National Manual of Assets and Facilities Management

Volume 5, Chapter 11

Communication Systems Operations – Schools & Universities Procedure

Document No. EOM-ZO0-PR-000053 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

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 5
2.0 SCOPE 5
3.0 DEFINITIONS 5
4.0 REFERENCES 8
5.0 RESPONSIBILITIES 8
5.1 Responsibility for Controlling Access to Infrastructure Assets / Communication Rooms 9
6.0 PROCESS 10
6.1 Communication System 10
6.2 Core Communication Assets 10
6.3 Internal Communication Assets 11
6.4 Communication System Applications 11
6.5 Communication System Pathways 12
6.6 Communication Systems Infrastructure Management 12
6.6.1 Infrastructure Alarms Management 14
6.6.2 Infrastructure Risk Management 14
6.6.3 Infrastructure Redundancy 15
6.6.4 Planned/Unplanned Shutdown 15
6.6.5 Documentation 15
6.6.6 Work Control Operations 15
6.6.7 KPI/SLA Monitoring 16
6.7 Infrastructure Management 16
6.7.1 Spatial Arrangements 16
6.8 Operation Procedures 17
6.8.1 Startup Procedure 17
6.8.2 Shutdown Procedure 17
6.8.3 Daily Reporting/Monitoring 17
6.8.4 Emergency Response Actions 18
7.0 ATTACHMENTS 19
Attachment 1 – EOM-ZO0-TP-000243 – Startup Checklist 20
Attachment 2 – EOM-ZO0-TP-000244 – Shutdown Checklist 21
Attachment 3 – EOM-ZO0-TP-000245 – Daily Monitoring Checklist 21
Attachment 4 – EOM-ZO0-TP-000246 – Emergency Response Action Checklist 23

1.0 PURPOSE

The purpose of this document is to provide an Entity and/or Facilities Management Company (FMC) with guidelines for the improvement, development, and enhancement of communication systems operations management in the schools and universities. Furthermore, its purpose extends to provide a range of essential competencies that communication systems specialists in an Entity should possess in order to achieve efficient and reliable operations.

2.0 SCOPE

The scope of this document includes communication infrastructure that will allow data, voice, and digital networks to operate in the facility. This document does not deal with the specifics of individual systems, as this would generally be undertaken by specialist service providers.

The systems that an Entity would typically expect to possess in a facility are highlighted, and guidance is provided for the development of procedure for effective operations management of these systems, to maintain a high level of efficiency and reduce disruption.

This document is primarily focused on the core assets of communication infrastructure that require continuous operations monitoring and management. The information contained in this document has been developed from international standards and best practice to enable the Entity to develop and improve or enhance the operations management of the communication systems found in the schools and universities. It will also support the Entity to achieve an understanding of the following:

- Elements involved in effective operations management
- Operations monitoring to optimize communication systems efficiency
- Network availability
- Network resilience
- Network speed and security

For the purpose of this document, a “school or university” has been defined as a form of building or facility which contains spaces designed to be used for teaching, training, or instructing students. Types of facilities considered within the document are as follows:

- Universities
- Schools
- Smaller regional schools (nursery schools)

3.0 DEFINITIONS

Term	Definition
Clean Agent	An electrically non-conductive, volatile, or gaseous fire extinguishant that does not leave a residue upon evaporation
Communication	Any transmission, emission, and reception of information (e.g., signs, signals, writings, images, sounds) by cable, radio, optical, or other electromagnetic systems
Emergency Systems	Those systems that are legally required and classified as emergency systems by codes or by governmental agency having jurisdiction. These systems are intended to automatically supply illumination, power, and cooling to designated areas and equipment in the event of failure
Ladder Rack	A cable tray with side stringers and cross members resembling a ladder, which may support cable either horizontally or vertically
Monitor/Head End PC	Oversee engineering equipment systems status for monitoring and control of operations

Term	Definition
Parameter	The name of a unit or metric e.g., pressure, hertz, temperature
Permit-To-Work	A documented safety management system adopted by most organizations for management of work activities
Raceway	An enclosed channel of metallic or non-metallic materials designed expressly for holding wires or cables
Rack	An open structure for mounting electronic and electrical equipment
Redundancy	Providing secondary components that either become instantly operational or are continuously operational so that the failure of the primary component will not result in failure
Riser	• Vertical section of cable (e.g., changing from underground or direct buried plant) • The space used for cable access between floors
Service Provider	An operator or third party specialist of any communication service who delivers content (transmission) over access provider facilities
Space (Telecommunications)	An area whose primary function is to house the installation and termination of communication equipment and cable (e.g., entrance room, Telecommunication room (TR), hub room, Network Distribution Room (NDR), or data center)
Switch (Network)	A network access device that provides a centralized access point for Local Area Network (LAN) communication, media connections, and management activities where each switch port represents a separate communication channel. It usually comes under IT or third party specialist's responsibility
Test	Confirming by means of observation or measurement that the system meets the expected and/or acceptable requirements
Uptime	The period of time, usually expressed as a percentage of a year, in which the Information Technology Equipment (ITE) is operational and able to fulfill its mission
Acronyms	
AMS	Asset Management System
ANSI	American National Standards Institute
AP	Authorized Person
ASHRAE	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
ATS	Automatic Transfer Switch
BIA	Business Impact Analysis
BICSI	Building Industries Consulting Service International
BMS	Building Management System
BSI	British Standards Institution
CAFM	Computer-Aided Facility Management
CCTV	Closed Circuit Television
CIBSE	Chartered Institution of Building Services Engineers
CMMS	Computer Maintenance Management System
CP	Competent Person
CPU	Central Processing Unit
DARS	Digital Audio Radio Service
DAS	Distributed Antenna System
DC	Direct Current
DSL	Digital Subscriber Lines
ELV	Extra Low Voltage
EMI	Electromagnetic Interference

