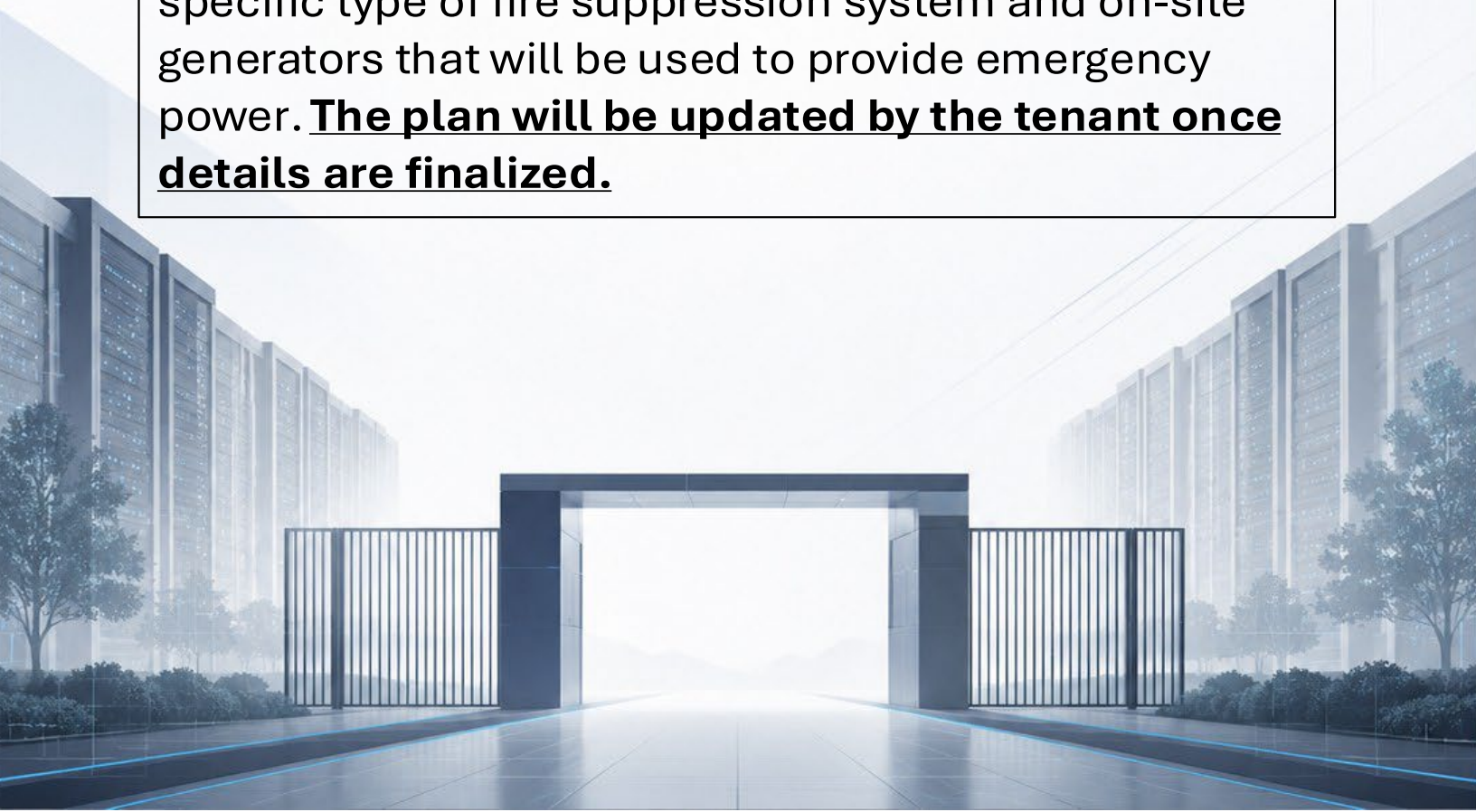
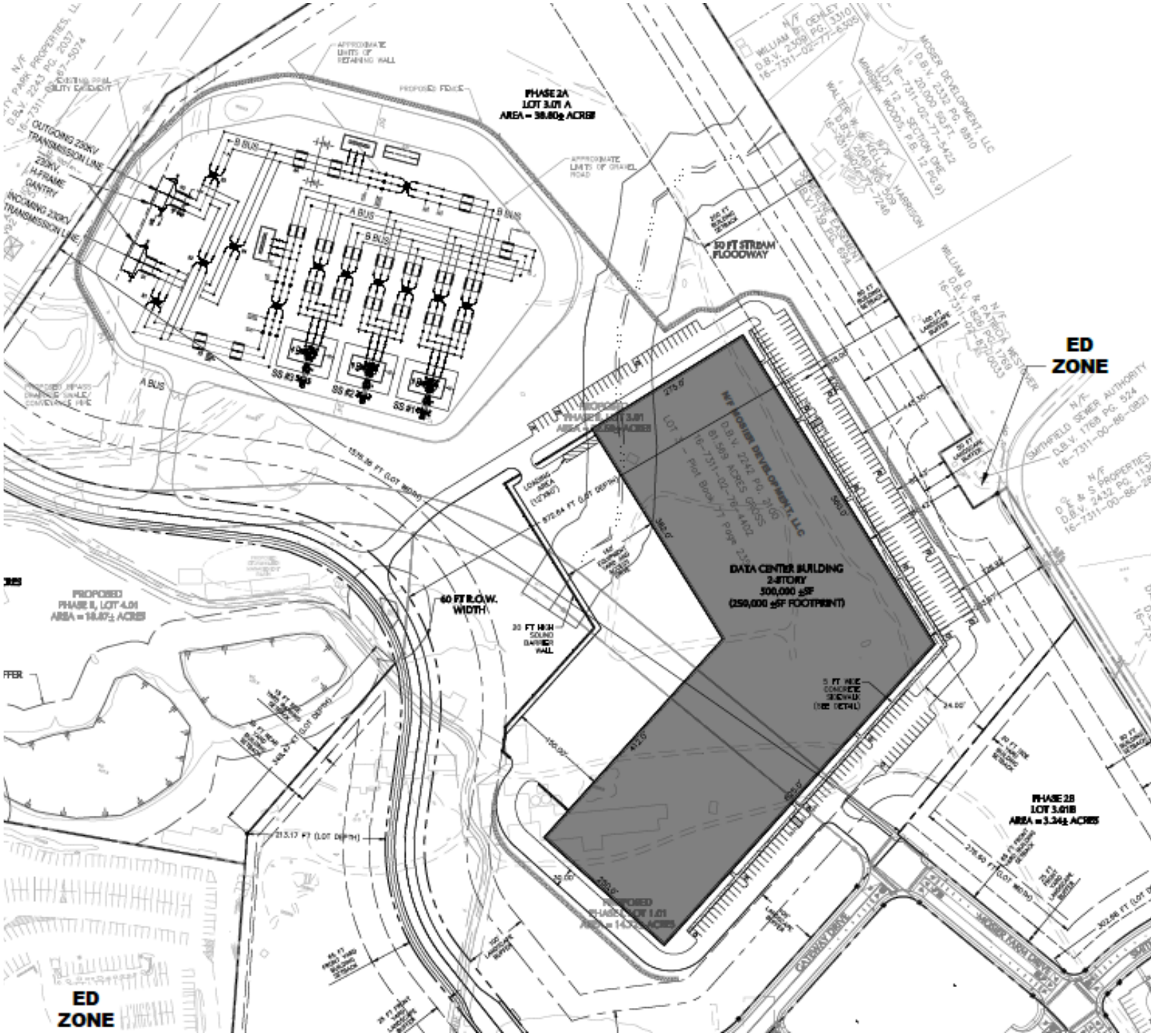
Smithfield Township
Gateway Data Center

Emergency Response Plan

The Smithfield Gateway Data Center Emergency Response Plan was developed for inclusion in the conditional use application. There are facility specific details that will not be known until the application is approved and a tenant is identified. This includes the specific type of fire suppression system and on-site generators that will be used to provide emergency power. **The plan will be updated by the tenant once details are finalized.**




PHASE 2A
LOT 3.01 A
AREA = 38.80± ACRES
50 FT STREAM FLOODWAY
ED ZONE
DATA CENTER BUILDING
2-STORY
500,000 ±SF
(250,000 ±SF FOOTPRINT)
60 FT R.O.W. WIDTH
PROPOSED PHASE II, LOT 4.01
AREA = 16.87± ACRES
PHASE 2B
LOT 3.01B
AREA = 3.34± ACRES
ED ZONE

Smithfield Gateway Data Center

Facility Address: Mosier Farm Dr. and Gateway Dr., Smithfield Township

Facility Developer: DEPG Mosier Associates LP & DEPG of Shawnee II LP

Prepared By: Delta Development Group, Inc.

Tenant Organization: To be determined

Effective Date: Once a tenant organization has been identified and the plan has been updated.

Last Revision Date: August 10, 2026

This Emergency Response Plan is a controlled document. The final version will be maintained by the tenant organization and is subject to formal review, approval, revision, and distribution controls. Printed or locally saved copies are considered uncontrolled unless specifically identified and issued as controlled copies. Users are responsible for confirming that they are using the most current approved version before relying on this plan for emergency preparedness or response activities.

DRAFT

Approval and Authorization

This Emergency Response Plan shall be submitted to the following agencies for review and acceptance as part of the conditional-use and/or land-development application process:

- Marshalls Creek Volunteer Fire Company
- Smithfield Township Emergency Management Coordinator

Comments or recommendations received from reviewing agencies shall be incorporated into the final plan, as appropriate.

