ZETA ALPHA MEDICAL

Government-Funded Medical Data Center

Comprehensive Policy Framework

DOCUMENT CLASSIFICATION: CONFIDENTIAL

Version 1.0

February 2026

Prepared by: John D. Williams

Chief Information Security Officer

Table of Contents

Section 1: Executive Summary and Organizational Context

1.1 Mission Statement

The Zeta Alpha Medical Data Center exists for one purpose: to serve as the secure, government-funded repository for protected health information (PHI) generated by physicians and their patients. This is a medical-first facility. Every architectural decision, every policy provision, every operational procedure flows from a single non-negotiable principle: the sanctity of the doctor-patient relationship and the absolute confidentiality of the information entrusted to this facility.

This data center houses clinical records, diagnostic data, treatment histories, and information generated by medical devices deployed in the field. While the facility maintains no direct operational connection to those medical devices, the data they produce is transmitted to and stored on our servers. This creates an obligation that is simultaneously legal, ethical, and operational. A breach of this data does not merely violate a regulation; it violates a patient’s trust in their physician and in the system that physician relies upon.

1.2 Government Funding Acknowledgment

This facility has received federal government funding, which imposes compliance obligations beyond those of a commercially funded data center. Federal funding triggers mandatory adherence to the Federal Information Security Modernization Act (FISMA), the National Institute of Standards and Technology Special Publication 800-53 security control framework, and, depending on the nature of hosted workloads, potential Federal Risk and Authorization Management Program (FedRAMP) requirements.

These obligations are not optional addenda. They are conditions of funding acceptance and carry the force of federal law. Non-compliance jeopardizes not only the organization’s funding but its authorization to operate.

1.3 Regulatory Compliance Commitment

Given the dual nature of this facility as both a medical data repository and a government-funded operation, Zeta Alpha Medical commits to full compliance with the following regulatory and standards frameworks:

Framework	Applicability	Governing Authority
HIPAA / HITECH	All PHI stored, processed, or transmitted within the facility	U.S. Department of Health and Human Services (HHS)
FISMA	All federal information systems and data housed in the facility	Office of Management and Budget (OMB) / CISA
NIST SP 800-53 Rev. 5	Security and privacy control baseline for all systems	National Institute of Standards and Technology

NIST SP 800-66 Rev. 2	HIPAA implementation guidance mapped to NIST controls	NIST
FedRAMP (if applicable)	Required if hosting federal agency workloads in a shared/cloud model	FedRAMP PMO / GSA
FIPS 199 / FIPS 200	System categorization and minimum security requirements	NIST / OMB
21 CFR Part 11	Electronic records and signatures for medical device data	FDA
NIST SP 800-171 / CMMC	Applicable if facility handles Controlled Unclassified Information (CUI)	Department of Defense / NIST

1.4 Applicability Matrix

The following matrix defines precisely who, what, and where this policy framework applies. Given your note about needing help determining this, I have constructed a recommended matrix based on the medical data center profile. This should be reviewed and adjusted based on the specific organizational structure and tenant agreements.

Category	In Scope	Partial Scope	Out of Scope
Personnel	All data center staff, system administrators, network engineers, security personnel, facility management	Contracted maintenance vendors (bound by ISA/MOU), government tenant liaisons	End-user patients, referring physicians (governed by tenant-level policies)
Systems	All servers, storage arrays, network infrastructure, security appliances, backup systems, management consoles	Medical devices generating data (governed by device-level policies; data is in scope once received)	End-user devices not connecting to data center infrastructure
Data	All PHI, ePHI, medical device telemetry data, clinical records, diagnostic imaging, system logs, audit trails	De-identified data sets (subject to HIPAA de-identification standards verification)	Publicly available marketing materials, non-sensitive corporate communications
Facilities	Data center floor, server rooms, network operations center (NOC), security operations center (SOC), power/HVAC plant rooms	Administrative offices within the facility perimeter	Remote offices, offsite disaster recovery (governed by separate DR policy)

Third Parties	Colocation tenants processing PHI, managed service providers with system access	Hardware vendors, courier services (facility access only, no data access)	Utility providers, external law enforcement (access governed by legal process)

1.5 Relationship to Parent Organization

This policy framework extends and supersedes the existing Zeta Alpha Medical Security Strategy developed as the organization's foundational cybersecurity posture. The original Zeta Alpha capstone policies (Information Security Program Policy, Risk Management Policy, Access Control Policy, Mobile Device and IoT Policy, Acceptable Use Policy, Non-Compliance Policy, and Email/Messaging Policy) serve as the structural foundation for this data center-specific framework.