Term	Definition
ERAP	Emergency Response Action Plan
ERP	Emergency Response Plan
EVC	Electronic Verification Code
FDD	Fault Detection and Diagnostics
FM	Facilities Management/Manager
FMC	Facilities Management Company
FTTH	Fiber to the Home
GSM	Global System for Mobile
HSQE	Health, Safety, Quality & Environment
HVAC	Heating, Ventilation, and Air Conditioning
IEC	International Electro-technical Commission
ISA	Instrumentation, Systems, and Automation
ISO	International Organization for Standardization
IT	Information Technology
ITC	Integrated Telecom Company
ITE	Information Technology Equipment
KPI	Key Performance Indicator
KSA	Kingdom of Saudi Arabia
LAN	Local Area Network
LEED	Leadership in Energy and Environmental Design
LOTO	Lock Out Tag Out
MEP	Mechanical, Electrical, and Plumbing
MMF	Multi-Mode Fiber
NDR	Network Distribution Room
NETPOP	Network Point of Presence
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NMA&FM	National Manual of Assets and Facilities Management
OEM	Original Equipment Manufacturer
OSHA	Occupational Safety and Health Administration
PAN	Personal Area Network
PAT	Portable Appliance Test
PAVA	Public Annunciation and Voice Alarm
PC	Personal Computer
PPE	Personal Protective Equipment
PSTN	Public Switched Telephone Network
PTW	Permit-To-Work
RAMS	Risk Assessment and Method Statement
RFI	Radio Frequency Interface
SLA	Service Level Agreements
SMF	Single-Mode Fiber
SOP	Standard Operating Procedure
STC	Saudi Telecom Company
TR	Telecommunication Room
UPS	Uninterruptible Power Supply
VDU	Visual Display Unit
WLAN	Wireless Local Area Network

Table 3: Definitions and Acronyms

4.0 REFERENCES

- American National Standards Institute (ANSI)
- American National Standards Institute (ANSI/ISA 18.2) – Alarm Management Standard
- British Standards (BS 5839) – Fire Detection and Fire Alarm Systems for Buildings
- Chartered Institution of Building Service Engineers (CIBSE)
- Information and Communication Technology (ICT) – Building Industry Consulting Service International (BICSI)
- International Electro-technical Commission (IEC 60870)
- International Organization for Standardization (ISO 55000) – Asset management: Overview, Principles and Terminology
- International Standards Organization (ISO 9001) – Quality Management Systems
- National Fire Protection Association (NFPA 297) – Communication Systems
- National Institute of Standards and Technology (NIST)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 10 – Health, Safety, Security, and Environment (HSSE)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 11, Chapter 5 – Quality Control Procedures
- National Manual of Assets and Facilities Management (NMA&FM) Volume 11 – Quality
- National Manual of Assets and Facilities Management (NMA&FM) Volume 12 – Risk Management
- National Manual of Assets and Facilities Management (NMA&FM) Volume 5, Chapter 4 – HVAC Systems Operations – Schools & Universities (EOM-ZO0-PR-000011)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 5, Chapter 5 – BMS Operations – Schools & Universities (EOM-ZO0-PR-000017)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 5, Chapter 6 – Instrumentation Systems Operations – Schools & Universities (EOM-ZO0-PR-000023)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 5, Chapter 7 – Mechanical Systems Operations – Schools & Universities (EOM-ZO0-PR-000029)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 5, Chapter 8 – Electrical Systems Operations – Schools & Universities (EOM-ZO0-PR-000035)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 5, Chapter 9 – Security Systems Operations – Schools & Universities (EOM-ZO0-PR-000041)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 5, Chapter 10 – Life Safety Systems Operations – Schools & Universities (EOM-ZO0-PR-000047)
- National Manual of Assets and Facilities Management (NMA&FM) Volume 5, Chapter 12 – Escalators & Lifts Operations – Schools & Universities (EOM-ZO0-PR-000059)
- Occupational Safety and Health Administration (OSHA) – Occupational Safety and Health

5.0 RESPONSIBILITIES

Only trained and competent persons shall be appointed by management to perform operations management tasks on communication systems.

Role	Description
Entity	Governmental Entity having jurisdiction over schools and universities
The Responsible Person (RP)	The RP, employed directly by the Entity, is the “Duty Holder” of the communication systems and the staff who operate those systems, and has overall responsibility for their design, installation, operations, and maintenance. The RP has a legal responsibility of ensuring that the Entity has complied with the relevant legal regulations pertaining to communication systems and the staff involved.