Reviewing Agency	Representative	Review Date	Signature
Marshalls Creek Volunteer Fire Company	Jerry Grafal Chief		
Smithfield Township Emergency Management Coordinator	Julia Heilakka Township Manager		

DRAFT

Table of Contents

Smithfield Gateway Data Center 2
Approval and Authorization 3
Part I - Plan Administration 8
Purpose 8
Scope 8
Facility and System Description 9
Facility Information 9
Known or Potential Threats to the Facility 12
Fire 12
Flooding 13
Transportation Corridor Vulnerability. 14
Cyber Threat 14
Utility Failure 15
Emergency Management Framework 16
Mitigation 16
Preparedness 16
Response 16
Recovery 16
Part II - Mitigation 17
Fire Protection and Suppression Design 17
Fire and Smoke Containment Design 18
Ventilation and Smoke-Control Design 18
Battery-Area Ventilation Design 18
Emergency Access Road Evaluation 19
Hydrant and Fire-Water Evaluation 19
Battery Energy-Storage System Safety 19

DRAFT

Applicability 19
Battery-Specific Fire Protection 20
Annual Fire-Safety Inspections 21
Part III - Preparedness 22
Emergency Organization and Responsibilities 22
Emergency Coordinator 22
Facility Personnel 22
Security Personnel 22
Local Fire Department 23
Emergency Notification and Communications 23
Evacuation Planning 23
Evacuation Routes 23
Assembly Areas 24
First-Responder Training 24
Twenty-Four-Hour Emergency Contact Signage 25
Plan Finalization and Implementation 26
Training and Exercises 26
Part IV - Response 27
Fire Reporting and Initial Actions 27
Response to a Fire Alarm 27
Emergency Shutdown Procedures 27
Authority to Initiate an Emergency Shutdown 28
Conditions That May Require Shutdown 28
General Shutdown Priorities 28
Partial and Full Facility Shutdown 29
Electrical System Shutdown 30
UPS and Battery System Shutdown 30

DRAFT

Generator and Fuel-System Shutdown 30
HVAC and Ventilation Shutdown 31
Fire-Protection and Life-Safety Systems 31
Shutdown Status and Documentation 32
System Restoration 32
Utility Interruption and Degraded Operational Response 33
Initial Notification and Assessment 33
Automatic Transfer to UPS and Emergency Generators 34
Generator and Emergency-Power Verification 35
Cooling-System Verification 36
Generator Fuel and Remaining Runtime 37
Loss of Water or Wastewater Service 37
Cyber Incident Response 38
Reporting Suspected Cyber Compromise 39
Initial Cyber Incident Assessment 40
Cyber Incident Lead 40
Facility Emergency Coordinator 41
Critical Operations Personnel 41
Immediate Containment 41
Restricting Vendor and Remote Access 42
Transition to Manual Facility Operations 43
Verification of Life-Safety and Critical Systems 43
Alternate Communications 44
Preservation of Logs and Forensic Evidence 45
Simultaneous Cyber and Physical Emergency 46
External Notifications 46

DRAFT

Manual Fire-Suppression Procedures 47
Electrical Equipment Fire 47
Generator or Fuel-System Fire 48
Battery Emergency Procedures 48
Fire and Smoke Containment Actions 48
Emergency Ventilation and Smoke-Control Actions 49
Battery-Area Ventilation Response 49
Evacuation and Personnel Accountability 49
Evacuation Initiation 49
Occupant Actions 50
Personnel Accountability 50
Part V - Recovery 51
Reentry 51
Restoration and Electrical Resynchronization 51
Cyber System Restoration Authorization 52
Controlled Reconnection and Return to Service 53
Cyber Incident Documentation and Corrective Actions 53
Post-Incident Assessment 54
Restoration of Facility Systems 55
Incident Documentation and Investigation 55
Corrective Actions and Plan Revision 56

DRAFT

Part I - Plan Administration

Purpose

The purpose of this Emergency Response Plan (ERP) is to establish a coordinated framework for protecting on-site personnel, visitors, emergency responders, critical infrastructure, and data center operations during an emergency or disruptive event affecting Smithfield Gateway Data Center.

This plan defines the roles, responsibilities, notification procedures, protective actions, communication protocols, and response priorities necessary to support a safe, timely, and organized response. It also provides guidance for coordinating with public safety agencies, utility providers, contractors, customers, and other external partners, as appropriate.

The plan is intended to reduce risks to life safety, limit damage to equipment and facilities, minimize environmental impacts and operational disruptions, and support the stabilization, recovery, and restoration of critical data center services.

Scope

This ERP applies to Smithfield Gateway Data Center, including all buildings, utility areas, generator and fuel-storage areas, loading areas, exterior grounds, and supporting infrastructure planned for the designated parcel of land at Mosier Farm Dr. and Gateway Dr., Smithfield Township.

The plan applies to all employees, contractors, vendors, tenants, customers, and visitors who may be present at the facility during an emergency. It addresses incidents occurring during normal business hours, after-hours operations, maintenance activities, and periods of reduced staffing.

This plan establishes procedures for responding to emergencies that may affect life safety, facility operations, critical infrastructure, information technology systems, the physical environment, and continuity of services.

The plan addresses:

- Fire suppression actions that may be performed by trained and authorized personnel
- Containment measures intended to limit the spread of fire, smoke, heat, and other hazardous elements
- Ventilation and smoke-control procedures, including the shutdown or adjustment of HVAC systems when appropriate

DRAFT

- Evacuation procedures for employees, contractors, visitors, and other facility occupants

The plan addresses initial notification, incident command, evacuation, personnel accountability, emergency communications, coordination with public safety agencies, stabilization of critical systems, and transition to recovery.

Facility and System Description

Facility Information

General Information	
Facility Name	Smithfield Gateway Data Center
Facility Address	Mosier Farm Dr. and Gateway Dr., Smithfield Township
Property Owner	DEPG Mosier Associates LP & DEPG of Shawnee II LP
Facility Operator	To be determined by tenant organization
Primary Facility Contact	To be determined by tenant organization
Twenty-Four-Hour Telephone	To be determined by tenant organization
Normal Operating Hours	24/7
Maximum Anticipated Occupancy	Estimated 60 Employees based off current plans

Structure Information	
Building Footprint	± 250,000 square feet
Building size	± 500,000 square feet
Number of stories	2
Construction type	[Construction Type] – to be built upon approval
Fire-resistance ratings	[Description] – to be built upon approval

DRAFT

Number of data halls	To be determined by tenant organization
Number of electrical rooms	To be determined by tenant organization
Number of battery rooms or enclosures	To be determined by tenant organization
Number and type of generators	To be determined by tenant organization
Fuel type and storage capacity	To be determined by tenant organization
Primary cooling system	To be determined by tenant organization

Critical Electrical Systems	
Utility electrical service	To be determined by tenant organization
Transformers	To be determined by tenant organization
Switchgear	To be determined by tenant organization
Uninterruptible power supplies	To be determined by tenant organization
Battery systems	To be determined by tenant organization
Emergency generators	To be determined by tenant organization
Automatic transfer switches	To be determined by tenant organization
Electrical disconnects	To be determined by tenant organization
Emergency shutdown controls	To be determined by tenant organization

DRAFT

Fire Protection Systems	
Automatic fire alarm system	To be determined by tenant organization
Smoke and heat detection	To be determined by tenant organization
Very Early Smoke Detection Apparatus (VESDA), if installed	To be determined by tenant organization
Automatic sprinkler systems	To be determined by tenant organization
Pre-action sprinkler systems	To be determined by tenant organization
Clean-agent suppression systems	To be determined by tenant organization
Portable fire extinguishers	To be determined by tenant organization
Fire department connections	To be determined by tenant organization
Fire pumps	To be determined by tenant organization
Hydrants	To be determined by tenant organization
Fire-rated walls and doors	To be determined by tenant organization
Smoke-control or exhaust systems	To be determined by tenant organization

DRAFT

Known or Potential Threats to the Facility

Fire

Fire represents a significant potential threat due to the concentration of electrical equipment, energized conductors, cabling, power-distribution equipment, emergency generators, fuel systems, and heat-producing equipment anticipated at the facility. Potential fire scenarios may include:

- Electrical faults, arcing, overheating, or equipment failure within data halls, switchgear rooms, transformer areas, and utility spaces
- Generator, fuel-storage, or fuel-transfer system fires
- Cable, rooftop equipment, HVAC, or cooling-system fires
- Fires resulting from maintenance, hot work, construction, or contractor activities
- Battery overheating or thermal runaway where lithium-ion or other energy-storage systems are installed
- A brush or wildfire originating on or near the property and spreading toward facility structures, utility equipment, or access roads

A significant fire could produce smoke, heat, hazardous gases, equipment damage, loss of electrical distribution, cooling-system interruption, or cascading failures in other building systems. A fire affecting switchgear, transformers, generators, batteries, or fuel systems could require isolation of multiple systems and implementation of an emergency shutdown. Smoke or combustion products could also require evacuation of the affected building/immediate area or the entire facility.

The data center will be between Marshalls Creek Volunteer Fire Company, Shawnee Fire Company, Delaware Water Gap Fire Department, and Acme Hose Co. No 1. Coordination with these departments will be necessary to confirm apparatus access, water supply, fire department connections, equipment hazards, shutdown locations, and responder staging areas. A full access plan will be developed, including specific routes and fire hydrant locations once site plans are approved.

Specific details are not yet available for the specific automatic detection and suppression, compartmentation, hydrant and fire-flow requirements, battery hazards, fuel-system protection, vegetation management, and emergency shutdown systems. Proposed actions are provided in the Fire Suppression and Containment Procedures, Emergency Shutdown Procedures, and Evacuation Procedures sections of this ERP based on industry best practices.