Where the original Zeta Alpha policies were designed around NIST Cybersecurity Framework (CSF) alignment and a four-tier data classification model, this data center framework upgrades the compliance baseline to NIST SP 800-53 Rev. 5 with a HIGH impact baseline, implements the NIST SP 800-37 Risk Management Framework, and introduces data center-specific policies for physical security, environmental controls, operations, network architecture, and tenant management that did not exist in the original suite.

In cases of conflict between the parent organization's policies and this framework, this framework governs for all operations within the data center facility boundary.

1.6 FIPS 199 Security Categorization

The security categorization of information systems within this data center is determined per Federal Information Processing Standard (FIPS) 199. Given that the primary mission is to house protected health information including doctor-patient records and medical device telemetry data, the categorization is as follows:

Security Objective	Impact Level	Justification
Confidentiality	**HIGH**	Unauthorized disclosure of PHI would cause severe harm to individuals (identity theft, discrimination, reputational damage to patients and physicians). Doctor-patient privilege is a legal and ethical absolute. Federal law (HIPAA/HITECH) imposes breach notification requirements and penalties up to $1.5M per violation category per year.
Integrity	**HIGH**	Unauthorized modification of medical records or device telemetry data could directly endanger patient lives. A corrupted lab result, altered medication record, or manipulated device reading could lead to misdiagnosis, incorrect treatment, or death. The standard of care depends on data integrity.

Availability	**MODERATE**	While this facility serves as a data repository rather than a real-time clinical decision support system, extended downtime would disrupt physician access to patient histories, impede continuity of care, and violate SLA obligations to government tenants. The assessment is MODERATE rather than HIGH because the facility is not the primary point-of-care system; clinical operations do not cease if the repository is temporarily unavailable.

Overall System Categorization: HIGH

Per FIPS 199, the overall categorization is the highest watermark across all three security objectives. With Confidentiality and Integrity both at HIGH, the system is categorized as HIGH impact. This determination drives the selection of the NIST SP 800-53 HIGH baseline control set, which is the most rigorous and comprehensive control suite NIST publishes for non-classified systems.

Section 2: Information Security Program Policy

2.1 Purpose

This policy establishes the Information Security Program for the Zeta Alpha Medical Data Center. It defines the organizational structure, governance mechanisms, and strategic direction for protecting all information assets housed within this facility. This policy supersedes the original Zeta Alpha Information Security Program Policy and extends its scope to address the specific requirements of a government-funded medical data repository operating under a NIST SP 800-53 HIGH baseline.

2.2 Scope

This policy applies to all personnel, systems, data, and facilities identified in the Applicability Matrix (Section 1.4). It governs the entire lifecycle of information security within the data center, from risk assessment through continuous monitoring, and is applicable across all operational shifts, including after-hours and emergency operations.

2.3 Policy Governance Structure

The Information Security Program is led by the Chief Information Security Officer (CISO) in coordination with the Chief Technology Officer (CTO) and the Data Center Operations Director. The governance structure includes the following key roles and responsibilities:

1. **Chief Information Security Officer (CISO):** Holds overall accountability for the security posture of the data center. Responsible for policy development, risk oversight, compliance reporting, and serving as the primary liaison with federal oversight bodies. Authorizes the System Security Plan (SSP) and signs the Authorization to Operate (ATO) package.
2. **Chief Technology Officer (CTO):** Responsible for the technical architecture and engineering decisions that implement security controls. Works in coordination with the CISO to ensure that technology selections meet the NIST SP 800-53 HIGH baseline requirements.
3. **Data Center Operations Director:** Manages day-to-day operational implementation of security policies, including physical security, environmental controls, and operational procedures. Reports to the CTO with a dotted-line reporting relationship to the CISO on all security matters.
4. **Information System Security Officer (ISSO):** Serves as the hands-on security practitioner responsible for implementing and monitoring security controls, maintaining the SSP, managing the POA&M, and conducting continuous monitoring activities.
5. **Privacy Officer:** Ensures HIPAA/HITECH compliance for all PHI processing and storage operations. Conducts Privacy Impact Assessments (PIAs) and manages breach notification obligations.

2.4 Federal Compliance Alignment

The original Zeta Alpha Information Security Program was aligned to the NIST Cybersecurity Framework (CSF). This data center framework upgrades the compliance baseline as follows:

2.4.1 FISMA Compliance

As a recipient of federal funding, this facility is subject to FISMA requirements. This means the data center must:

1. Maintain an inventory of all federal information systems.
2. Categorize systems per FIPS 199 (completed in Section 1.6; overall categorization: HIGH).
3. Implement the NIST SP 800-53 Rev. 5 HIGH baseline control set.
4. Conduct annual security assessments.
5. Develop and maintain a System Security Plan (SSP) for each major system boundary.
6. Submit annual FISMA reports through the designated federal reporting mechanism (CyberScope or its successor).
7. Maintain an active Authorization to Operate (ATO) signed by the Authorizing Official.

2.4.2 NIST SP 800-53 Rev. 5 Control Baseline

The HIGH impact categorization established in Section 1.6 requires implementation of the NIST SP 800-53 HIGH baseline. This is the most comprehensive control set NIST publishes for non-national-security systems. It encompasses 20 control families and over 400 individual controls and control enhancements. Key families with particular relevance to a medical data center include:

- **AC (Access Control):** Governs who can access what data under what conditions. Critical for enforcing doctor-patient confidentiality at the system level.
- **AU (Audit and Accountability):** Requires comprehensive logging of all access to PHI and system-level events. Non-negotiable for HIPAA compliance and government audit readiness.
- **SC (System and Communications Protection):** Mandates FIPS 140-2/140-3 validated encryption for all PHI in transit and at rest. This is a government mandate, not a recommendation.
- **PE (Physical and Environmental Protection):** Addressed in detail in Section 4 of this framework.
- **IR (Incident Response):** Must comply with both HIPAA breach notification timelines and CISA incident reporting requirements.
- **CM (Configuration Management):** Requires hardened baselines, change control, and configuration monitoring for all systems housing PHI.

2.4.3 FedRAMP Considerations

If this data center hosts federal agency workloads in a shared or cloud service model, FedRAMP authorization will be required. The HIGH baseline under FedRAMP aligns with NIST

SP 800-53 HIGH but adds specific requirements for continuous monitoring, incident response timelines, and third-party assessment organization (3PAO) engagement. The decision on FedRAMP scope should be made based on the specific tenant agreements with federal agencies. This policy framework is designed to support FedRAMP authorization if required.

2.5 Security Control Baseline Selection and Tailoring

The NIST SP 800-53 HIGH baseline serves as the starting point. The ISSO, in coordination with the CISO, shall conduct a formal tailoring process that:

1. Documents the rationale for any controls deemed not applicable to the medical data center operating environment.
2. Identifies additional controls or control enhancements required by HIPAA, HITECH, or specific government tenant agreements that exceed the standard HIGH baseline.
3. Incorporates organization-defined parameters for each control (e.g., specific audit log retention periods, session timeout values, password complexity rules).
4. Produces a tailored baseline that is documented in the System Security Plan (SSP).
5. Submits the tailored baseline for review and acceptance by the Authorizing Official.

2.6 Continuous Monitoring Strategy (ConMon)

Continuous monitoring is a federal requirement, not an optional best practice. The Zeta Alpha Medical Data Center shall implement a continuous monitoring program that provides ongoing awareness of the security posture of all systems within the authorization boundary. The ConMon strategy shall include:

1. Automated vulnerability scanning of all systems on a frequency no less than every 72 hours for HIGH impact systems, with results fed into the POA&M tracking system.
2. Automated Security Control Assessment (SCA) using tools such as SCAP-compliant scanners to validate configuration compliance against the tailored baseline.
3. Monthly reporting to the CISO on the security posture, including new vulnerabilities identified, POA&M status, and any deviations from the approved baseline.
4. Annual comprehensive security assessment conducted by an independent assessor or 3PAO (if FedRAMP is in scope).
5. Real-time security event monitoring through the Security Operations Center (SOC) with correlation to the SIEM platform.
6. Ongoing authorization process that replaces the traditional three-year ATO cycle with a risk-based continuous authorization model.