Role	Description
	The RP shall ensure that the systems are kept up to date with the latest relevant legal regulations. The RP shall not be the Authorizing Engineer (AE)
Facilities Manager (FM)	The Facilities Manager representing the FMC, in collaboration with the client, controls the operations management of communication and other engineering systems; who is responsible and accountable for the APs and CPs as well as the site communication systems, maintenance, and ensuring that control of those systems is in-line with the client SOP for the operations management
The Authorizing Engineer (AE) (Independent)	The AE is appointed by the Responsible Person (normally under the recommendation of the client), to take responsibility for the effective management of the safety guidance The AE shall possess the necessary degree of independence from local management to take action where necessary and alert the Chief Executive (in the event the local management do not take action to avoid harm)
Authorized Person (AP)	A person who has been appointed by the AE (or by an authorizing body in the Entity); who is trained, competent, skilled, experienced, responsible, and has gained the necessary site knowledge, to operate and maintain the system in a controlled and safe manner. The AP is responsible for work or testing carried out on the system
Competent Person (CP)	A person with the necessary training and relevant experience, and who has been appointed by an AP (or by an authorizing body in the Entity), after conformation of competence, knowledge, skill, and experience. The CP can execute the required actions within a Permit to Work (PTW) and/or other directional documents as may be assigned to him
Communication Systems Operator	An authorized individual who operates the communication systems
Operations and Maintenance Person	An individual of the engineering staff, communication, manufacturer, or operations management organization, employed by management to carry out duties on communication assets
Health, Safety, Quality, and Environment (HSQE) Manager	The operations HSQE Manager shall ensure that safe practices are undertaken and conduct periodic inspections of these areas HSQE Manager shall also establish a strategy using Business Impact Analysis and Business Continuity Tools to manage and minimize risk from service interruptions

Table 4: Roles and Responsibilities

5.1 Responsibility for Controlling Access to Infrastructure Assets / Communication Rooms

It is the responsibility of the Entity to ensure that all assets are protected and secured from unauthorized entry. These shall be protected from unauthorized entry to avoid loss of communication services in the Entity facilities, which could seriously impact operations or business continuity. The Entity shall ensure that processes and systems are in place for surveillance of and for authorized access into the communication rooms, cable shafts, cable risers, and other associated communications assets.

External ducts to the facility shall be monitored for building works that may affect supporting accessories of the communication systems e.g., risers, cable trenches, cable arrangement entry points, fire insulation/sealant/foam to fix and fill holes.

Personnel attending the facility should be vetted to ensure that they are familiar with policies, special procedures, and any site restrictions. Their induction should be followed by registration with the site security to ensure untrained personnel do not access vulnerable areas. All contractors shall also directly report to the site security upon arrival at site.
Communications rooms and risers shall be locked and/or secured at all times, and where access control is operational, regular reviews should be undertaken to ensure the validity of staff access. A review process shall be undertaken to ensure that an effective access control mechanism is in place to avoid unauthorized entries to these critical areas.

6.0 PROCESS

6.1 Communication System

The primary purpose of communication systems is to provide effective, secure, and resilient audio, visual, and data systems that support the operations of a school or university. A reliable infrastructure is critical for the accurate, effective, and safe operations of communication services. The overall system shall only be considered “fit for purpose” when all elements are collectively working as expected and delivering the desired results.

Communication assets need to be effectively monitored to ensure 100% uptime of the critical services, without operational disruptions. This support is required to maintain high operating standards of these services and mitigating the downtime, which could otherwise affect the Entity’s business function and its staff, students, and visitors.

In schools and universities, there are specialized operations that are performed through various communication protocols, which as a result, have increased the need for Information Technology (IT) and other specialized communication media to support internal and external stakeholders.

Communication systems play a significant role in supporting organizations globally under normal, emergency, and exceptional circumstances. They also support a wide range of services, and data collection and analysis in the utilities system network in a school or university.

IT data networks are not covered in this document; external resources should be consulted, especially, in relation to data confidentiality and IT infrastructure.

6.2 Core Communication Assets

The list provided below is not intended to be exhaustive, only including typical core assets supporting the communication infrastructure of the schools and universities:

- Closed Circuit Television (CCTV)
- Communication risers and raceways
- Communication room – access control
- Communication lines
- Data cables and accessories
- Data connectivity management systems
- Digital and analogue fiber optic transmission links
- Heating, Ventilation, and Air Conditioning (HVAC)
- Leased lines
- Lifts Communication – Auto Dialer
- Public Annunciation and Voice Alarm (PAVA)
- Public Switched Telephone Network (PSTN)
- Routers
- Telephone infrastructure
- Tunnels from street levels to communication room

- Electrical and HVAC services

The operations management of the above communication components shall be the responsibility of Entity and/or FMC.

6.3 Internal Communication Assets

The list provided below is not intended to be exhaustive, only including typical internal communication assets found in the schools and universities:

- Attack alarms
- Audio alarms
- Digital networks
- Headsets
- Integrated communication services
- Intercoms
- Intruder alarms
- Mimic indicators
- Global System for Mobile (GSM) networks
- Network systems infrastructure
- Radio services
- Staff communication base
- Teleconsultation
- Telephone systems
- Televisions
- Videoconferencing
- Wi-Fi network

The operations management responsibility for these assets shall be with IT services or third-party specialists.

6.4 Communication System Applications

Some schools and universities consist of typical communication applications including, but not limited to:

- Management and business information systems
- Automation and control communication systems
- Radio communications
- Network management
    - Personal Area Network (PAN)
    - LAN
    - WLAN
    - Others
- Land line phones/intercoms/mobile phones/smart work management devices
- Closed Circuit Television (CCTV) cameras, access control systems, security and facility operations control center
- Office equipment, such as Personal Computers (PC) servers, desktops, and printers
- Public display units and fixtures, such as televisions and clocks
- Local base stations, such as internal/external antennae and towers, satellite base stations and dish antennae
- Leased and rental antenna systems for cellular networks
- Engineering systems function and data management

6.5 Communication System Pathways

It is essential that the communication systems pathways/routes are secure and accessible for the operations team during inspection and fault-finding or rectification processes. The elements listed below may be found in cable risers, either concealed or surface mounted and require periodic inspections to ensure end user safety and the integrity of the connected systems.

