PLAN

MDC and LDC Data Center Operations

Document Control

This section outlines the control and ownership of this document.

Organization	Anonymous Company
Plan Owner	Team Member 02, Director, Infrastructure, anonymized@example.com, XXX-XXX-XXXX
BCMS Manager	Team Member 01, Program Manager, Emergency Management, anonymized@example.com, XXX-XXX-XXXX (mobile)
Publish Date	[Publish Date]
Version	v1.0
Classification	Confidential/ Internal
Next Review	2/6/2027

Approval Signatures

Role	Signature	Date
Plan Owner		Click or tap to enter a date.
Executive Sponsor		Click or tap to enter a date.
BCMS Manager		Click or tap to enter a date.

Table of Contents

Executive Summary

This Business Continuity Plan (BCP) addresses the New Jersey Data Centers (Middletown and Lyndhurst) critical infrastructure supporting physical and virtual servers, storage, and networking equipment essential to AnonCo's business and clinical applications.

Core Definitions and Scope

- **Disaster Definition:** All hazards approach requiring data center core systems, facilities, and alternate resources.
- **Planning Assumption:** Complete loss of a single facility and/ or loss of primary systems during peak processing periods, with the plan assuming full relocation/replacement is required.
- **Activation Triggers:** Activation occurs for All-Hazards events as defined in AnonCo's Emergency Management Operations Plan, encompassing any natural or human-made emergency that impacts technology operations.
- **Scope of Plan Coverage:** This BCP covers the critical infrastructure systems at the Middletown (MDC) and Lyndhurst (LDC) Data Centers that support business and clinical applications:
    - **Power Systems**
    - **Environmental Controls Systems**
    - **Network Infrastructure Systems**
    - **Monitoring and Alerting Systems**
    - **Physical Security, Access, and Safety Systems**

Exclusions: This plan does not cover application recovery, end-user systems, and business process continuity. Theoretical impacts or risks are covered under separate business documents.

Operational Assumptions

- AnonCo Data Centers are
    - Maintained at high levels of readiness
    - Capable of activation with or without warning
    - Achieve operational status no later than 1-24 hours after activation
    - Can sustain operations for up to 30 days or until termination

Operational Targets

Availability Targets

- **Target Uptime**: 99.9% annually
- **Mean Time to Recovery (MTTR):** <4 hours for critical systems
- **Mean Time Between Failures (MTBF):** Tracked monthly

Environmental Targets

- **Temperature Compliance:** <95°F threshold
- **Humidity Range:** Within manufacturer specifications
- **Power Quality:** Voltage and frequency within tolerance

Facility Infrastructure

This section details the physical infrastructure including power systems (dual generators, UPS systems), environmental controls (HVAC, fire suppression), monitoring systems, and general network infrastructure for both data center locations.

Data Center Locations

Facility	MDC/ Mammoth Data Center
Location Address	490 Blue Hill Road, Middletown, NJ 07748
Facility	LDC/ Lemon Data Center
Location Address	1080 Safe Street West, 5th Floor, Lyndhurst, NJ 07071

Power Systems

- **MDC**
  - **Commercial Utility Power:** Dual 1500kVA transformers
  - **Backup Generation:** Two 3125kVA/2500kW parallel generators
  - **UPS Systems:**
    - Multiple UPS configurations
    - **Redundancy:** N+1 for critical systems with automatic transfer switches
    - **Fuel management and delivery coordination**
    - **Power Management Systems**
- **LDC**
  - **Commercial Utility Power:** Dual 1500kVA transformers
  - **Backup Generation:** Two 3125kVA/2500kW parallel generators
  - **UPS Systems:**
    - 2N A/B system with 750kVA/675kW modules
    - **Redundancy:** N+1 for critical systems with automatic transfer switches
    - **Fuel management and delivery coordination**
    - **Power Management Systems**

Environmental Controls Systems

- **HVAC Systems:** Comprehensive cooling with glycol loops and direct expansion units
- **Temperature Monitoring:** 95°F threshold with 5-minute alert delay
- **Fire Suppression:** Multi-zone systems
- **Raised Flooring:** 18" plenum for air distribution

Network Infrastructure Systems

The two datacenters in Middletown and Lyndhurst provide for redundant server/storage connections via multi-chassis spine-leaf architectures, minimizing single points of failure. The access layer at-large provides for high-throughput with redundant uplinks.

- **External Fiber Entry:**
  - **Physical Separation:** At both MDC and LDC, fiber enters the building at two geographically distinct points to ensure a single construction accident or localized disaster cannot sever all communications.
  - **Internal Redundancy:** In LDC, these 2 separate entry points for the dark fiber (Ciena) terminate on the fourth floor of the data center. The ISP's point of entry leads to one Meet-Me Room (MMR) on the first floor and is then routed to the fourth floor via internal risers. At MDC, the fibers come in and terminate in the Carrier Room. From there the connections are extended into the MDF area and then throughout the data center.

- **Data Center Interconnect and Inter-site links:**
  - MDC and LDC are linked via
    - 2x 40Gbps managed wavelength services from Lumen
    - 4x 100Gbps wavelength services through Ciena based AnonCo optical networks over dark fiber
  - **Geographic Route Diversity:** The primary and secondary fiber paths between datacenters follow completely different geographical routes. They do not share common bridges, tunnels, or utility conduits.
  - **Automated Failover:** