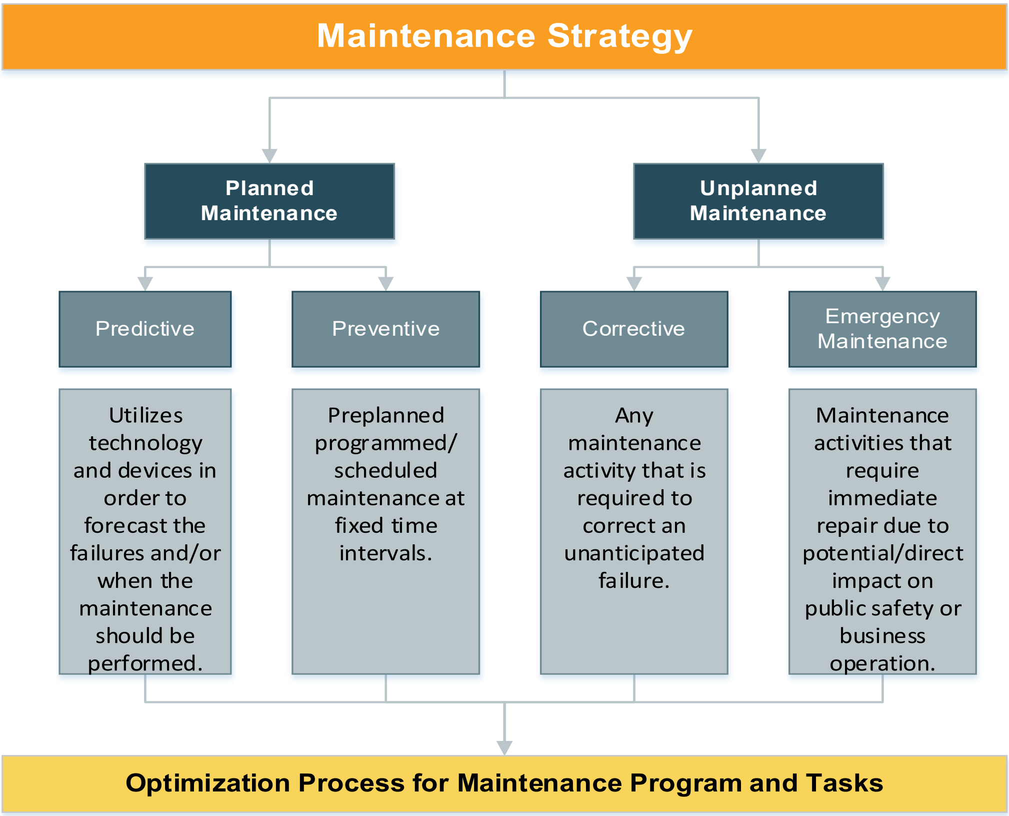
- Fencing and gates
- Vehicle blockers, rising barriers, and tire spike systems

These systems will need inspection and maintenance to maintain a safe and secure environment.

6.2 Security Systems Maintenance Strategy

Maintenance is a combination of all technical, administrative, monitoring and managerial actions during the life cycle of an item, intended to retain it, or restore it into a state, in which it can perform the required function. Security systems maintenance shall cover inspections, tests, measurements, replacements, adjustments, programming and repairs intended to retain or restore a unit or equipment to as state where equipment or asset can perform a function. It is essential to keep and preserve equipment and facility in a functional state.

Figure 1 given below shows the various type of maintenance activities involved to operate and maintain a reliable security system and as an example of a Quality Management System (QMS):



Maintenance Strategy

Planned Maintenance

Unplanned Maintenance

Predictive

Preventive

Corrective

Emergency Maintenance

Utilizes technology and devices in order to forecast the failures and/or when the maintenance should be performed.

Preplanned programmed/ scheduled maintenance at fixed time intervals.

Any maintenance activity that is required to correct an unanticipated failure.