Communication systems contain various pathway/routing components including, but not limited to:

- Fiber optics, including Single-Mode Fiber (SMF) or Multi-Mode Fiber (MMF)
- Digital Subscriber Lines (DSL)
- Distributed Antenna Systems (DAS)
- Hub rooms
- Telecommunication rooms (TR)
- Service risers/cabinets
- Cable ducts/Conduit/Trays
- Fire proofing
- Raceways/conduits/trunking
- Various connectors
- Grounding/Bonding/Junction boxes

Figure 1 shows block diagram of a typical communication systems network.

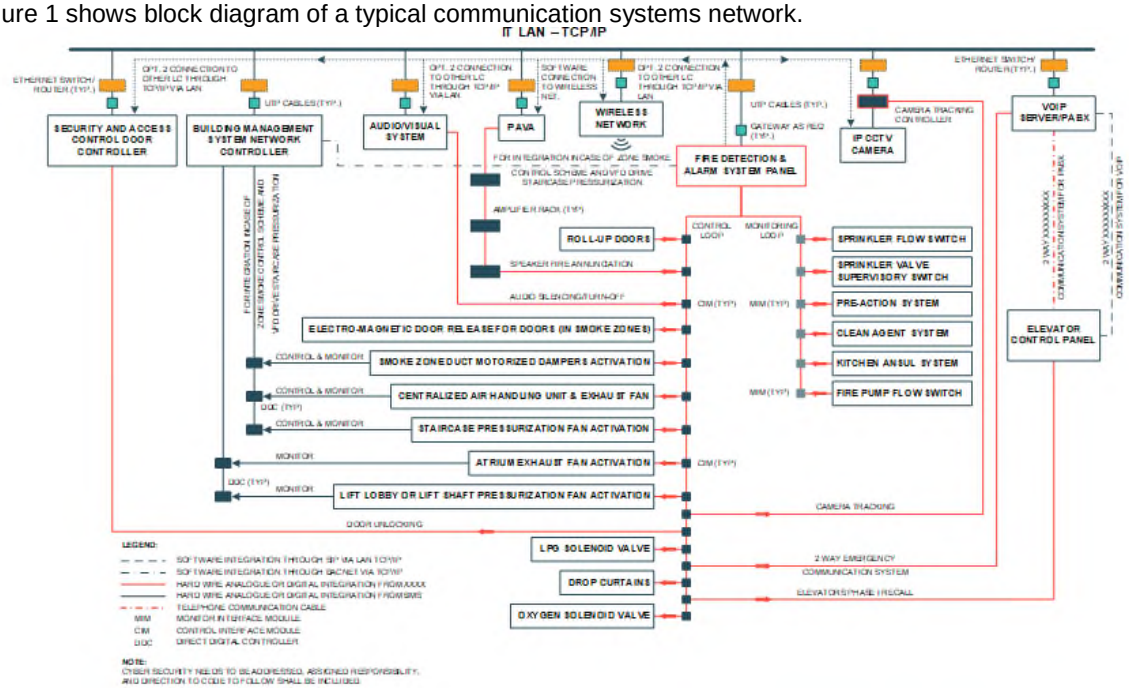

Figure 1: Typical Communication Systems Network

6.6 Communication Systems Infrastructure Management

Due to the critical nature of these communication systems, spaces where assets are installed shall be maintained in a strictly controlled manner including, but not limited to, climate control, power backups, Uninterruptible Power Supply (UPS), and security management.

The Entity shall arrange for the monitoring and periodic inspection of a facility's communication infrastructure as specified in Original Equipment Manufacturers (OEMs) recommendations and the requirements of statutory compliance.

There are a number of communication assets and systems that require statutory maintenance and inspections. These assets are normally associated with emergency power supply assets, life safety assets, and security e.g., PAVA, fire detection, suppression systems.

For further information on specific statutory requirements and obligations regarding the infrastructure assets, see NMA&FM references in Section 4.0.

Figure 2 below provides the block diagram of communication systems riser distribution.