2.7 Plan of Action and Milestones (POA&M) Management

All identified security weaknesses, vulnerabilities, and non-compliant controls shall be documented in the Plan of Action and Milestones (POA&M). The POA&M is not merely an administrative document; it is the facility’s binding remediation commitment to the Authorizing Official and, by extension, to the federal government.

POA&M management shall include:

- Documented weakness identification with risk rating (Critical, High, Moderate, Low).
- Assigned responsible parties for each remediation action.
- Realistic but aggressive milestone dates for remediation completion.
- Monthly POA&M reviews by the ISSO with quarterly reviews by the CISO.
- Escalation procedures for POA&M items that exceed their milestone dates.
- Critical and High findings from vulnerability scans must have POA&M entries created within 72 hours of identification, with remediation timelines not exceeding 30 days for Critical and 90 days for High.

2.8 Policy Review and Maintenance

This policy shall be reviewed annually at minimum, or upon the occurrence of any of the following trigger events: a significant security incident, a material change in the regulatory environment, a new government tenant onboarding, a change in the facility’s FIPS 199 categorization, or direction from the Authorizing Official. All revisions shall be documented with version control and require CISO approval before implementation.

Section 3: Risk Management Policy

3.1 Purpose

This policy establishes the risk management framework for the Zeta Alpha Medical Data Center. It upgrades the original Zeta Alpha Risk Management Policy from a NIST Cybersecurity Framework (CSF) alignment to the NIST SP 800-37 Risk Management Framework (RMF), which is the mandatory risk management methodology for federal information systems. This upgrade is required by the facility's government funding and HIGH impact categorization.

3.2 Scope

This policy applies to all information systems, data repositories, network infrastructure, and supporting operational technology within the data center authorization boundary. It encompasses the identification, assessment, mitigation, and ongoing monitoring of risks to the confidentiality, integrity, and availability of all information processed, stored, or transmitted by the facility, with particular emphasis on protected health information and medical device telemetry data.

3.3 NIST SP 800-37 Risk Management Framework Implementation

The RMF provides a structured, six-step process for managing security and privacy risk. Each step is mandatory and must be documented. The six steps are:

Step 1: Categorize

Categorize the information system and the information processed, stored, and transmitted by the system based on FIPS 199 impact analysis. This step has been completed in Section 1.6 of this framework, resulting in an overall HIGH categorization. The categorization shall be reviewed annually or whenever there is a significant change to the types of data processed or the system's operational profile.

Step 2: Select

Select the appropriate set of security controls from NIST SP 800-53 Rev. 5 based on the categorization. For a HIGH impact system, this is the HIGH baseline. The selection process shall include formal tailoring as described in Section 2.5, with documentation of all tailoring decisions in the System Security Plan (SSP). Additional controls required by HIPAA, HITECH, 21 CFR Part 11, or government tenant agreements shall be overlaid onto the tailored baseline.

Step 3: Implement

Implement the selected security controls and document the implementation details in the SSP. Each control implementation statement shall describe how the control is satisfied within the data center environment, identify the responsible party, and specify the technology, process, or procedure used to achieve compliance. Implementation shall follow a risk-prioritized sequence, with controls protecting PHI confidentiality and integrity receiving the highest priority.

Step 4: Assess

Assess the security controls to determine whether they are implemented correctly, operating as intended, and producing the desired outcome. Assessment shall be conducted by an independent assessor (not the team responsible for implementation). For FedRAMP-scoped systems, a 3PAO shall conduct the assessment. Assessment results shall be documented in a Security Assessment Report (SAR).

Step 5: Authorize

The Authorizing Official (AO) reviews the SAR, the SSP, and the POA&M to make a risk-based authorization decision. The AO may issue an Authorization to Operate (ATO), an Interim Authorization to Operate (IATO) with conditions, or a Denial of Authorization to Operate (DATO). No system shall process PHI or government data without an active authorization.

Step 6: Monitor

Continuously monitor the security controls, the operating environment, and risk posture of the system. This step integrates with the Continuous Monitoring Strategy described in Section 2.6. Monitoring activities shall include automated scanning, log analysis, change detection, and periodic reassessment of controls.