Maintenance activities that require immediate repair due to potential/direct impact on public safety or business operation.

Optimization Process for Maintenance Program and Tasks

Figure 1: Relationship of Maintenance Concepts and Activities

6.3 Types of Maintenance

Security systems are found in all the engineering disciplines of a building. They shall need applicable maintenance based on the OEM specifications, recommendations and guidelines. A focus on this program is to work towards developing a proven maintenance strategy that is based on collecting data and planning ahead. A Planned Maintenance (PM) program is a proven strategy to reduce costs, and be effective and efficient at ensuring longevity of any asset, and is discussed in detail below.

Depending on the Entity’s asset management strategy, organizational maturity, and funding, the following types of maintenance may be applied to security systems within each office facility:

- Planned Maintenance: Preventive and Predictive (PM, PdM)
- Unplanned Maintenance: Corrective and Emergency (CM, EM)

This document focuses primarily on Planned Maintenance, other maintenance types are described within NMA & FM, Volume 6 Chapter 3 – Descriptions and Definitions (EOM-ZM0-PR-000002).

6.3.1 Planned Maintenance (PM)

Planned maintenance is a regime that is regularly performed on an overall system or elements thereof to lessen the likelihood of failure, maintain safe operating/running conditions, and efficiencies. PM is performed while the equipment or asset is still operating to eliminate unexpected breakdowns.

Key elements and advantages while scheduling and executing PM are as follows:

- Ensures consistent practices designed to improve the performance and safety of the equipment
- Reduces major repairs and failures; and ensures equipment availability
- Allows for better management and increased life expectancy of assets
- Allows for efficient manpower resources use of the required specialization, to ensure that activities are carried out in a correct manner
- Reduces costs and ensures efficient utilization of maintenance staff due to working on a scheduled basis instead of a reactive basis
- Improves safety and quality conditions for stakeholders and those coming in contact with maintenance activities

Preventative Maintenance Program (PMP) and Post Maintenance Testing (PMT) procedures are provided within NMA & FM. Whilst all equipment may not be subject to PMT, it is the Entities responsibility to identify equipment that may need to undergo PMT, for statutory compliance.

The Entity shall consider the specific requirements detailed in the following:

- NMA & FM, Volume 6 – Preventative and Predictive Maintenance Program Procedure
- NMA & FM, Volume 6 – Post Maintenance Testing procedure (PMT)
- NMA & FM, Volume 6 – Maintenance Plan Writers Guide

Utilization of a PM strategy in combination with a CMMS system will assist the Entity in following a proven strategy that can be demonstrated to internal and external stakeholders. The use of QA/QC will further assist on continuous improvement and review processes.

Refer to International Organization of Standardization (ISO 9001) – Quality Management System for more details.

Attachment 1 will illustrate an example document for ensuring a maintenance strategy is applied and followed. It will outline Frequency (FQ) for maintaining the equipment involved in the security of an office facility.

6.3.2 Statutory Requirements

It is incumbent that security system maintenance shall be performed on system/assets that require regular maintenance/inspections at set intervals as specified by OEM recommendations, and Statutory Compliance (SC) requirements. The security system monitors and control a wide range of surveillance systems such as CCTV, ACS, Intruder Detection System (IDS), Door Intercom System (DIS), Public Address and Voice Alarm (PAVA), security panic alarm and others. These integrated systems shall be inspected and maintained according to the standards highlighted within the **Section 4.0** of this document

For further information regarding statutory requirements, refer to the following:

- Chartered Institute of Building Services and Engineers (CIBSE) Guide M – Maintenance Engineering and Management Standards
- Health Technical Memorandum (HTM 2005)
- National Fire Protection Association (NFPA)

- National Manual of Assets and Facilities Management, Volume 6 – Preventative and Predictive Maintenance Program Procedure

6.4 Maintenance Planning & Scheduling

Planning decides what, how, and a time estimate for maintenance tasks. Scheduling of maintenance activities decides when and who will perform the maintenance tasks. Proper planning is a vital part in successfully managing the maintenance of equipment. Planners must collaborate with internal or external stakeholders to achieve optimum results. A comprehensive maintenance schedule shall be developed, and equipment or assets be listed in the maintenance schedule. When compiling security systems maintenance schedule together, all maintenance activities, along with other department's recommendations, personal experiences, equipment history, and OEM recommendations shall be considered. Moreover, the schedule shall define the types of maintenance activities, corrective maintenance, preventative maintenance, predictive maintenance, Run to Failure (RTF) checks, and planned shutdowns. Security system integrates other engineering critical or non-critical assets and their critical parameters. Hence, a proper cause and effect matrix shall be considered to comprehend the full impact of maintenance on security services and systems.

Security systems require particular attention as they are a crucial part of ensuring the safety of the facility occupants. There needs to be strict attention paid to priority scheduling of maintenance for the security systems. Planning schedules shall take into account the crossover of systems to ensure that no part of an office facility goes unprotected. Secondary measures need to be taken into consideration when a primary system is shut down for maintenance. This may include manned guard post stations that would usually have an electronic system in place. Therefore, planning of resources to accommodate the maintenance schedules must be considered.

In Figure 2, the below elements shall be taken into consideration when planning and scheduling security system maintenance tasks.

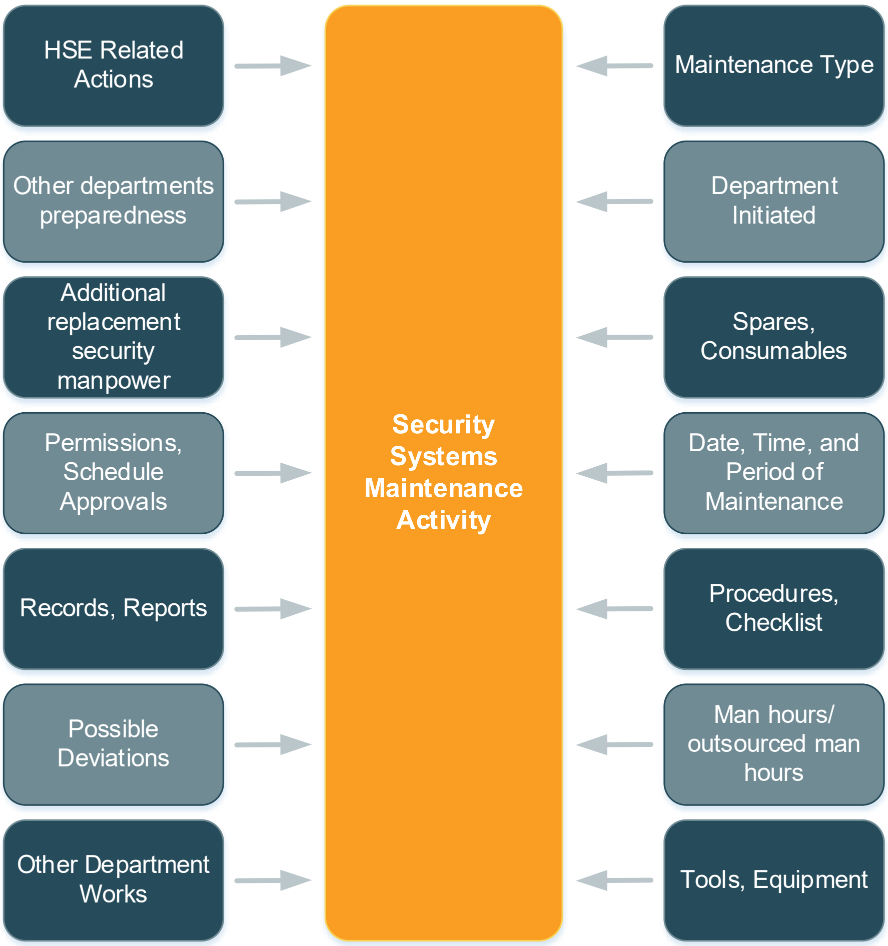

HSE Related Actions
Other departments preparedness
Additional replacement security manpower
Permissions, Schedule Approvals
Records, Reports
Possible Deviations
Other Department Works
Security Systems Maintenance Activity
Maintenance Type
Department Initiated
Spares, Consumables
Date, Time, and Period of Maintenance
Procedures, Checklist
Man hours/ outsourced man hours
Tools, Equipment

Figure 2: Pictorial Representation of Links of Maintenance Activity

The Entity shall consider the specific requirements detailed in the NMA & FM Volume 7 – Requesting, Prioritizing, Scheduling and Planning Maintenance Tasks.

6.5 CMMS Requirements

It is at the discretion of the Entity, dependent on the size of the facility whether they shall employ a Computerized Maintenance Management System (CMMS) or other Entity-approved centralized system to capture maintenance plans and outcomes. Security system maintenance plans captured within CMMS shall:

- Feature a list of tasks numbered by priority, and associated frequencies
- Enable decision making which supports optimized system performance, maximizes equipment life, and offers energy and cost-saving opportunities
- Highlight equipment criticality and procedures for deferring maintenance activities

Security system maintenance plans captured within CMMS shall also:

- Refer to an industry resource and feature site specific guidelines to support maintenance activities
- Recommend the storage method for integrated data and control points
- Feature check points for additional parameters (record sheets shall be attached to work orders to validate the results during testing and maintenance)

The Entity shall consider the specific requirements detailed in the NMA & FM Volume 2 – Asset Management

6.6 Health and Safety

While the maintenance activity is being undertaken, human error is a factor that can lead to near misses, accidents, and system malfunction. Therefore, only trained and competent staff shall undertake the maintenance activities and undertake measures to protect staff, visitors and those that may come into contact with their actions. The security system governs facility perimeter, entry & exit protocols and additionally other engineering or communications functions within a facility so measures shall be in place to restrict entry and monitor areas during maintenance.

Maintenance personnel are therefore required to plan maintenance appropriately based on analysis of system data and performance history. In addition, ensure that key stakeholders are informed at all phases of the maintenance.

The Entity shall consider the specific requirements detailed in the NMA & FM Volume 10 – Health, Safety, Security & Environment (HSSE)

6.7 Risk Management

The maintenance team shall complete a comprehensive set of Risk Assessments and Method Statements (RAMS) covering every system within office facilities. For task specific activities, a Job Hazard Analysis (JHA) shall be conducted, using the content of RAMS as a basis for the JHA. Visitors, contractors, and others working under site specific health and safety plans shall be considered within all RAMS and shall sign onto JHA, as required and applicable.

The below elements shall be considered when carrying out risk assessments for security systems maintenance:

- Identify hazards associated with each maintenance activity, for example: loss of security system-controlled systems, impact on operation of facilities, data loss, corruption of systems software, configurations, and applications and equipment failure

- Establish maintenance personnel, service providers, and building users who are at risk as a result of the maintenance activity
- Quantitatively evaluate risks using a risk matrix (involve maintenance team, subject matter experts, and HSSE team in risk assessment process and hold a Risk Workshop as necessary)
- Decide if mitigation or fall back measures are needed, required investment, responsibilities, and timeline
- Review the risk evaluation following implementation of mitigation measure
- Record findings and update CMMS systems

The Entity shall consider the specific requirements detailed in the NMA & FM Volume 12 – Risk Management.

6.8 Quality Control and Quality Assurance

Quality Control (QC) represents the quality standards which shall be met by each Entity, whereas Quality Assurance (QA) is the method by which indicate quality standards are being met and opportunities for continuous improvement are captured.

QC shall be determined by the content of security systems maintenance plans, for example:

- Actions to be undertaken through maintenance are based on system specific and site specific performance data
- FQ of maintenance is based upon OEM recommendations
- Data point thresholds which are set up in CMMS and used for refining maintenance plans

QA shall be determined using a number of techniques and data analysis, for example:

- Findings deduced from CMMS data trending
- Checklists designed for each maintenance activity
- Permit to Work (PTW) which ensures a safe system of work to protect people from the system, but also limits human error by removing single point of failure through involvement of Authorized Persons (AP)

The Entity shall consider the specific requirements detailed in the NMA & FM Volume 11 – Quality.

6.9 Spare Parts

Having a spares/consumables inventory allows for quick decision making, if a failure occurs onsite. A list of spare equipment that can be accessed and used wherever standard practice applies, shall be in place. Clear description of part numbers, makes, models and quantities shall be captured. Ideally, this shall be part of CMMS information to retrieve material details whenever required.

CMMS systems will generally contain scheduling and procurement modules linked to the asset. This will also include functions for creating a work order, ordering parts, tracking and adjusting the parts and consumables on the system, and further make it efficient and interfaced to the entire maintenance program. This will assist in the monitoring of maintenance actives performed on an asset and provide information to stakeholders on current conditions and future investment required on spares, consumables and equipment life cycles.

These types of lists can be programmed to have minimum stock levels allowing reordering in place with procurement, as inventory levels of regularly used parts may be replenished. Additionally, using Just-in-Time processes may allow for parts to be contained within central warehousing facilities or vendor premises until needed, thereby, reducing associated costs of storage facilities to the Entity.

Inventory control process shall define critical/non-critical items and below elements shall be considered while developing the inventory details:

- High cost spares/consumables
- Long lead items

- Items obsolete in market
- High/Low use items
- Alternate material selection options
- Technical specifications
- Others

Parts/consumables with high failure rate shall be highlighted during maintenance activity and further analysis shall be performed to identify root cause analysis of the components failure. These components shall run up to their designed life in order to optimize efficiency and cost. Each Entity shall ensure that a Bill of Materials (BOM) is established for the security systems and associated equipment. An asset hierarchy shall be established with equipment criticality identified in order to develop:

- Maintenance strategy
- Spare parts list
- Critical spare parts list
- Running arrangements
- Risk assessments

The BOM shall include the following as a minimum:

- Part number
- Make and model
- Quantity
- Replacement cost
- Asset ID and location indicator

The Entity shall consider the specific requirements detailed in NMA & FM Volume 4 – Financial Planning, to develop a life cycle model and exercise obsolescence management for security systems and their associated components.

6.10 Security Systems Maintenance Methodology

6.10.1 Security Systems Maintenance

The maintenance team shall establish a periodic maintenance schedule for the security systems, based on experience, OEM manuals, and best practice guidelines. This schedule shall cover routine tests, visual inspections, and other planned maintenance activities against prescribed schedules to ensure reliability and continuous robust systems performance throughout their lifetime. A sample schedule has been appended within the document for reference purposes in **Attachment 1**.

The timely completion of planned maintenance tasks without compromising quality of the work will increase equipment reliability and service life. Depending on several factors, including failure history, impact of failure (asset criticality), and cost of equipment replacement; planned maintenance tasks shall be scheduled at a prescribed FQ by the Operations and Maintenance (O&M) person assigned to manage security system maintenance.

In the absence of OEM recommendations, the periodic maintenance schedule shall cover weekly, monthly, quarterly, biannual, or annual maintenance as a minimum. Maintenance activities shall be applied against system boundaries, which are based on asset tagging, asset hierarchy, and direction from the security systems supervisor.

In office facilities, as a minimum, the following inspections shall be made to maintain system integrity against the Basis of Design (BOD) and uninterruptable operational requirements.

The security systems maintenance shall incorporate the following critical points:

- Checking of controllers and supply power voltage
- Termination tags

- Panels shall be free from dust and debris
- Controllers network communication
- Checking and maintaining the integrity of data connections and cabling within risers and vulnerable areas, to prevent communication failure
- Checking and verification of the reliability and functionality of all security system workstations graphics and applications
- During maintenance, checking and verification shall be carried out to ensure monitoring system PC is free from unwanted programs and temporary files
- All gathered results and data shall be filled in PM sheets for references and use
- Visual inspection checks of the electronic security systems & CCTV surveillance systems
- Infrared Screening Tests (IST) for planned maintenance regimes
- Critical maintenance components e.g., external lighting luminaires, cameras, storage media, passive infrared sensors (PIRs), locking systems, card readers, batteries
- Visual verification of video recording devices, network hardware, and Uninterruptible Power Supply (UPS)
- Monitoring of communications, data infrastructure and items storage logs utilizing encryption protocols and access protection
- Emergency response protocol maintenance of access control system elements e.g., identification system, control system, facility restricted access (emergency lockdown), visitor control system
- Monitoring integrity of conductors, interconnecting wiring between various security systems
- Exterior structural detectors e.g., audio sensors, contacts (door and window), fiber optic, protective cabling, proximity, shock sensors, stress sensors, hold-up devices (e.g., potable, fixed-in-place), duress devices, ambush devices
- External buried detectors e.g., electromagnetic, fiber optic, leaky coaxial, seismic types
- Functional testing of access control system components such as controller, power supply, reader (e.g., key, magnetic stripe, Radio-Frequency Identification card, biometric), electric lock, electric latch, electromagnetic lock, position sensor along with their control units, primary power circuit disconnect, secondary power sources (e.g., batteries, voltage at end of test, generator records, power supply)
- Functional testing of video surveillance system components such as video controller, video switcher, video multiplexer, monitor, recorder (e.g., tape or DVR), camera (e.g., enclosure or Pan Tilt Zoom), alarming inputs and sequencing methodologies
- Functional testing of intrusion detection, hold-up and duress system components e.g., line security, supervisory signal, trouble signal
- Central equipment rooms/Cubicles used to house and protect surveillance and security equipment shall be maintained such that environmental parameters e.g. ambient temperature, humidity, mechanical impact/vibrations, dust/ moisture ingress do not adversely affect system operation or equipment operating life
- Regular system updates, patches, and necessary upgrades e.g., security, virus protection
- Licenses shall be renewed and copies kept at site, with contract details and list of authorized passwords kept securely, in accordance with site security protocols.

6.10.2 Pre-Requisites of the Maintenance

- **Tools/Specialized Tool Kits/PPE**
    - All software, databases, configuration tools, and analysis tools shall be used as needed during inspection and performance test
    - Measurement and calibration tolls shall be Portable Appliance Test (PAT) tested and National Institute of Standards and Technology (NIST) certified
    - Where necessary, calibration procedures shall be programmed within the CMMS for periodic testing
- **Risk Assessment Method Statement (RAMS)**
    - Risk assessment and a comprehensive method statement shall be in use as a safe practice of work. All results identified from risk assessments shall be documented and shall include and referred to method statement for the completion of maintenance tasks
    - A person performing maintenance activity shall be deemed and competent to carry out maintenance tasks on security and integrated equipment and systems
    - Shall have recognized qualification relevant to security systems and engineering

    - Shall have sufficient training and experience in security systems or electrical engineering field
    - JHA shall be carried by personnel carrying out maintenance
- **Permit to Work (PTW)**
    - Switching off any switch – fuse, power circuits, distribution boards, or mains circuit board that may affect any of the equipment associated to controllers and server shall be subject to PTW authorized by an engineer or manager of the facility
    - All PTW shall include an approved RAMS to perform maintenance tasks
    - Where required, a Lock Out Tag Out (LOTO) shall be applied to prevent inadvertent energizing of equipment during maintenance activities
- **Drawings/Schematics**
    - The drawings/schematics shall be included along with PTW to identify the point of maintenance activities, and consequences shall be marked up at planning stage to keep stakeholders who are aware about the maintenance activities
    - All security systems schematics as built drawings, shall be updated and in case any works have been carried out, all updated drawings shall be available for maintenance
- **Sequence of Operation (SOO)**
    - Maintenance task shall include SOO so that process and system, cause and effect shall be cleared and understood to all parties involved in the maintenance task
- **Redundancy Planning**
    - Storage architectures shall be scalable and utilize methods such as; monitoring of the storage devices, data stripping, data parity, and redundancy in a balanced configuration that delivers fault tolerance to protect against
        - Storage device failure
        - Primary power supply failure
        - Irrecoverable data corruption
        - Optimum storage capacity utilization
        - Optimum storage system rebuild/recovery time
- **Documentation**
    - Documentation is an essential element of maintenance tasks. Facilities operations team shall ensure that relevant documentation of the pre and post maintenance tasks to be available with facilities technicians, supervisors, and engineers to track maintenance logs/records. These shall be kept within the CMMS as digital copies for historical purpose and monitoring of system. Below documents shall be available within facilities team but not limited to:
        - Written maintenance plans and RAMS
        - SOO
        - PTW
        - Drawings/Schematics
        - Task matrix sheets
        - Work orders to record non-conformities
        - Others site-specific
        - Completed job orders and maintenance reports
        - O&M documentation

Contained within **Attachment 1** is a Security Systems Maintenance Schedule presented in the form of a checklist. The Entity shall use the format presented within attachment 1 to prepare its own site specific security systems PM Schedule. While preparing its own PM schedule, the Entity shall ensure that aforementioned requirements are reflected as applicable, and that site specific considerations are included in consideration with OEM guidelines.

7.0 ATTACHMENT

Attachment 1: EOM-ZM0-TP-000187 – Security Systems Planned Maintenance Schedule for Offices

Attachment 1 – EOM-ZM0-TP-000187 Security Systems Planned Maintenance Schedule for Offices

An example task instruction sheet for security systems is featured below. The Entity shall use it as a basis by which to develop its own site specific task instruction sheets for maintenance of security systems.

Skill Types

- Specialist Engineer (SE) (Security Systems)
- Extra Low Voltage (ELV)
- Maintenance Engineer (ME)

Item	FQ	Action	Skill Level
Electronic Security Systems (ESS)	Biannually	Check functionality of primary and secondary drive	SE
Primary drive and secondary drive			
Visually inspect system connections		Conduct physical inspection of all terminals	
System faults		Check for system faults	
Hard disks		Check space in hard disk	
Delete/Archive log files as necessary		Check for unwanted files and archive	
Clean Monitor Screen	Annually	Clean screens	
Complete a data archive		Check and archive irrelevant data as applicable	
Complete hard drive defragmentation		Integration check, layout of files. Do process run as necessary	
Verify operating systems file integrity	Biannually	Check for corrupted files, database, software files	
Verify Program File Integrity	Biannually		
Verify data file integrity	Annually	Follow manufacturer step by step instructions to perform these checks	SE
Perform a virus scan			
Authenticate system operators and privileges			
Check field panel communications			
Inspect field panel wiring and connections			
Workstations, CPU, and UPS are clean and without any trouble			
Ports connectivity/Ethernet Switches			
Sensors and controllers are healthy and functioning			
Hardware communication with server			
Access Control System			
Batteries	Annually	Test field panel battery levels	SE
Power Supply	Annually	Check function	
Key	Annually	Check function	
Magnetic Stripe	Annually	Check function	
Readers	Annually	Check card reader operations	
RFID card	Annually	Check function	

Item	FQ	Action	Skill Level
Biometric	Annually	Check function	
Position Sensors	Annually	Check function	
Electric latch	Annually	Check function	
Electric Lock	Annually	Check function	
Electromagnetic lock	Annually	Check function	
Manual/Auto Operation	Annually	Check function	
Electric hardware	Biannually	Clean, lubricate, and adjust locks	
	Biannually	Verify door contact operation	
	Biannually	Inspect, clean, and adjust card printers	
	Biannually	Inspect, clean, and adjust image capture camera	
CCTV Surveillance Systems			
Visually inspect CCTV monitor image quality	Monthly	Conduct Visual Inspection	ME
Visually inspect CCTV recording equipment	Monthly	Conduct Visual Inspection	ME
Inspect video record and playback operations	Monthly	Conduct Visual Inspection	ME
Check CCTV system switcher operation	Weekly	Conduct Visual Inspection	ME
Cameras primary input power	Weekly	Conduct Visual Inspection	ME
Video signal transmission	Weekly	Conduct Visual Inspection	ME
Check PTZ operation		Functionality of camera, left, right, up, down, zoom functions, customization	SE
Visually inspect CCTV system connections	Annually	Cable termination checks, POE checks, and communication ports	ME
Clean Monitors Screens	Monthly	Conduct inspections for cleaning and ensure displays are clear	ME
Inspect, clean, and adjust cameras according to facility requirements	Annually	Ensure to consider weather conditions and may more frequent checks required	ME
Alarming inputs	Annually	Check alarm functions	SE
Intruder Alarm System			
System Integrity	Annually	Record and report any evidence of tampering or damage	ME
Sensors and contacts		Confirm correct operation and sensitivity, where appropriate check spatial configuration for volumetric devices	
Alarm signals		Check response to signal at con troll panel. Reset alarm points after test	
Sensor covers, terminal boxes and fixings		Check integrity for signs of overheating, ingress of dust and moisture. Clean internal components with soft brush and remove any dirt or fluff. When replacing covers, check operation of any tamper switches which may be fitted	
Power supplies	Biannually	Check power supplies and associated batteries. Batteries should be checked for signs of leakage or corrosion	SE
Detection modules exterior (if applicable)	Annually	Check and adjust (if necessary)	SE
Detection modules interior (if applicable)	Annually	Check and adjust (if necessary)	SE

Item	FQ	Action	Skill Level
Batteries	Annually	Check function and state of battery charger Check battery terminals connections Check that the inter-cell connections are secure and clean	SE
Sealed lead acid, sealed nickel-cadmium	Triennially	Check and dispose batteries in accordance to facility Entity environmental regulations	SE
Control Panel	Annually	Check control panel internally, check all control devices, fuse bridges, and phase barriers for signs of arcing and burning. Check all indication lamps are working, replace any defective lamps Check panel/cabinet door, if securely locked, and that door protection and isolation device is operative	SE
External Lighting			
Inspection of streetlights	Monthly	Look for breakages, wear/deterioration/signs of corrosion	ME
		Check any missing parts, screws, covers, loose fittings	ME
Electrical wiring and connections	Biannually	Check the integrity and look for Sign of burn/spark, loose connection, expose cabling	ME
		Inspect for grounding and bonding arrangements	ME
		Check the accessibility to conductor and connections	ME
Security of light fittings		Check for cleaning, condition, and security of fittings	ME
Lamps/Tubes		Check for faulty or blackened tubes or lamps	ME
Controls		Check for functionality and correct operation of timer and sensor (if available)	ME
Ingress Protection (external lights)		Check and ensure fitting integrity is maintained	ME
Vehicle Blockers/Bollards			
Bollard Function	Quarterly	Follow OEM inspection and maintenance guidelines	SE
Control Function	Quarterly		SE
Physical Conditions	Quarterly		SE
Leaks	Quarterly		SE
Cabling Connectivity	Quarterly		SE
Communication	Quarterly		SE
Sounding Devices	Annually	Check functions	SE
Batteries	Annually	Conduct general tests	SE
Off premises transmission equipment (if any)	Quarterly or by automatic monthly test	Check functions	SE
All interface equipment	Annually	Check functions	SE