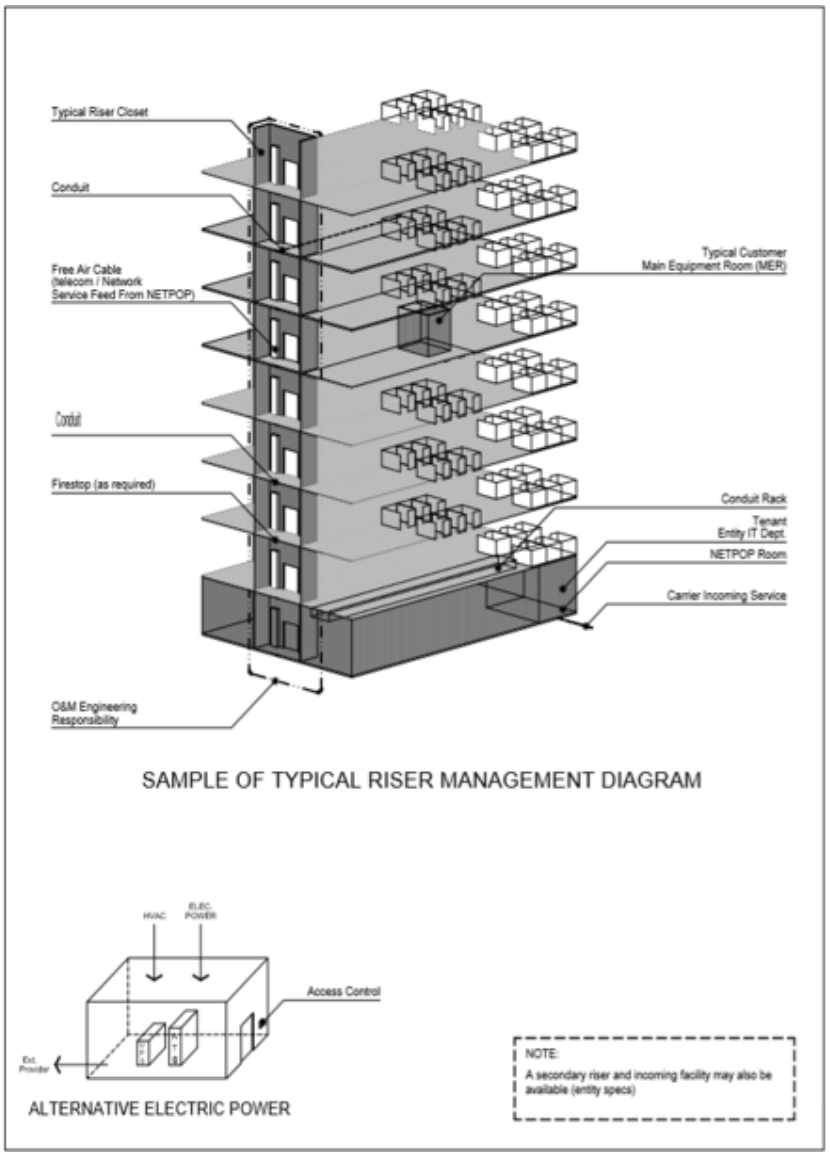

Figure 2: Typical Communication Systems Riser Distribution

The Entity shall ensure that these assets are identified and periodically inspected. In addition to the effective management of the infrastructure, it is also crucial that contractors and staff carrying out the tasks are demonstrably competent.

6.6.1 Infrastructure Alarms Management

Due to multiple parties' involvement in managing communication systems functions, it is essential to have an agreed scope of activity for all relevant stakeholders, defining clear roles and action plans.

The Entity shall ensure that a process is in place between the tenant, third party specialist, and FMC to manage infrastructure and communication service providers such as Saudi Telecom Company (STC), Zain, and ITC.

The Entity and/or FMC shall only be responsible for the facility infrastructure, and not the assets located in tenanted areas.

The service scope may cover following level of responses, but not be limited to:

- **Level 1 Response**: This may be defined as an initial response to any report in terms of defects found in the infrastructure, power issues, operational malfunction detected in any of the communication systems core assets or pathways/routing components.The operations team can provide a response during Level 1 issues, which should not have any impact on communication services
- **Level 2 Response**: This may be defined as an IT related issue or network issue from a specialist service provider. Operations team shall not be responsible for these issues. However, work activities overseen by the operations team in these secure areas that come under the FMC shall have their Risk Assessment and Method Statement (RAMS) applied
- **Level 3 Response**: Communication outage, IT component failure, specialist system outage and overload alarms shall be managed by tenant, IT, or the specialist service contractor providing data and communication services

6.6.2 Infrastructure Risk Management

In the development of communication systems operations management processes, it is essential to assess and analyze the risks associated with inappropriate operation, unexpected breakdown or power outage, and air conditioning outage, which could affect the educational Entity's communication services. These include typical situations including, but not limited to:

- Breach of statutory obligations
- Emergency situations
- Asset loss or system failure, including consequential financial loss
- Creating an unhealthy or unsafe environment and consequential liabilities
- Risk of harm to the environment
- Reduced asset life
- Inefficient operational performance
- Adverse stakeholder perception

These spaces shall be kept away from sources including, but not limited to:

- Heat
- Moisture
- High voltage
- Corrosive atmospheric or environmental conditions
- Radio Frequency Interface (RFI)
- Electromagnetic Interference (EMI)

The restricted communication rooms and areas shall not be used for material storage, and access and egress shall be strictly controlled. Combustible substances or materials shall be excluded from these restricted areas.

6.6.3 Infrastructure Redundancy

Critical systems in any school or university shall have redundant sources available in order to maintain 100% uptime without any disruptions in the facility's services. Fire alarm, planned/unplanned shutdowns, and natural disasters can potentially lead to long-term facility outage. The operations team shall be aware of the functions of redundant equipment or systems that can be operated in manual or auto mode. Therefore, it is important that periodic inspections are performed on these redundant systems to ensure their continued operation.

Facility IT department and/or third party specialists shall be responsible for the redundant systems associated with internal communication network and IT.

6.6.4 Planned/Unplanned Shutdown

Any shutdown of the communication systems shall be planned, insofar as is reasonably practicable and communicated to all stakeholders in advance. If an unplanned shutdown is unavoidable, the impact on the services shall be assessed and interim contingency plans shall be communicated to all operations teams and stakeholders.