DRAFT

Flooding

Based on current site plans and available floodplain mapping, the proposed facility site is not located within the mapped 1-percent annual-chance (100-year) or 0.2-percent annual-chance (500-year) floodplain. Accordingly, direct riverine flooding is not considered a primary threat to the facility.

Residual flood-related risk remains from localized heavy rainfall, flash flooding, stormwater accumulation, drainage-system failure, blocked culverts, erosion, and runoff from surrounding properties or impervious surfaces. The Monroe County Hazard Mitigation Plan notes that flash flooding may occur outside traditionally identified flood-prone locations and that increased impervious cover can reduce infiltration and increase runoff.

Potential impacts may include:

- Temporary ponding near buildings, loading areas, generators, transformers, or access roads
- Overloading or blockage of stormwater-management infrastructure
- Erosion or slope instability around drainage channels, utility corridors, or retaining features
- Water intrusion through doors, utility penetrations, roof drains, or other low openings
- Restricted access for employees, emergency responders, fuel suppliers, or utility crews because of flooding on nearby roads
- Disruption of off-site electric, telecommunications, water, or transportation infrastructure located within flood-prone areas

The data center developer will verify finished-floor elevations, site grading, drainage pathways, stormwater-system capacity, equipment elevations, and protection of utility penetrations. Emergency generators, fuel systems, electrical equipment, and other critical infrastructure should be positioned or protected so localized stormwater accumulation does not impair facility operations. Primary and alternate access routes should also be evaluated for potential roadway flooding, even though the facility itself remains outside mapped flood-hazard areas.

Facility personnel will monitor severe-weather and flash-flood warnings and inspect drainage systems before and after significant rainfall. If water accumulation threatens electrical equipment, fuel systems, access routes, or occupied portions of the facility, personnel shall restrict access to affected areas, notify the Facility Emergency Coordinator, and initiate protective shutdown or evacuation procedures as conditions warrant.

DRAFT

Transportation Corridor Vulnerability.

The proposed Smithfield Gateway facility is located near the intersection of U.S. Route 209 and Pennsylvania Route 447 and approximately one-half mile from Interstate 80. The Township identifies the project as being located behind the existing St. Luke's and Wawa developments.

These transportation corridors provide important access for employees, emergency responders, contractors, utility crews, equipment deliveries, and generator-fuel deliveries. They also create exposure to:

- Vehicle crashes and roadway fires
- Hazardous-material transportation incidents
- Major highway closures, detours, or extended traffic congestion
- Severe-weather-related road closures
- Damage to roadside electrical, telecommunications, or utility infrastructure
- Construction activities or incidents that restrict access to the facility
- Chemical or smoke plumes requiring shelter-in-place or evacuation

A major incident on Route 209, Route 447, or Interstate 80 could delay emergency response, interrupt fuel deliveries, limit employee access, or prevent utility personnel from reaching the facility. A hazardous-material release could require the facility to shut down outdoor air intake, shelter personnel indoors, evacuate selected areas, or coordinate protective actions with Monroe County emergency management and responding fire departments.

The facility should identify primary and alternate response routes, designate emergency staging areas, maintain contact procedures for roadway closure information, and coordinate access planning with Township officials and local first responders. Where feasible, emergency access should not depend on a single roadway, intersection, or transportation corridor.

Cyber Threat

The facility may be exposed to ransomware, malware, denial-of-service attacks, credential compromise, unauthorized remote access, insider threats, vendor-access compromise, or manipulation of network-connected operational systems. Systems potentially affected may include:

- Building management and environmental controls
- Electrical power monitoring and control systems
- Cooling-system controls

DRAFT

- Physical access control and security cameras
- Fire detection, alarm monitoring, and notification interfaces
- Telecommunications and emergency notification systems
- Equipment monitoring, maintenance, and remote-support platforms

A cyber incident could cause loss of system visibility, unauthorized changes to operating parameters, interruption of cooling or electrical controls, loss of access-control functionality, or delayed recognition of a developing fire or equipment failure. Cyber incidents may also occur simultaneously with a physical emergency or utility outage, complicating emergency decision-making.

The facility should maintain network segmentation between information-technology and operational-technology systems, multifactor authentication, controlled vendor access, offline backups, manual operating capabilities, redundant communications, incident logging, and procedures for isolating compromised systems. Emergency procedures will identify which safety systems can be operated manually when network monitoring or automated controls are unavailable.

Utility Failure

The facility will depend on external electric power, telecommunications, data connectivity, water, wastewater, and fuel-delivery systems. Minor utility interruptions occur regularly within Monroe County and are often associated with storms, wind, winter weather, damaged lines, transportation incidents, or equipment failures. A severe thunderstorm affecting Smithfield Township in July 2026 caused extended electrical outages and resulted in the opening of an emergency shelter for residents remaining without power.

Potential utility-failure scenarios include:

- Loss of normal electrical service
- Failure of one or more telecommunications or fiber providers
- Loss of water needed for domestic use, cooling, or fire protection
- Natural-gas or fuel-supply interruption
- Generator failure, insufficient fuel, or inability to obtain refueling
- Simultaneous loss of utility power and communications
- Failure of cooling or heat-rejection systems during an electrical outage
- Failure of multiple redundant systems because of a common upstream dependency

Backup generators, uninterruptible power supplies, and redundant utility connections can reduce the likelihood of an immediate shutdown but do not eliminate the possibility of a

DRAFT

prolonged or common-mode failure. An extended outage could eventually exceed battery capacity, onsite fuel reserves, cooling capacity, or equipment operating limitations.

Emergency Management Framework

This ERP uses the four phases of emergency management; mitigation, preparedness, response, and recovery, to organize the processes that will protect facility occupants, emergency responders, neighboring properties, and the surrounding community.

Mitigation

Mitigation includes the design and construction measures intended to prevent emergencies or reduce their consequences. These measures include fire-detection and suppression systems, fire-rated construction, smoke containment, emergency ventilation, battery-specific protection, emergency access roads, hydrants, and fire-water systems.

Preparedness

Preparedness includes the actions completed before facility operation to ensure that personnel and emergency responders are ready to manage an emergency. These actions include assigning responsibilities, establishing notification procedures, planning evacuation routes, coordinating with public safety agencies, providing first-responder training, conducting fire-safety inspections, and maintaining emergency contact signage.

Response

Response includes the immediate actions taken when a fire, smoke condition, battery emergency, fuel-system incident, or other life-safety emergency occurs. Response actions include emergency notification, fire suppression, containment, ventilation control, evacuation, personnel accountability, emergency shutdown, responder access, and incident command coordination.

Recovery

Recovery includes the actions taken after the immediate emergency has been controlled. These actions include reentry authorization, damage and safety assessments, restoration of affected systems, incident investigation, documentation of corrective actions, and revision of this plan as necessary.

DRAFT

Part II - Mitigation

Fire Protection and Suppression Design

The facility will include automatic fire-suppression systems appropriate to the hazards in each protected area. Suppression systems shall be designed and installed in accordance with applicable fire, building, electrical, and mechanical codes and the requirements of Smithfield Township.

The design shall provide protection for:

- Data halls
- Electrical and switchgear rooms
- Uninterruptible Power Supply system (UPS) and battery areas
- Generator rooms or enclosures
- Fuel-related equipment areas
- Mechanical rooms
- Offices and occupied support spaces

The selected systems shall be identified in the final design documents:

Protected Area	Suppression System
Data halls	To be determined by tenant organization
Electrical rooms	To be determined by tenant organization
UPS areas	To be determined by tenant organization
Battery areas	To be determined by tenant organization
Generator areas	To be determined by tenant organization
Offices and support areas	To be determined by tenant organization

DRAFT

Fire and Smoke Containment Design

The facility design shall use fire-rated construction and compartmentation to limit the movement of fire, smoke, heat, and hazardous gases.

Containment measures shall include, as applicable:

- Fire-rated walls and partitions
- Fire-rated doors with automatic closing devices
- Fire-stopping around cable, pipe, and conduit penetrations
- Fire and smoke dampers
- Separation of data halls, electrical rooms, battery areas, generator areas, and fuel systems
- Spill containment for fuels and liquid electrolytes
- Separation distances required by applicable codes and standards

Ventilation and Smoke-Control Design

The mechanical design will prevent smoke and hazardous gases from being distributed to unaffected occupied areas.

The final HVAC and smoke-control design shall incorporate the following automatic functions, as applicable:

- Shutdown of air-handling equipment serving the affected area
- Closure of fire and smoke dampers
- Isolation of the affected ventilation zone
- Shutdown of recirculated air
- Activation of dedicated smoke exhaust
- Continued ventilation of designated safe areas
- Prevention of smoke migration through cable or utility spaces

Battery-Area Ventilation Design

Battery areas will include ventilation and gas-detection systems suitable for the selected battery technology.

DRAFT

Emergency Access Road Evaluation

Access Element	Design
Primary access-road width	[Width]
Secondary emergency access	[Location or Not Applicable]
Fire-lane width	[Width]
Road load capacity	[Capacity]
Minimum turning radius	[Radius]
Gate clear width	[Width]
Gate emergency override	[Method]
Minimum vertical clearance	[Height]
Apparatus staging location	[Location]
Building perimeter access	[Description]

Hydrant and Fire-Water Evaluation

Fire-Water Element	Design
Number of on-site hydrants	[Number]
Water-main size	[Size]
Required fire flow	[Flow]
Available fire flow	[Flow]
Static pressure	[Pressure]
Residual pressure	[Pressure]
Fire-pump capacity	[Capacity or Not Applicable]
Maximum hydrant spacing	[Distance]
Fire department connection locations	[Locations]

Battery Energy-Storage System Safety

Applicability

The facility will include a battery storage system identified by the by tenant organization.

DRAFT

The battery storage system shall comply with NFPA 855, applicable codes, manufacturer requirements, and requirements established by the authority having jurisdiction.

The following information shall be completed when the battery system is selected:

Battery Element	Design
Battery chemistry	To be determined by tenant organization
Manufacturer	To be determined by tenant organization
Model	To be determined by tenant organization
Total energy capacity	To be determined by tenant organization
Battery location	To be determined by tenant organization
Cabinet or enclosure type	To be determined by tenant organization
Listing or certification	To be determined by tenant organization
Suppression system	To be determined by tenant organization
Gas-detection system	To be determined by tenant organization
Ventilation system	To be determined by tenant organization
Emergency shutdown method	To be determined by tenant organization

Battery-Specific Fire Protection

Battery areas will be protected by a suppression system designed specifically for the selected battery chemistry and configuration.

The final battery safety design addresses:

- Fire detection
- Heat detection
- Gas detection
- Thermal-runaway monitoring
- Automatic suppression
- Fire-rated separation
- Ventilation and gas exhaust
- Electrical isolation
- Emergency shutdown
- Spill containment, where applicable
- Deflagration protection, where required
- Re-ignition monitoring

DRAFT

- Emergency responder access

Annual Fire-Safety Inspections

Beginning within one year of facility occupancy, a qualified professional shall conduct an annual fire-safety inspection on behalf of the tenant organization.

The inspection shall include:

- Fire alarm and detection systems
- Automatic fire-suppression systems
- Battery-specific suppression systems
- Portable fire extinguishers
- Hydrants and fire department connections
- Fire pumps, where installed
- Fire-rated doors and barriers
- Visible or hidden penetrations
- Fire and smoke dampers
- Emergency exits and evacuation routes
- Emergency lighting and exit signs
- Emergency access roads and fire lanes
- Gates and emergency entry systems
- Battery monitoring, gas detection, and ventilation
- Generator and fuel-system safety features
- Emergency shutdown controls
- Twenty-four-hour emergency contact signage

The qualified professional shall prepare a written report documenting:

- Systems inspected
- Applicable standards
- Inspection findings
- Hazardous penetrations
- Identified deficiencies
- Required corrective actions
- Responsible parties
- Completion dates

The facility operator shall maintain inspection reports and corrective-action records and shall provide them to Smithfield Township upon request.

DRAFT

Part III - Preparedness

Emergency Organization and Responsibilities

Emergency Coordinator

The Emergency Coordinator is responsible for coordinating facility actions until command is transferred to the appropriate responding agency such as the Marshalls Creek Volunteer Fire Company or other public safety agency, when applicable.

Name: To be determined by tenant organization

Title: Emergency Coordinator

Primary Telephone: To be determined by tenant organization

Alternate Telephone: To be determined by tenant organization

Facility Personnel

Facility personnel shall:

- Immediately report fire, smoke, overheating, unusual odors, alarms, or visible equipment damage
- Activate the fire alarm when appropriate
- Call 9-1-1
- Follow established equipment shutdown procedures when safe to do so
- Follow evacuation instructions
- Report to the designated assembly area
- Avoid entering areas containing fire, smoke, electrical hazards, or hazardous gases
- Provide technical information to emergency responders when requested

Security Personnel

Security personnel shall:

- Notify 9-1-1 and designated facility representatives
- Open gates and controlled-access points
- Direct responders to the appropriate building or incident location
- Provide keys, access cards, site plans, and emergency contact information
- Keep fire lanes and emergency access routes clear
- Restrict unauthorized entry into the affected area

DRAFT

Local Fire Department

Upon arrival, the responding fire department shall assume command of fire-suppression and life-safety operations.

Facility personnel shall support responders by providing:

- Site plans
- Electrical one-line diagrams
- Battery-system information
- Safety Data Sheets
- Utility disconnect locations
- Fire-suppression system information
- Ventilation controls
- Access credentials
- Facility technical representatives

Emergency Notification and Communications

The facility operator will maintain emergency notification procedures and a current twenty-four-hour contact list. The fire alarm, monitoring, and communications systems shall be configured to notify designated personnel and emergency services in accordance with the approved facility design.

The following parties will be notified as conditions warrant:

- Marshalls Creek Volunteer Fire Company
- Emergency Medical Services to be determined by tenant organization
- Smithfield Township Emergency Management Coordinator
- Local Power Company to be determined by tenant organization
- Environmental Agency to be determined by tenant organization
- Fire Protection Contractor to be determined by tenant organization
- Battery System Manufacturer or Contractor to be determined by tenant organization
- Insurance Carrier to be determined by tenant organization
- Other Appropriate Contact to be determined by tenant organization

Evacuation Planning

Evacuation Routes

The facility design will include code-compliant primary and alternate evacuation routes from all occupied areas.

DRAFT

Evacuation maps shall identify:

- Primary exits
- Alternate exits
- Travel paths
- Fire alarm pull stations
- Portable fire extinguishers
- Areas of refuge, where applicable
- Primary and alternate assembly areas

The final evacuation maps shall be inserted into Appendix A before facility occupancy.

Assembly Areas

The proposed assembly areas are:

- Primary Assembly Area: To be determined by tenant organization
- Alternate Assembly Area: To be determined by tenant organization

Assembly areas will be positioned:

- Away from buildings and exterior equipment
- Outside emergency vehicle access routes
- Away from fuel, transformer, generator, and battery hazards
- Outside likely smoke or hazardous-gas pathways
- In locations that allow personnel accountability

First-Responder Training

Before the facility begins operation, the tenant organization shall coordinate facility-specific training with:

- Marshalls Creek Volunteer Fire Company
- Emergency Medical Services to be determined by tenant organization
- Smithfield Township Emergency Management Coordinator
- Pennsylvania State Police
- Hazardous Materials Team, if applicable to be determined by tenant organization

Training shall address:

- Site access and gate operation
- Fire apparatus routes and staging
- Hydrant and fire department connection locations

DRAFT

- Building and data hall layout
- Electrical hazards and stored energy
- Electrical disconnects
- Generator and fuel systems
- Battery chemistry and capacity
- Battery thermal-runaway and off-gassing hazards
- Fire-suppression systems
- Gas detection and ventilation
- Emergency shutdown controls
- Restricted areas
- Facility emergency contacts

Training shall include a site walk-through after construction and before occupancy. Refresher training shall be provided when major systems are modified or when requested by local response agencies.

Training records shall document the date, participating agencies, attendees, topics covered, instructor, and identified corrective actions.

Twenty-Four-Hour Emergency Contact Signage

Twenty-four-hour emergency contact signage shall be installed conspicuously at each facility access entrance before the facility begins operation.

The sign shall include:

- Facility Company Name: To be determined by tenant organization
- Owner or Representative: To be determined by tenant organization
- Twenty-Four-Hour Telephone Number: To be determined by tenant organization
- Local Power Company: Power Company to be determined by tenant organization
- Power Company Telephone Number: To be determined by tenant organization

The signage shall be:

- Visible from the facility entrance
- Constructed of durable, weather-resistant materials
- Reflective or illuminated where required
- Maintained in a legible condition
- Updated whenever emergency contact information changes
- Included in the annual fire-safety inspection

DRAFT

Plan Finalization and Implementation

Because the data center has not yet been constructed, this ERP is based on the proposed facility design and establishes requirements that shall be incorporated into final construction and operating documents.

Before facility occupancy, the tenant organization shall:

1. Update the ERP using final equipment and system information.
2. Insert final site, floor, fire-protection, ventilation, and evacuation drawings.
3. Confirm battery chemistry, capacity, and NFPA 855 compliance.
4. Complete the access-road and hydrant evaluations.
5. Obtain fire department and emergency management review.
6. Complete facility-specific first-responder training.
7. Install the required emergency contact signage.
8. Confirm that emergency systems have been tested and commissioned.
9. Provide the completed ERP to the facility operator and reviewing agencies.

The ERP shall be reviewed whenever there is a material change to the facility design, fire-protection systems, battery systems, access roads, hydrants, or emergency procedures.

Training and Exercises

The data center tenant, once identified, will conduct at a minimum, one emergency response drill annually, addressing a known or potential threat. In addition, fire drills will be conducted quarterly, rotating between the three (3) proposed shifts, to ensure participation from all employees over the course of a year.

All staff will be provided training on facility evacuation, safety protocols, emergency system shutdowns relevant to their role and position, fire safety, and emergency communications.

DRAFT

Part IV - Response

Fire Reporting and Initial Actions

Any person discovering fire, smoke, overheating equipment, battery off-gassing, or another potentially hazardous condition shall:

1. Activate the nearest fire alarm, when appropriate.
2. Call 9-1-1.
3. Provide the facility name and address.
4. Describe the location and nature of the emergency.
5. Report known electrical, fuel, or battery hazards.
6. Notify the Emergency Coordinator.
7. Evacuate or follow other protective-action instructions.

Response to a Fire Alarm

Upon activation of a fire alarm:

1. Occupants shall immediately begin evacuation.
2. The monitored alarm system shall make appropriate notifications to the local fire department.
3. The fire department shall be notified automatically or by telephone.
4. Access gates shall be opened or made accessible to emergency responders.
5. Designated facility personnel shall meet responders at the approved entry point.
6. Facility personnel shall provide site plans, equipment information, utility shutoff locations, master keys where appropriate, and battery or fuel hazard information.
7. Access to the affected area shall be restricted.
8. Equipment shutdowns shall only be performed when they can be completed remotely or without exposing personnel to fire, smoke, electrical hazards, or hazardous gases.