3.4 System Security Plan (SSP) Requirements

The SSP is the single most important document in the RMF process. It is the comprehensive record of the system’s security posture and the organization’s commitment to the Authorizing Official. The Zeta Alpha Medical Data Center shall maintain an SSP that includes, at minimum:

1. System identification and categorization (including FIPS 199 results).
2. Authorization boundary definition with clear diagrams showing what is inside and outside the boundary.
3. System architecture description, including data flow diagrams showing how PHI moves through the environment.
4. Complete inventory of hardware, software, and firmware within the boundary.
5. Personnel roles and responsibilities for security.
6. Control implementation statements for every control in the tailored baseline.
7. Interconnection details for all external system connections, documented via Interconnection Security Agreements (ISAs).
8. Continuous monitoring strategy summary.
9. POA&M reference.

The SSP shall be maintained as a living document, updated whenever there are significant changes to the system, and reviewed in its entirety at least annually.

3.5 FIPS 199/200 Categorization Process

The initial categorization has been performed in Section 1.6. This section establishes the ongoing process for maintaining accurate categorization:

- Categorization shall be reviewed annually as part of the ATO renewal cycle.
- Any change in the types of data processed (e.g., onboarding a tenant that processes data with different sensitivity) triggers a recategorization review.
- If recategorization results in a higher impact level, the organization has 90 days to implement the additional controls required by the new baseline.
- If recategorization results in a lower impact level, the organization may reduce controls only after the Authorizing Official approves the change in writing.
- All categorization decisions shall reference the data types catalog maintained by the Privacy Officer, which maps each data type to its FIPS 199 impact level across all three security objectives.

3.6 Supply Chain Risk Management (SCRM)

The medical data center supply chain introduces risks that are distinct from and in addition to traditional cybersecurity risks. A compromised hardware component, a backdoored firmware update, or a malicious insider at a vendor can undermine every other control in this framework. NIST SP 800-161 Rev. 1 provides guidance specific to cybersecurity supply chain risk management.

The Zeta Alpha Medical Data Center shall implement the following SCRM provisions:

1. Maintain a critical supplier registry identifying all vendors whose products or services directly support systems within the authorization boundary.
2. Require SCRM flow-down clauses in all contracts with critical suppliers, mandating that they maintain security practices commensurate with the data center’s HIGH impact baseline.
3. Conduct supply chain risk assessments for all new hardware and software acquisitions before deployment within the authorization boundary.
4. Prohibit the deployment of products from vendors identified on government restriction lists (e.g., Section 889 of the NDAA, Entity List administered by BIS).
5. Require tamper-evident packaging and chain-of-custody documentation for all hardware deliveries to the facility.
6. Validate firmware and software integrity against vendor-published hashes before installation on any system within the boundary.
7. Conduct annual reviews of critical supplier security postures, including the right to audit or require SOC 2 Type II reports.

3.7 Risk Assessment Methodology

Risk assessments shall follow NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments. Assessments shall be conducted annually and upon any significant change to the system or operating environment. The methodology shall include:

- Threat identification using current threat intelligence sources relevant to the healthcare and government sectors.
- Vulnerability identification through automated scanning, manual testing, and review of vendor advisories.
- Likelihood determination based on threat capability, intent, and targeting, combined with the effectiveness of existing controls.
- Impact determination referencing the FIPS 199 categorization and considering both quantitative (financial) and qualitative (reputational, patient safety) factors.
- Risk determination combining likelihood and impact into a risk rating that drives prioritization in the POA&M.

3.8 Policy Review

This policy shall be reviewed annually, or upon the occurrence of a significant security incident, a material change in the threat landscape, a new government tenant onboarding, or a directive from the Authorizing Official.

Section 4: Physical and Environmental Security Policy

4.1 Purpose

This policy establishes the requirements for physical and environmental protection of the Zeta Alpha Medical Data Center. This is a net-new policy that did not exist in the original Zeta Alpha suite and addresses the unique physical security requirements of a facility housing protected health information under government funding. Physical security is the first line of defense; if an adversary can physically access the servers, every logical control in this framework is moot.

4.2 Scope

This policy applies to the entire data center facility, including all perimeter boundaries, entry points, server rooms, network operations center (NOC), security operations center (SOC), power and HVAC plant rooms, loading docks, storage areas, and administrative spaces within the facility perimeter. It covers all personnel who require physical access, including full-time employees, contractors, vendors, government tenant representatives, and visitors.

4.3 Facility Access Control

4.3.1 Security Zones

The facility shall be organized into concentric security zones, with each successive zone requiring additional authentication and authorization. The following zones are established:

Zone	Description	Access Method	Examples
Zone 1	Public/Reception	Sign-in, valid government-issued photo ID	Lobby, visitor reception area
Zone 2	Administrative/General	Badge access (proximity card)	Offices, conference rooms, break areas
Zone 3	Restricted Operations	Badge + PIN	NOC, SOC, cable plant rooms
Zone 4	High Security / Data Halls	Badge + Biometric (fingerprint or iris scan) + Mantrap	Server rooms, storage arrays, network core
Zone 5	Vault / Critical Infrastructure	Dual-person integrity + Badge + Biometric	Encryption key management systems, backup media vault

4.3.2 Mantrap Requirements

All Zone 4 and Zone 5 access points shall be equipped with mantrap (airlock) entry systems. Mantrap design and operational requirements include:

1. Two interlocking doors that cannot be open simultaneously.
2. Weight sensors or optical turnstile integration to prevent tailgating and piggybacking.

3. CCTV coverage of both the exterior and interior of the mantrap with a minimum of 30 days of footage retention.
4. Emergency release mechanisms that comply with local fire codes while maintaining an auditable record of emergency activations.
5. Anti-passback controls that prevent a single credential from being used to enter twice without an intervening exit event.

4.3.3 Visitor Management

1. All visitors must present a valid, government-issued photo ID at reception. The ID shall be verified against the visitor’s physical appearance and recorded in the visitor management system.
2. Visits must be pre-authorized by a sponsor who holds Zone 3 or higher access. Walk-in visitors without pre-authorization shall be denied entry beyond Zone 1.
3. Visitors shall be issued a temporary, visually distinct badge that must be worn and visible at all times. The badge shall include the visitor’s name, sponsor name, authorized zones, and expiration date/time.
4. Visitors shall be escorted at all times in Zone 3, Zone 4, and Zone 5 areas. The escort must hold access authorization equal to or greater than the zones being visited.
5. Visitor badges shall be collected upon departure and deactivated. Failure to return a badge triggers a security incident report.
6. The visitor log shall be retained for a minimum of three years for government audit purposes.

4.4 Perimeter Security

1. The facility perimeter shall be secured with anti-climb fencing (minimum 8 feet) with detection sensors (vibration or fiber-optic).
2. Vehicle barriers (bollards or planters) shall be installed at all vehicle approach points to prevent ram attacks.
3. Exterior lighting shall provide continuous illumination of all perimeter boundaries, entry points, and parking areas, with a minimum of 5 foot-candles at ground level.
4. CCTV cameras with pan-tilt-zoom capability and infrared night vision shall cover 100% of the perimeter with no blind spots. Footage shall be retained for a minimum of 90 days.
5. A security guard station shall maintain 24/7 staffing at the primary vehicle and pedestrian entry points.
6. All perimeter alarms shall be monitored in real time by the SOC, with a maximum response time of 5 minutes for alarm investigation.

4.5 Environmental Controls

4.5.1 HVAC and Temperature Management

1. Server room ambient temperature shall be maintained between 64°F and 80°F (18°C to 27°C) per ASHRAE TC 9.9 guidelines, with a target operating range of 68°F to 72°F.
2. Relative humidity shall be maintained between 40% and 60% to prevent static discharge and condensation.
3. HVAC systems shall be configured in an N+1 redundancy model at minimum, ensuring that the failure of any single cooling unit does not result in thermal exceedance.
4. Temperature and humidity monitoring sensors shall be deployed at the rack level (not merely the room level) with alerts triggering at 77°F and critical alarms at 80°F.
5. Hot aisle/cold aisle containment shall be implemented to maximize cooling efficiency and prevent recirculation.

4.5.2 Fire Detection and Suppression

1. Very Early Smoke Detection Apparatus (VESDA) shall be deployed in all server rooms, providing air-sampling smoke detection that identifies threats before they are visible to the human eye.
2. Fire suppression shall use clean agent systems (FM-200, Novec 1230, or equivalent) in all areas housing IT equipment. Wet-pipe sprinkler systems are prohibited in server rooms.
3. Pre-action dry-pipe sprinkler systems may be used in administrative and common areas.
4. Fire suppression system testing shall occur semi-annually, with full discharge tests conducted annually in coordination with the local fire marshal.
5. Emergency Power Off (EPO) buttons shall be installed at all server room exits, with clearly marked signage and tamper-evident covers to prevent accidental activation.

4.5.3 Water Detection

Water detection sensors shall be installed under all raised floors, beneath all HVAC units, and at all potential water ingress points (exterior walls, pipe penetrations, roof drains). Detection shall trigger immediate alerts to the NOC and facilities management team, with automatic shutoff valves on all water supply lines entering server room areas.

4.5.4 Power Management

1. Uninterruptible Power Supply (UPS) systems shall provide a minimum of 15 minutes of battery runtime at full load, sufficient to perform an orderly shutdown or bridge to generator power.
2. Diesel generators shall provide backup power for the entire facility with a minimum of 72 hours of fuel on-site at full load capacity, with fuel delivery contracts guaranteeing replenishment within 24 hours.
3. Power distribution shall follow a 2N design for Zone 4 and Zone 5 areas, providing dual independent power paths to every rack.

4. Automatic Transfer Switches (ATS) shall transfer load to generator power within 10 seconds of utility power loss.
5. Generator testing shall occur monthly under load, with annual full-load tests of a minimum of 4 hours duration.
6. Power monitoring at the rack level using intelligent PDUs that report real-time consumption and alert on anomalies.

4.6 Rack-Level Security and Cable Management

1. All racks in Zone 4 and Zone 5 shall be equipped with locking front and rear doors. Key management shall be centralized and auditable, with key checkout/check-in logged.
2. Electronic rack locks with audit trails are preferred over keyed locks and shall be deployed for all racks housing systems that process or store PHI.
3. Cable management shall ensure physical separation between power and data cables, with color-coded cabling standards to distinguish between network types (management, production, storage, out-of-band).
4. Structured cabling shall follow TIA-942 data center cabling standards, with all cabling labeled at both endpoints.
5. Unused ports on network switches and patch panels shall be physically disabled or covered to prevent unauthorized connections.

4.7 Media Handling, Sanitization, and Destruction

Given that this facility houses protected health information, media sanitization is not merely a best practice; it is a HIPAA and government mandate. All media handling shall comply with NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization.

- All storage media shall be tracked in a media inventory system from acquisition through destruction, with chain-of-custody documentation maintained throughout the lifecycle.
- Media leaving the authorization boundary for any reason (including RMA returns to vendors) shall be sanitized to the Clear or Purge level as appropriate for the data classification before leaving the facility.
- Media containing PHI or government data that cannot be sanitized to the Purge level (e.g., damaged drives) shall be destroyed using NSA/CSS-approved destruction methods. Destruction shall be witnessed by two authorized personnel and documented with certificates of destruction retained for the media's required record retention period.
- On-site media destruction equipment (degausser and physical shredder) shall be maintained for immediate destruction needs. Off-site destruction services shall be approved by the CISO, bonded and insured, and subject to annual audit.
- Sanitization verification shall be performed using forensic tools to confirm that no residual data remains after the sanitization process.

4.8 Delivery and Loading Dock Procedures

7. All deliveries shall be scheduled in advance through the facilities management team. Unscheduled deliveries shall be held at the perimeter until verified.
8. The loading dock is a Zone 2 area and shall be physically separated from Zone 3 and higher areas by a secure barrier with controlled access.
9. Delivery personnel shall not enter beyond the loading dock area without a visitor badge and escort as described in Section 4.3.3.
10. All incoming packages and equipment shall be inspected for tampering before being moved to staging or deployment areas.
11. Outgoing shipments containing equipment that has been in contact with systems processing PHI shall follow the media sanitization procedures in Section 4.7 before shipment.
12. CCTV coverage of the loading dock area shall be continuous, with footage retained for a minimum of 90 days.

4.9 Policy Review

This policy shall be reviewed annually, or upon any physical modification to the facility, a change in the facility’s Uptime Institute tier certification, a significant physical security incident, or direction from the Authorizing Official or the CISO.