Activities associated with IT services or assets under third party service provider responsibility, shall not be managed by the operations team. Site specific RAMS and Permit-To-Work (PTW) process shall be followed by the parties involved in performing and managing such works.

6.6.5 Documentation

Operations management documentation is necessary for the successful and continuous operation of the communication systems and for other services dependent on these systems. Managing an updated and current inventory and asset register with key information on how to operate, request for service, track warranty, and assess in the event of an emergency are essential features and shall be available in the communication rooms.

The following are considerations needed for the operations management of communication systems and their associated assets in a facility, but not limited to:

- Copies of certificate of compliance with relevant standards
- Data sheets for communication equipment
- Drawings/schematics
- Escalation matrix
- Instructions for any precautionary measures
- Location details
- Warranties
- Installation and commissioning dates and details of the commissioning organization
- Status in operation/out of operation
- Mains power
- Standby power
- Backup switching sequence
- Startup switching sequence
- Shutdown and restart sequence
- Access points and communication room security codes
- Panel keys and security lock
- Emergency infrastructure

6.6.6 Work Control Operations

The Entity shall ensure that quality standards are built into the infrastructure's operations management processes. The Facilities Manager shall ensure that inspection, retrofit by specialist service provider or any tenant activity, takes place in a controlled and effective way to mitigate any hazard or risk to the wider communications infrastructure or stakeholders.

Any planned or unplanned work that could potentially impact on communication assets, internal components, and pathways shall be managed with due diligence.

The operations team shall have a PTW and RAMS process in place to assess and control the work activities in order to avoid any impact to operations. It is advisable to assign communication systems operations staff to escort and monitor contractors where communications equipment or services are present.

For further information on specific requirements, refer to NMA&FM Volume 11 – Quality.

6.6.7 KPI/SLA Monitoring

Communication systems are key sub-systems in a facility that provide essential support during both normal and emergency operations and maintaining them in an operable condition at all times shall be considered as an essential requirement. A contracted service level with a defined Service Level Agreement (SLA) Key Performance Indicators (KPIs) associated with communication shall be established between relevant parties e.g., performance guarantees associated with restoration of communications networks with local telephone/internet service providers, such as STC and Mobily.

6.7 Infrastructure Management

The operations team shall establish inspection regimes and frequencies similar to other critical assets in the schools and universities. This will ensure that the long-term strategic plans address current and future needs of the communication operations.

The management of communication systems operations should undertake continuous monitoring of the infrastructure including, but not limited to:

- Power/panel rooms (e.g., UPS, Automatic Transfer Switch (ATS))
- Precise air conditioning (e.g., closed circuit units, precision air conditioners, computer room air conditioning
- Humidity controls
- Fire protections systems
- Wireless networks
- Raised flooring and void space
- Water detection systems and alarms
- Redundant power sources
- Critical/non-critical power sources
- Fire proofing
- Access security
- Others

6.7.1 Spatial Arrangements

Operation teams should carry out periodic inspections and manage changes to the spatial arrangements of the communication equipment including, but not limited to communication lines, data cables, routers.

6.8 Operation Procedures

6.8.1 Startup Procedure

A startup procedure is a reference document to be used when preparing the process to operate a system from an offline position. The actions in the procedure are intended to ensure that a methodical approach is taken when bringing any communication system or associated infrastructure back online.

A startup procedure shall include the following:

- Health & Safety
- Pre-approvals
- System readiness
- Pre-start checks
- Start checks
- Notifications

This process shall be followed by the operations team meant to perform communication systems startup up listed in Section 7.0. Refer to **Attachment 1** for full generic communications infrastructure startup procedure.

6.8.2 Shutdown Procedure

A shutdown procedure is a reference document to be used for a planned activity to take a system or a piece of equipment offline. The shutdown procedure should be clear, prescriptive, and well understood.

The specific steps often mirror those of the startup procedure but include additional consideration for the effect on utilities and other connected building services. A shutdown procedure for communication systems or associated services such as HVAC and power shall include, but not be limited to, the following:

- Health and Safety
- Pre-approvals
- Standby system condition
- Pre-shutdown checks
- Routine stop
- Post-stop checks
- Notifications

This process shall be followed by all parties listed in Section 7.0. Refer to **Attachment 2** for full generic communications infrastructure shutdown procedure.

6.8.3 Daily Reporting/Monitoring

External facilities should be monitored by Entity management and maintenance teams as communications infrastructure extends beyond the Entity's buildings' boundaries. Works undertaken beyond the boundaries of properties, such as roadworks can contribute to the potential failure of communication systems. Therefore, close monitoring of vulnerable entry points should be a part of the security personnel inspection activities.

Key Performance Indicators (KPIs), which are agreed upon between the FMC and the specialist contractor e.g., Work Order (WO) completion times are within an agreed threshold time, recorded as a percentage for the KPI, graded according to % category, i.e.