Emergency Shutdown Procedures

Emergency shutdown procedures are intended to place affected facility systems and equipment in a safe condition during a fire or other emergency. Shutdown actions shall be performed only when they can be completed without delaying emergency notification or evacuation and without exposing personnel to fire, smoke, electrical hazards, hazardous gases, or other unsafe conditions.

Life safety shall always take priority over equipment protection, continuity of operations, and emergency shutdown activities.

DRAFT

Because the facility has not yet been constructed, the system-specific shutdown sequences shall be finalized after the equipment, controls, and fire-protection systems have been selected, installed, tested, and commissioned.

Authority to Initiate an Emergency Shutdown

Emergency shutdown actions may be initiated by:

- Automatic control or protection systems incorporated into the facility design
- Authorized Facility Position to be determined by tenant organization
- Emergency Coordinator
- Qualified Electrical or Critical Operations Personnel to be determined by tenant organization
- The fire department Incident Commander
- Other Authorized Position or Agency to be determined by tenant organization

Only trained and authorized personnel may operate electrical disconnects, emergency power-off controls, generator shutdowns, battery isolation controls, fuel shutoffs, or mechanical-system overrides.

General employees shall not attempt to shut down facility systems unless specifically trained, authorized, and directed to do so.

Conditions That May Require Shutdown

A partial or complete emergency shutdown may be required when:

- Fire, smoke, or excessive heat threatens electrical or mechanical equipment
- An electrical fault, arc-flash condition, or equipment failure creates an immediate hazard
- Battery overheating, off-gassing, smoke, or thermal runaway is detected
- A generator, fuel-storage, or fuel-transfer system is involved in an emergency
- A fuel, coolant, refrigerant, or other hazardous-material release occurs
- Continued equipment operation could contribute to fire spread, smoke movement, or hazardous-gas generation
- The fire department Incident Commander directs that equipment or systems be shut down
- Automatic protective systems initiate a shutdown
- Other Facility-Specific Shutdown Condition to be determined by tenant organization

General Shutdown Priorities

When emergency shutdown is necessary, actions shall be prioritized as follows:

DRAFT

1. Notify 9-1-1 and activate the appropriate facility alarm.
2. Initiate evacuation or other required protective actions.
3. Notify Emergency Coordinator.
4. Identify the affected equipment, room, or operating zone.
5. Determine whether shutdown can be completed remotely.
6. Isolate only the equipment or systems necessary to control the hazard.
7. Avoid shutting down fire alarms, fire pumps, suppression systems, emergency lighting, smoke-control systems, access controls, or other life-safety systems unless directed by the fire department or required by the approved emergency sequence.
8. Confirm the shutdown status when it can be done safely.
9. Report completed and unsuccessful shutdown actions to the fire department Incident Commander.
10. Maintain the affected system out of service until reactivation is authorized.

Personnel shall immediately stop shutdown activities and evacuate when conditions become unsafe or when directed by emergency responders.

Partial and Full Facility Shutdown

Whenever practicable, the emergency response shall use a localized or partial shutdown to isolate the affected area while maintaining unaffected life-safety and critical systems.

A full facility shutdown shall only be initiated when:

- The incident cannot be safely controlled through localized isolation
- Continued operation creates an unacceptable risk to occupants, responders, or the public
- Required by the approved automatic sequence of operations
- Directed by the fire department Incident Commander
- Authorized by the tenant organization

The decision to conduct a full shutdown shall consider potential impacts on:

- Fire alarms and detection systems
- Automatic suppression systems
- Fire pumps
- Emergency lighting
- Exit and evacuation systems
- Smoke-control and ventilation systems
- Security and responder access

DRAFT

- Battery monitoring and gas detection
- Communications systems
- Other systems required to support emergency operations

Electrical System Shutdown

Electrical shutdown shall only be performed by trained and authorized personnel.

Procedures shall include:

- Identification of the affected electrical equipment or distribution zone
- Use of remote shutdown controls where available
- Isolation of affected switchgear, transformers, electrical rooms, or data halls
- Operation of emergency power-off controls, if provided and appropriate
- Coordination with Local Power Company to be determined by tenant organization
- Notification of the fire department regarding energized equipment
- Confirmation that life-safety systems remain operational or are supported by an alternate source
- Lockout/tagout or other energy-control measures following emergency stabilization

The final electrical shutdown sequence shall be based on the approved electrical one-line diagrams and manufacturer instructions.

UPS and Battery System Shutdown

During an emergency involving a UPS or battery system:

- Personnel shall not enter an area containing smoke, excessive heat, off-gassing, or suspected thermal runaway
- The affected UPS or battery system shall be isolated remotely when an approved remote shutdown capability is available
- Battery disconnects shall only be conducted by trained and authorized personnel
- Responders shall be informed that stored electrical energy may remain after the upstream power supply has been disconnected
- Battery monitoring, gas detection, suppression, and ventilation systems shall remain operational unless directed otherwise by the fire department
- The affected equipment shall remain out of service until evaluated by Battery Manufacturer, Qualified Engineer, or Authorized Service Provider to be determined by tenant organization

Generator and Fuel-System Shutdown

During an emergency involving a generator or fuel system:

DRAFT

- Fuel-transfer operations shall stop
- The affected generator shall be shut down using the approved emergency stop when it can be operated safely or remotely
- Fuel-supply valves shall be closed when authorized and safe
- Ignition sources shall be controlled where practicable
- Generator and fuel-system locations shall be communicated to responders
- The fire department shall be informed of the fuel type, storage capacity, containment measures, and emergency shutoff locations

Shutdown of unaffected emergency generators shall not occur unless continued operation presents a hazard or the shutdown is directed by the fire department Incident Commander.

HVAC and Ventilation Shutdown

HVAC and ventilation systems shall operate according to the approved fire alarm and smoke-control sequence. Emergency actions may include:

- Shutting down air-handling equipment serving the affected area
- Closing fire and smoke dampers
- Isolating the affected ventilation zone
- Stopping recirculated air
- Activating dedicated smoke or hazardous-gas exhaust
- Maintaining ventilation for designated safe areas
- Preventing smoke or gas migration to unaffected areas

Manual operation or override shall be limited to the fire department Incident Commander and Authorized Facility Position to be determined by tenant organization

Battery-room ventilation shall not be shut down during an off-gassing or thermal-runaway event unless directed by the fire department or required by the approved system design.

Fire-Protection and Life-Safety Systems

Fire alarms, suppression systems, fire pumps, smoke-control systems, emergency lighting, and other life-safety systems shall not be manually disabled during an emergency unless:

- Continued operation creates an immediate hazard
- Shutdown is required by the approved sequence of operations
- Directed by the fire department Incident Commander
- Performed by trained and authorized personnel

DRAFT

Any life-safety system taken out of service shall be reported immediately to the fire department Incident Commander and Emergency Coordinator.

Shutdown Status and Documentation

The following information shall be communicated to the fire department Incident Commander:

- Systems successfully shut down
- Systems that remain energized or operating
- Systems that could not be accessed or isolated
- Locations of disconnects and emergency controls
- Known stored-energy hazards
- Impacts on fire protection, ventilation, communications, or security
- Personnel performing shutdown activities

Following the incident, the tenant organization shall document:

- The reason for the shutdown
- The person authorizing the shutdown
- Systems and equipment affected
- Shutdown actions completed
- Automatic systems activated
- Problems or unsafe conditions encountered
- Notifications made
- Time of shutdown
- Time and authorization for restoration

System Restoration

No system that has been shut down during an emergency shall be returned to service until:

1. The immediate hazard has been controlled.
2. The affected equipment has been inspected by qualified personnel.
3. Required repairs have been completed.
4. Fire-protection and monitoring systems are operational.
5. Testing confirms that the system can operate safely.
6. The fire department or other reviewing authority has provided approval when required.
7. Restoration is authorized by Authorized Facility Position to be determined by tenant organization.

DRAFT

Utility Interruption and Degraded Operational Response

Utility-interruption procedures are intended to maintain life-safety systems, stabilize critical facility operations, protect equipment, and support an orderly transition to emergency power, degraded operations, partial shutdown, or full shutdown.

A utility interruption may involve:

- Loss or instability of normal electrical service
- Loss of one or more electrical feeds
- Failure of an automatic transfer switch, UPS, battery system, generator, switchgear component, or electrical distribution path
- Loss of water required for cooling, domestic service, or fire protection
- Failure of a cooling or heat-rejection system
- Loss of telecommunications, internet, fiber, or data connectivity
- Loss of wastewater service
- Interruption of natural gas, generator fuel, or fuel-delivery services
- Simultaneous failure of multiple utilities or redundant systems
- Failure of systems that share a common upstream dependency

Life safety shall take priority over continuity of operations, customer service, and equipment protection.

Only trained and authorized personnel may operate generators, transfer switches, UPS systems, electrical disconnects, fuel systems, cooling-system controls, or load-management systems.

Initial Notification and Assessment

Upon indication of a utility interruption or significant degradation, facility personnel shall:

1. Notify Emergency Coordinator.
2. Confirm the affected utility, system, building, room, or operating zone.
3. Determine whether the interruption is complete, intermittent, unstable, or limited to one distribution path.
4. Identify alarms, equipment failures, abnormal temperatures, water-pressure changes, communication failures, or other secondary conditions.
5. Confirm whether life-safety systems remain operational.
6. Determine whether the condition resulted from an internal equipment failure, an external utility interruption, severe weather, a transportation incident, a cyber incident, or an unknown cause.
7. Contact the affected utility provider or service contractor and request:

DRAFT

- Confirmation of the outage
- Known cause
- Estimated restoration time
- Expected system instability or repeated interruptions
- Utility-specific safety instructions

8. Establish an incident log documenting:
   - Time the interruption began
   - Systems affected
   - Alarms received
   - Transfer operations
   - Notifications made
   - Equipment status
   - Fuel status
   - Protective actions taken

When an interruption threatens fire protection, cooling, electrical safety, fuel systems, occupied areas, or emergency communications, the Emergency Coordinator shall determine whether emergency services must be notified.

Automatic Transfer to UPS and Emergency Generators

Upon loss or unacceptable degradation of normal electrical service, the facility's approved sequence of operations shall initiate transfer to UPS systems, battery systems, emergency generators, or other alternate electrical sources.

Facility personnel shall not interrupt or manually override an automatic transfer unless:

- The automatic sequence fails
- The transfer creates an unsafe condition
- Manual operation is required by the approved electrical sequence
- Directed by Authorized Facility Position to be determined by tenant organization
- Directed by the fire department Incident Commander during a life-safety emergency

Immediately following transfer, authorized personnel shall verify:

1. UPS systems accepted the designated critical load.
2. Battery discharge began as designed.
3. Emergency generators received a start signal.
4. Each required generator started and reached acceptable operating speed, voltage, and frequency.
5. Automatic transfer switches transferred to the intended emergency source.

DRAFT

6. Electrical distribution paths are energized as designed.
7. No unexpected overload, fault, arc-flash indication, abnormal vibration, smoke, odor, or fuel leakage is present.
8. Required fire-protection and life-safety systems remain energized.
9. Cooling, ventilation, security, monitoring, and communication systems remain operational.
10. Redundant systems are available or any loss of redundancy has been identified.

The final transfer-verification checklist shall be based on the approved electrical one-line diagrams, generator controls, UPS configuration, automatic transfer-switch design, and manufacturer requirements.

Generator and Emergency-Power Verification

During emergency-generator operation, authorized personnel shall monitor:

- Generator load
- Voltage and frequency
- Engine temperature
- Oil pressure
- Coolant temperature and level
- Fuel pressure and fuel level, including fuel levels in storage
- Runtime remaining
- Battery-charging status
- Exhaust condition
- Generator-room or enclosure ventilation
- Fuel-transfer system status
- Alarms and fault indicators
- Operating hours
- Condition of associated switchgear and transfer switches

Abnormal conditions shall be reported immediately to Emergency Coordinator and Generator Service Contractor to be determined by tenant organization.

A generator shall be removed from service when continued operation presents an immediate fire, electrical, mechanical, fuel-release, or life-safety hazard. Removal of a generator from service shall be coordinated with the affected load, remaining generators, UPS capacity, cooling requirements, and facility shutdown priorities.

DRAFT

Cooling-System Verification

After any electrical transfer or utility interruption, facility personnel shall verify that required cooling and heat-rejection systems started or remained operational.

Verification shall include, as applicable:

- Chillers
- Cooling towers
- Pumps
- Computer-room air handlers
- Computer-room air-conditioning units
- Fans
- Heat exchangers
- Control valves
- Water-treatment equipment
- Building-management-system monitoring
- Temperature and humidity sensors
- Leak-detection systems
- Outdoor-air and exhaust systems
- Freeze-protection systems

Facility personnel shall confirm:

1. Cooling is available to each occupied data hall or critical equipment area.
2. Required pumps and fans are operating.
3. Supply and return temperatures are within approved operating ranges.
4. Water flow, pressure, and level are adequate.
5. No cooling-system alarms or leaks are present.
6. Redundant cooling capacity remains available.
7. Cooling demand does not exceed available emergency-power capacity.
8. Temperature trends are stable.

Loss of cooling shall not be evaluated solely by the current room temperature. Personnel shall consider:

- Rate of temperature increase
- Current electrical and IT load
- Available redundant cooling
- Outdoor temperature
- Estimated repair time

DRAFT

- Safe equipment shutdown time
- Potential impacts of shutting down and restarting equipment

Generator Fuel and Remaining Runtime

During generator operation, authorized personnel shall determine the amount of usable fuel and estimated remaining runtime.

The following information shall be documented:

Fuel and Runtime Element	Current Status
Total measured fuel	To be determined by tenant organization
Usable fuel	To be determined by tenant organization
Required reserve	To be determined by tenant organization
Current generator load	To be determined by tenant organization
Current burn rate	To be determined by tenant organization
Estimated remaining runtime	To be determined by tenant organization
Estimated utility restoration	To be determined by tenant organization
Safe shutdown duration	To be determined by tenant organization
Required operational margin	To be determined by tenant organization
Next delivery status	To be determined by tenant organization

Loss of Water or Wastewater Service

Upon loss or degradation of water service, facility personnel shall determine whether the interruption affects:

- Fire-protection water
- Cooling-system makeup water
- Domestic water
- Sanitary fixtures
- Equipment cleaning
- Emergency eyewash or shower systems
- Other safety-related uses

DRAFT

Personnel shall verify:

1. Water pressure and available storage.
2. Fire-water system status.
3. Fire-pump suction or supply conditions.
4. Cooling-system water levels and makeup-water capacity.
5. Expected water-consumption rate.
6. Estimated duration of available onsite water.
7. Availability of an alternate water source.
8. Utility-provider restoration estimates.

If fire-protection water is impaired, the facility shall:

- Notify Marshalls Creek Volunteer Fire Company
- Notify Smithfield Township
- Implement required impairment procedures
- Restrict hazardous work
- Establish additional monitoring or fire-watch measures when required
- Consider partial shutdown, full shutdown, or evacuation when adequate fire protection cannot be maintained

Loss of wastewater service shall be evaluated for impacts on occupancy, sanitation, cooling, environmental compliance, and continued facility operation.

Cyber Incident Response

Cyber incident response procedures are intended to protect life-safety systems, facility controls, information systems, operational technology, physical security, and continuity of critical operations.

A cyber incident may include:

- Ransomware
- Malware
- Denial-of-service activity
- Credential compromise
- Unauthorized remote access
- Vendor-access compromise
- Insider activity
- Unexpected changes to control settings
- Loss or manipulation of system data

DRAFT

- Disabling of monitoring, alarms, or communications
- Unauthorized operation of electrical, cooling, security, or building systems
- An unexplained simultaneous failure of network-connected equipment
- A cyber incident occurring during a fire, utility outage, security incident, or other physical emergency

The facility cyber-threat profile identifies building-management controls, electrical monitoring, cooling controls, access control, cameras, fire-alarm interfaces, telecommunications, emergency notifications, and remote-support platforms as potentially affected systems. The County plan identifies networked and computer-controlled processes as major cyber vulnerabilities and notes the increasing prevalence of phishing, ransomware, and attacks on essential-service providers.

Reporting Suspected Cyber Compromise

Any employee, contractor, vendor, or system user who observes suspected cyber activity shall immediately report it to:

- IT or Cybersecurity Contact to be determined by tenant organization
- Emergency Coordinator
- Security Operations Center to be determined by tenant organization
- Other Designated Contact to be determined by tenant organization

Indicators may include:

- Unexpected login prompts
- Unauthorized password or account changes
- Unrecognized administrative accounts
- Repeated failed login attempts
- Unusual vendor or remote-access activity
- Ransom messages
- Files becoming encrypted or unavailable
- System commands occurring without operator input
- Unexpected changes to temperature, power, ventilation, or access settings
- Loss of camera, alarm, sensor, or control visibility
- Conflicting information between local equipment displays and network interfaces
- Simultaneous alarms or failures across unrelated systems
- Unexplained system restarts
- Disabled security tools
- Unexpected network traffic

DRAFT

- Unapproved USB devices or other connected equipment

Personnel **will not**:

- Delete suspicious files
- Power off affected equipment unless necessary for life safety or directed by authorized cybersecurity personnel
- Contact a suspected attacker
- Pay or negotiate a ransom
- Reconnect isolated equipment
- Use personal devices to access affected systems
- Share incident information externally without authorization

Initial Cyber Incident Assessment

The Cyber Incident Lead to be determined by tenant organization shall determine:

1. Systems affected.
2. Whether information-technology, operational-technology, or both environments are involved.
3. Whether the incident affects life-safety or emergency systems.
4. Whether the incident is ongoing.
5. Whether unauthorized changes have been made.
6. Whether credentials may be compromised.
7. Whether vendor or remote access was involved.
8. Whether data has been encrypted, altered, deleted, or removed.
9. Whether a physical equipment failure or utility interruption may be mistaken for a cyber incident.
10. Whether public safety agencies or external cybersecurity resources are needed.

When the extent of compromise is unknown, affected systems shall be treated as untrusted until evaluated.

Cyber Incident Lead

The Cyber Incident Lead to be determined by tenant organization shall direct:

- Cybersecurity investigation
- Network containment
- Account and credential controls
- Vendor-access restrictions
- Evidence preservation

DRAFT

- System recovery
- Technical coordination with external cybersecurity resources

Facility Emergency Coordinator

The Emergency Coordinator shall direct:

- Life-safety actions
- Facility protective actions
- Manual facility operations
- Evacuation or shelter-in-place
- Emergency-service coordination
- Utility and contractor coordination
- Operational shutdown decisions

Critical Operations Personnel

Critical operations personnel shall:

- Verify local equipment condition
- Compare network data with local displays and instruments
- Operate systems manually when authorized
- Report abnormal electrical, cooling, fuel, battery, or environmental conditions
- Implement approved shutdown procedures when required

When a cyber incident creates or accompanies a physical emergency, the fire department or other responding public safety agency shall exercise incident command over fire suppression, rescue, evacuation, hazardous conditions, and other public-safety operations. The Cyber Incident Lead shall continue directing technical containment and recovery in coordination with the Incident Commander and Emergency Coordinator.

Immediate Containment

When authorized by the Cyber Incident Lead, containment actions may include:

- Disconnecting affected devices from the network
- Isolating affected network segments
- Blocking malicious addresses or connections
- Disabling compromised accounts
- Resetting or revoking credentials
- Restricting privileged access
- Suspending remote access

DRAFT

- Disabling vendor-access connections
- Removing affected wireless access
- Blocking unapproved removable media
- Isolating backup systems from affected networks
- Preserving unaffected offline backups
- Restricting physical access to affected control rooms, network rooms, and equipment

Containment shall be performed in a manner that does not unintentionally disable:

- Fire alarms
- Fire pumps
- Automatic suppression
- Gas detection
- Battery monitoring
- Emergency lighting
- Smoke control
- Required cooling
- Electrical protection
- Emergency communications
- Security functions required for evacuation or responder access

Before disconnecting a network-connected operational system, personnel shall determine whether disconnection could cause the equipment to stop, fail to a hazardous condition, or become unavailable for manual control.

Restricting Vendor and Remote Access

Upon suspected compromise of remote or vendor access, the facility shall:

1. Disable affected accounts, sessions, certificates, tokens, or connections.
2. Suspend nonessential remote access.
3. Notify affected vendors through a known, independent contact method.
4. Require verification of vendor identity before restoring access.
5. Review recent vendor activity and system changes.
6. Establish time-limited and monitored access when emergency vendor support is necessary.
7. Require approval from [Cyber Incident Lead] before remote access is restored.
8. Document all temporary access granted during the incident.

Credentials suspected of compromise shall not be reused.

DRAFT

Transition to Manual Facility Operations

When automated controls or network monitoring cannot be trusted, authorized personnel shall transition affected systems to approved manual or local control.

Manual operations may include:

- Local generator monitoring
- Local UPS and battery monitoring
- Manual recording of temperatures and humidity
- Local observation of cooling equipment
- Manual operation of pumps, fans, or valves
- Local verification of electrical equipment
- Manual gate or door control
- Physical security patrols
- Manual personnel accountability
- Direct radio or telephone communication
- Manual alarm or incident logging

Personnel shall use approved hard-copy procedures, one-line diagrams, equipment manuals, contact lists, and checklists.

Manual operation shall only continue when:

- Local equipment condition can be verified
- Qualified personnel are available
- Required staffing can be maintained
- Life-safety systems remain operational
- Manual control does not expose personnel to electrical, mechanical, battery, fuel, fire, or hazardous-gas conditions

When safe manual control cannot be maintained, the affected equipment or area shall be placed in a safe condition or shut down.

Verification of Life-Safety and Critical Systems

During a cyber incident, facility personnel shall directly verify the independent operation of:

- Fire alarm panels
- Smoke and heat detection
- Automatic suppression systems
- Fire pumps

DRAFT

- Gas detection
- Battery monitoring
- Emergency lighting
- Exit signs
- Access-control systems
- Emergency gates and responder access
- Electrical protection systems
- UPS and generator controls
- Cooling equipment
- Environmental monitoring
- Emergency notification systems
- Facility communications

Verification shall use local panels, equipment displays, independent instruments, physical inspection, or other methods not dependent on the suspected compromised network.

The results shall be recorded in a cyber life-safety status checklist.

When a life-safety system cannot be verified, the facility shall:

1. Notify Emergency Coordinator.
2. Notify the Marshalls Creek Volunteer Fire Company or authority having jurisdiction when appropriate.
3. Establish required compensatory measures.
4. Restrict hazardous work and access.
5. Consider partial shutdown or evacuation.
6. Maintain the system as impaired until inspected and approved.

A network dashboard indicating normal status shall not be considered sufficient when the integrity of the network or monitoring system is in question.

Alternate Communications

When normal communications are compromised, facility personnel shall use available independent communication methods, including:

- Cellular telephones
- Two-way radios
- Satellite telephones
- Independent analog lines
- In-person messengers

DRAFT

- Facility intercoms not connected to the affected network
- Direct communication with the Monroe County Control Center
- Pre-established external conference lines or emergency communication platforms

Sensitive incident information shall only be transmitted using methods approved by Cyber Incident Lead.

Preservation of Logs and Forensic Evidence

Personnel shall preserve potential evidence, including:

- System logs
- Firewall logs
- Authentication records
- Remote-access records
- Building-management-system logs
- Electrical and cooling control logs
- Access-control records
- Camera footage
- Alarm records
- Email and messaging records
- Ransom notes
- Malicious files
- Memory images and disk images, when collected by qualified personnel
- Photographs of system displays
- Notes documenting operator observations and actions

Personnel shall record:

- Date and time of discovery
- Person discovering the incident
- Initial indicators
- Systems affected
- Actions taken
- Accounts disabled
- Devices isolated
- Commands issued
- Notifications made
- Evidence collected
- Persons handling the evidence

DRAFT

Original evidence shall not be altered unnecessarily. Access shall be limited, and chain-of-custody procedures shall be used when evidence may be provided to law enforcement, an insurer, legal counsel, or an external investigator.

Simultaneous Cyber and Physical Emergency

A simultaneous cyber and physical emergency may include:

- A cyber incident during a utility outage
- Manipulation of cooling or electrical controls causing overheating or equipment failure
- Loss of access control during a fire
- Loss of alarm monitoring during a battery emergency
- A cyber incident used to conceal unauthorized physical access
- Failure of networked systems during a hazardous-material or severe-weather incident

During a combined incident:

1. Life safety shall take priority.
2. Occupants shall follow fire alarm, evacuation, shelter-in-place, or emergency responder instructions.
3. The fire department or appropriate public safety agency shall be notified of unreliable or compromised facility systems.
4. Facility personnel shall identify which alarms, controls, cameras, access systems, and communications cannot be trusted.
5. Local and manual verification shall replace network-dependent status information.
6. Cyber containment shall not delay evacuation, 9-1-1 notification, fire suppression, or emergency shutdown.
7. Physical access to network rooms, control rooms, electrical rooms, and other affected areas shall be restricted.
8. Cybersecurity personnel shall coordinate with the public safety Incident Commander before isolating systems that support emergency operations.
9. An alternate facility command location shall be established if the normal control room is compromised.
10. A controlled shutdown shall be initiated when safe operation cannot be verified.

External Notifications

The following parties shall be notified as conditions warrant:

- Tenant Organization

DRAFT

- Cybersecurity Leadership to be determined by tenant organization
- Emergency Coordinator
- Security
- Legal Counsel
- Cyber Insurance Carrier to be determined by tenant organization
- Affected Customers or Tenants to be determined by tenant organization
- Critical Vendors to be determined by tenant organization
- Pennsylvania State Police
- Marshalls Creek Volunteer Fire Company
- Smithfield Township Emergency Management Coordinator
- Applicable Regulatory Agency to be determined by tenant organization
- External Cybersecurity Response Provider to be determined by tenant organization
- Other Appropriate Contact to be determined by tenant organization

Notification to customers or tenants shall be coordinated through authorized management and legal personnel and shall not disclose unverified information.

Manual Fire-Suppression Procedures

Portable fire extinguishers shall be installed based on the hazards present and applicable code requirements.

Only trained and authorized personnel may attempt to extinguish a small, incipient-stage fire. Personnel shall not attempt suppression when:

- Smoke affects visibility or breathing
- The fire is spreading
- The fire involves battery thermal runaway
- Energized electrical equipment is exposed
- An explosion or arc-flash hazard is present
- The person does not have a clear evacuation route
- The appropriate extinguisher rating is not immediately available

Evacuation and notification of the fire department shall take priority over manual fire suppression.

Electrical Equipment Fire

During a fire involving electrical equipment:

- Personnel shall not approach exposed energized equipment

DRAFT

- Water-based portable extinguishers **will not** be used on energized electrical equipment
- Electrical isolation shall only be performed by trained and authorized personnel
- Responders shall be informed of equipment voltage, stored-energy hazards, and disconnect locations
- Areas containing damaged electrical equipment shall remain restricted until inspected and declared safe

Generator or Fuel-System Fire

During a generator or fuel-system fire:

1. The fire alarm shall be activated.
2. 9-1-1 shall be notified.
3. Personnel shall evacuate the affected area.
4. Fuel-transfer operations shall stop.
5. Emergency fuel shutoffs shall be activated when they can be reached safely or operated remotely.
6. Responders shall be provided with the fuel type, storage quantity, tank locations, containment features, and shutoff locations.

Battery Emergency Procedures

Upon indication of battery overheating, off-gassing, smoke, or thermal runaway:

1. The fire alarm shall be activated.
2. 911 shall be notified.
3. The affected battery area and required adjacent areas shall be evacuated.
4. Access shall be restricted.
5. The approved battery shutdown shall be activated remotely when available.
6. Dedicated ventilation and gas exhaust shall operate according to the approved sequence.
7. Responders shall be provided with battery chemistry, capacity, Safety Data Sheets, manufacturer guidance, and system drawings.
8. The affected system shall remain out of service until inspected and approved by qualified personnel.
9. Monitoring shall continue for potential re-ignition.

Fire and Smoke Containment Actions

During an emergency:

DRAFT

1. Fire doors shall remain closed.
2. Doors shall not be blocked or propped open.
3. The affected area shall be isolated from unauthorized entry.
4. Fire and smoke dampers shall operate in accordance with the approved sequence.
5. Ventilation serving the affected area shall be isolated as designed.
6. Adjacent areas shall be evaluated for smoke, heat, or hazardous-gas migration.
7. Fire-rated barriers shall not be reopened or bypassed without approval from the fire department.

Emergency Ventilation and Smoke-Control Actions

Manual operation or override of smoke-control systems shall be limited to:

- The fire department Incident Commander
- Authorized Facility Position to be determined by tenant organization
- Other Authorized Position to be determined by tenant organization

Normal ventilation shall not be restored until:

1. The fire department confirms that suppression operations are complete.
2. The affected area has been evaluated for re-ignition.
3. Electrical hazards have been controlled.
4. Smoke and hazardous gases have been removed.
5. Required air monitoring has been completed.
6. The area is authorized for reentry.

Battery-Area Ventilation Response

During a battery off-gassing or thermal-runaway event:

- The affected area shall be evacuated
- Air recirculation from the battery area shall stop
- Dedicated exhaust systems shall operate in accordance with the approved design
- Personnel shall not enter the area without appropriate training and protective equipment
- Ventilation settings shall not be altered without coordination with the fire department
- Gas monitoring shall be completed before reentry

Evacuation and Personnel Accountability

Evacuation Initiation

Evacuation shall begin upon:

DRAFT

- Activation of the building fire alarm
- Direction from facility management
- Direction from security personnel
- Direction from the fire department or another public safety agency
- Observation of fire, smoke, battery off-gassing, or another immediate life-safety threat

Occupant Actions

Upon notification to evacuate, occupants shall:

- Stop work when it is safe to do so
- Leave the area using the nearest safe exit
- Avoid elevators unless directed by emergency responders
- Close doors behind them
- Assist visitors and individuals requiring additional support
- Proceed to the designated assembly area
- Report to the person conducting accountability
- Remain at the assembly area until released
- Do not re-enter the facility for any reason unless specifically directed to return to work locations by on scene fire department or first responder in charge of the incident

Personnel Accountability

The facility operator shall establish an accountability system using employee rosters, access-control records, visitor logs, contractor records, and supervisor reports.

Missing persons shall be reported to the fire department Incident Commander. Employees shall not reenter the building to search for missing persons.

DRAFT

Part V - Recovery

Reentry

No person shall reenter an evacuated or restricted area until the fire department or other agency having incident command has determined that emergency operations are complete and the area may be evaluated for reentry.

Reentry shall also require authorization from Emergency Coordinator or Authorized Facility Representative to be determined by tenant organization.

Before reentry is authorized:

- Fire, smoke, and hazardous-gas conditions shall be controlled
- Electrical hazards shall be isolated
- Battery systems shall be evaluated for continued heating or re-ignition
- Structural conditions shall be assessed
- Required air monitoring shall be completed
- Fire-protection and life-safety systems shall be evaluated
- Restricted areas shall be clearly identified

Reentry authorization does not constitute approval to return affected equipment or systems to normal operation.

Restoration and Electrical Resynchronization

Normal operations shall not resume solely because utility service appears to have returned.

Before restoration, authorized personnel shall confirm:

1. The utility provider has identified the service as stable.
2. The cause of the interruption has been identified when practicable.
3. No unsafe voltage, frequency, phase, grounding, surge, or equipment condition is present.
4. Switchgear, transfer switches, UPS systems, generators, electrical rooms, and distribution equipment have been inspected.
5. Cooling systems are available.
6. Water, telecommunications, security, and life-safety systems are operational.
7. Required repairs have been completed.
8. Restoration has been authorized by Authorized Facility Position to be determined by tenant organization.

DRAFT

Transfer from emergency generation to normal utility service shall:

- Follow the approved electrical sequence
- Be performed by trained and authorized personnel
- Confirm acceptable utility voltage, frequency, and phase conditions
- Confirm synchronization requirements where applicable
- Transfer one approved distribution path or load group at a time
- Avoid simultaneous restoration of loads that could cause an excessive inrush or demand condition
- Verify each restored system before proceeding to the next
- Maintain life-safety and cooling systems throughout the transfer
- Allow generators to complete the approved cooldown sequence
- Return generators, UPS systems, batteries, and transfer switches to automatic standby status
- Replenish generator fuel
- Reset alarms only after their causes have been confirmed
- Continue heightened monitoring for Time Period To be determined by tenant organization

The facility shall document the restoration sequence, system status, person authorizing restoration, abnormalities encountered, and time normal operations resumed.

Cyber System Restoration Authorization

No compromised or potentially compromised system shall be restored to production service solely because it appears functional.

Restoration shall require authorization from:

- Cyber Incident Lead
- Emergency Coordinator, when operational systems are involved
- Authorized Facility Position to be determined by tenant organization
- System Owner to be determined by tenant organization
- Other Required Approver to be determined by tenant organization

Before restoration:

1. The affected system shall be isolated and evaluated.
2. The method of compromise shall be identified when practicable.
3. Malicious access shall be removed.
4. Compromised credentials shall be replaced.

DRAFT

5. Required security corrections shall be applied.
6. The system shall be rebuilt from a known-good source when required.
7. Backups shall be scanned and validated.
8. Configuration settings shall be compared with approved baselines.
9. Operational and life-safety functions shall be tested locally.
10. Network connectivity shall be restored in a controlled manner.
11. Monitoring shall be active.
12. A rollback or re-isolation method shall be available.

Controlled Reconnection and Return to Service

Systems shall be restored in phases.

Recommended restoration order:

1. Independent life-safety systems.
2. Emergency communications.
3. Core network-security and monitoring services.
4. Electrical monitoring and control.
5. Cooling and environmental control.
6. Physical access control and security.
7. Critical operations systems.
8. Vendor and remote-support access.
9. Noncritical administrative systems.

After reconnection, personnel shall monitor for:

- Repeated unauthorized activity
- Unexpected configuration changes
- Abnormal network traffic
- Recurring alarms
- Conflicting local and remote status information
- Equipment instability
- Loss of cooling, electrical, security, or alarm functionality

A restored system shall be immediately re-isolated if suspicious activity resumes.

Cyber Incident Documentation and Corrective Actions

Following the incident, the tenant organization shall document:

- Systems and networks affected
- Operational impacts

DRAFT

- Life-safety impacts
- Utility or customer impacts
- Initial access method, when known
- Containment actions
- Manual operations implemented
- Shutdowns or evacuations
- Evidence preserved
- Notifications made
- Restoration actions
- Time systems returned to service
- Required corrective actions

The post-incident review shall determine whether changes are needed to:

- Network segmentation
- Remote and vendor access
- Account privileges
- Multifactor authentication
- Backup procedures
- Manual operating capabilities
- Life-safety-system independence
- Emergency communications
- Cyber and facility incident-command coordination
- Staff training
- Contractor requirements
- This Emergency Response Plan

Because the facility has not yet been constructed, the bracketed roles, communication methods, load priorities, operating thresholds, fuel reserves, safe-shutdown periods, and system-specific manual procedures must be completed after the final electrical, mechanical, telecommunications, security, and control-system designs are available and before occupancy.

Post-Incident Assessment

Following an emergency, qualified personnel shall evaluate the affected facility areas and systems. The assessment shall address, as applicable:

- Structural damage
- Electrical equipment and wiring

DRAFT

- Fire alarm and suppression systems
- Fire-rated walls, doors, and penetrations
- HVAC and smoke-control systems
- Battery systems
- Generators and fuel systems
- Emergency access roads and hydrants
- Environmental releases
- Conditions affecting adjacent properties or the public

Unsafe equipment and areas shall remain isolated until repaired, tested, and approved.

Restoration of Facility Systems

Affected systems shall be restored in a controlled manner based on life safety, system dependencies, equipment condition, and manufacturer requirements.

Before a system is returned to service:

1. The source and extent of damage shall be identified.
2. Required repairs shall be completed.
3. The system shall be inspected and tested by qualified personnel.
4. Fire-protection and monitoring systems shall be restored.
5. Applicable regulatory or fire department approvals shall be obtained.
6. The return-to-service decision shall be documented.

Battery equipment involved in overheating, off-gassing, fire, or thermal runaway shall not be returned to service until evaluated by Battery Manufacturer, Qualified Engineer, or Authorized Service Provider to be determined by tenant organization.

Incident Documentation and Investigation

The tenant organization shall document each significant emergency. Documentation shall include:

- Date, time, and location of the incident
- Conditions initially observed
- Notifications made
- Emergency actions taken
- Evacuation and accountability results
- Agencies and contractors involved
- Systems or equipment affected
- Injuries or exposures

DRAFT

- Property or environmental damage
- Restoration actions
- Photographs, reports, and supporting records

An investigation shall be completed to identify the cause of the incident and determine whether facility design, maintenance, training, or emergency procedures contributed to the event.

Corrective Actions and Plan Revision

Corrective actions identified through the post-incident assessment or investigation shall be documented and assigned to a responsible party.

Corrective Action	Responsible Party	Target Completion Date	Completion Status

This ERP will be reviewed and revised when an incident identifies a deficiency in fire suppression, containment, ventilation, evacuation, emergency access, responder training, battery safety, or another emergency management measure.

DRAFT

DRAFT

DELTA | DEVELOPMENT | GROUP
INC.