Work Order Completion Times KPI Result %	Grading
95%<100%	Excellent
80%<94%	Good
70%<79%	Room for improvement
50%<69%	Poor
0%<49%	Unacceptable

Table 2: Typical KPI Performance Grading

The Facilities Manager at a school or university shall monitor the following:

- Analyze energy high consumption areas in the building and its different systems to look for savings opportunities. A custom-made report could be set to determine the power consumption in case of separate billing for tenants
- Power quality and energy usage monitoring, in relation to communications infrastructure
- Work Orders (WO) under the Computer (or paper-based) Maintenance Management System (CMMS) should be actioned in accordance with the agreed contract requirement and standards
- Assets related to communications infrastructure in the CMMS should be audited and kept up-to-date as per the agreed contract requirement and standards
- Staff training matrix should be visible and kept up-to-date by clarifying roles and responsibilities. Staff training should be relevant and include any new applicable statutory and mandatory legislation. A percentage of operational staff should be first aid trained as per the site requirement
- Review of training and competencies, and organization of refresher or additional courses
- Regular checks must be carried out to ensure that operations remedial actions are swiftly followed in order to ensure that minor faults do not become showstopper. Moreover, WOs must be closed within specified Service Level Agreements (SLAs)

The Entity should consider the requirements detailed in NMA&FM Volume 5 – Operations Management (Chapters 4,5,6,7,8,10, and 12), while specifying operations monitoring of infrastructure assets.

See **Attachment 3** for full generic communications infrastructure monitoring/daily rounds checklist.

6.8.4 Emergency Response Actions

Emergency response actions shall be in writing, including designated actions, to ensure staff, students, and visitors' safety from fire and other emergencies.

The following elements, at a minimum, shall be included in the procedure:

- Emergency escape procedures and emergency escape route assignments
- Designated muster points
- Procedures to be followed by employees who remain to operate critical operations before they evacuate
- Procedures to account for all employees after emergency evacuation has been completed
- Details of Fire Wardens and First Aiders preferred means of reporting fires and other emergencies
- Names, job titles and contact information for personnel or departments who can be contacted for further information or explanation of duties under the plan

This procedure shall be communicated to all stakeholders with responsibility to manage such emergency situations. Post-incident reviews and desktop tests of the procedure should be performed to ensure the effectiveness of control measures

Emergency procedures shall include the critical assets of the communication systems that need to be monitored or switched to a 'fall back' role. In particular, radio and telephone systems that may be required for reporting of functions of the life safety systems in a facility or assist with Civil Defense activity.

The Entity should consider the specific requirements detailed in NMA&FM Volume 5 – Operations Management (Chapter 4,5,6,7,8,10, and 12), while developing emergency responses.

See **Attachment 4** as an example for communications infrastructure emergency response actions.

7.0 ATTACHMENTS

1. EOM-ZO0-TP-000243 – Startup Checklist
2. EOM-ZO0-TP-000244 – Shutdown Checklist
3. EOM-ZO0-TP-000245 – Daily Monitoring Checklist
4. EOM-ZO0-TP-000246 – Emergency Response Plan Checklist

Attachment 1 – EOM-ZO0-TP-000243 – Startup Checklist

Building Name:		Reference No.	REV:00A		
No.	**Startup Procedure Checklist**		**CHECKED SATISFACTORY**		
			N/A	**YES**	**NO**
	Communication Systems – Schools & Universities				
	Pre-approvals				
1	Inspect risers and trunk trays (secured properly and not loose, check for corrosion and moisture)		☐	☐	☐
2	Availability of System owner/Manager/Engineering Teams' approvals		☐	☐	☐
3	Task and documentation complete/Work order has been signed off		☐	☐	☐
4	Availability of Quality, Health, Safety, and Environment Management's (QHSE) approvals		☐	☐	☐
5	Specialist contractor's schedule of work		☐	☐	☐
6	Availability of approved PTW/OEM procedure		☐	☐	☐
7	Availability of end user department head's approvals		☐	☐	☐
	Communications inspection				
8	Inspect risers and trunk trays (secured properly and not loose, check for corrosion and moisture)		☐	☐	☐
9	Inspect Water Leak Detection (WLD) alarms are functioning		☐	☐	☐
10	Inspect ventilation and proper Air Conditioner (AC) operation in UPS rooms		☐	☐	☐
11	Inspect alarms in power systems (UPS, Direct Current (DC) power supply systems) batteries for leakage, charge, terminals, and connections		☐	☐	☐
12	Ensure the health of restricted entry systems (access control, CCTV, Biometric)		☐	☐	☐
13	Ensure identification labels, guarding, covers, and panel are present, secure, and in good condition and free of moisture and dust		☐	☐	☐
	System Readiness				
14	Verify if all work and housekeeping is completed		☐	☐	☐
15	Verify for no active alarms		☐	☐	☐
16	Verify for no logged events posing risks		☐	☐	☐
17	Verify if Building Network communication is enabled		☐	☐	☐
	Pre-Start/Start checks				
18	Check for System fault free/alarm free		☐	☐	☐
19	Check if access restrictions are enabled		☐	☐	☐
20	Check for tooling inspection/Housekeeping		☐	☐	☐
21	Check if HVAC in Control rooms are functioning properly		☐	☐	☐
22	Check for parameters set point		☐	☐	☐
23	Check for previous service reports (3rd party specialist)		☐	☐	☐
	Start Checks				
24	Check for Systems functioning as required		☐	☐	☐
25	Check for no faults in systems		☐	☐	☐
26	Check if power is stable		☐	☐	☐
27	Check for health of HVAC		☐	☐	☐
	Notifications				
28	Department heads (FM)		☐	☐	☐

Attachment 2 – EOM-ZO0-TP-000244 – Shutdown Checklist

Building Name:		Reference No.	REV:00A		
No.	**Shutdown Procedure Checklist**		**CHECKED SATISFACTORY**		
			N/A	**YES**	**NO**
	Communication Systems – Schools & Universities				
	Health and Safety				
1	Availability of required Personal Protective Equipment (PPE)		☐	☐	☐
2	Availability of RAMS		☐	☐	☐
3	Availability of emergency contact details of the responsible person and the contractors		☐	☐	☐
4	Availability of life safety systems (fire extinguishers, sprinklers, gas suppression, and fire alarm)		☐	☐	☐
5	Completion of Job Hazard Analysis		☐	☐	☐
	Pre-approvals				
6	Availability of System owner/Manager/Engineering Team's approvals		☐	☐	☐
7	Clarity of Work orders raised/Scope of task		☐	☐	☐
8	Availability of end-user department head's approvals		☐	☐	☐
9	Availability of QHSE Management's approvals		☐	☐	☐
10	Availability of specialist contractor's schedule of work		☐	☐	☐
11	Availability of approved PTW		☐	☐	☐
	Stand-by Condition System Checks				
12	Check for tooling inspected/Housekeeping		☐	☐	☐
13	Check for Data saved		☐	☐	☐
14	Check for Auto mode/overrides		☐	☐	☐
15	Check for Events/logs saved		☐	☐	☐
	Pre-shutdown Checks (Integrated system functional checks)				
16	Check if Standby systems are working		☐	☐	☐
17	Check if overrides/auto functions are active		☐	☐	☐
	Routine Stop Checks				
18	Check for Lock Out Tag Out (LOTO)		☐	☐	☐
19	Check if back-up server is working		☐	☐	☐
20	Check for no events/alarms on standby systems		☐	☐	☐
	Post-stop Checks				
21	Verify device to be changed out		☐	☐	☐
22	Verify recorded Alarms/warnings		☐	☐	☐
23	Verify system architecture functioning		☐	☐	☐
	Notifications				
24	Department heads (FM)		☐	☐	☐
25	Computer-Aided Facility Management (CAFM) system		☐	☐	☐
26	Reporting		☐	☐	☐
27	End-user/stockholders notification checks		☐	☐	☐
No.	**Reviewer's Comments**	**Resolution**			

Attachment 3 – EOM-ZO0-TP-000245 – Daily Monitoring Checklist

Building Name:	Reference No.	REV:00A

No.	Daily Monitoring Checklist	CHECKED SATISFACTORY		
		N/A	YES	NO
	Communication Systems – Schools & Universities			
	This monitoring checklist is intended to highlight the key issues that may arise day-to-day at the local level. The procedure and any supporting information should be reviewed and amended as necessary to ensure that the document remains up-to-date and definitive for the facility			
1	Systems visual inspection	☐	☐	☐
2	System assessment (Is the unit and its associated secure from unauthorized access)	☐	☐	☐
3	Identification of risks on equipment and raising work orders in case of any discrepancy into communication systems	☐	☐	☐
4	Investigation of fault/alarms for communication systems (Logged events/Active Codes)	☐	☐	☐
5	Duty/standby systems are healthy and communicating	☐	☐	☐
6	Field controllers, routers, and switches are online and communicating	☐	☐	☐
7	Infrastructure facilities services are healthy and functioning	☐	☐	☐
8	Maintenance of daily logs and records of all operation functions	☐	☐	☐
9	Compliance with appliance standards and with occupational health and safety	☐	☐	☐
10	Compliance with service standards, work instructions, and user requirements	☐	☐	☐
11	Set points accurate (unchanged)	☐	☐	☐
12	Voltages/Pressures/Flow in specification as per manufacturer	☐	☐	☐

No.	Reviewer's Comments	Resolution

Originator's Name/Signature and Date:	Checker's Name/Signature and Date:

Attachment 4 – EOM-ZO0-TP-000246 – Emergency Response Action Checklist

Building Name:		Reference No.	REV:00A		
No.	**Emergency Response Action (ERP) Checklist**		**CHECKED SATISFACTORY**		
			N/A	YES	NO
	Communication Systems – Schools & Universities				
	This Emergency Response Action (ERA) Plan is a guide intended for areas of a facility with complex services, for example, a major data center or telecommunication room or specialist plant room services. The actions to be taken by designated and APs may be expressed in a checklist. The steps below are simple indication of some issues that may arise although a more detailed list may be appropriate for each specific area. The designated staff functions of school or university infrastructure need to be made clear in the order that the correct measures are taken to minimize the impact of any crisis				
1	Define ownership of the problem		☐	☐	☐
2	Will evacuation be required		☐	☐	☐
3	Risk of fire outbreak or reduced re-fighting ability		☐	☐	☐
4	Consider impact on electricity supply and power surges on controls		☐	☐	☐
5	Consider impact on water supply and electrical controls		☐	☐	☐
6	Consider impact on drainage electrical controls		☐	☐	☐
7	Consider impact on any third party system and Communication controls		☐	☐	☐
8	Consider impact on site security		☐	☐	☐
9	Consider impact on data loss and data security		☐	☐	☐
10	Consider impact on re-alarms		☐	☐	☐
11	Will critical system be affected and time period of outage		☐	☐	☐
12	Agree responsibility boundaries		☐	☐	☐
13	Control of infection team involvement if BMS data is not available		☐	☐	☐
14	Do public relations need to be addressed		☐	☐	☐
15	Consider SLAs with suppliers		☐	☐	☐
16	Involve commercial services		☐	☐	☐
17	Record entities personnel contact details		☐	☐	☐
No.	**Reviewer's Comments**	**Resolution**			
Originator's Name/Signature and Date:		Checker's Name/Signature and Date:			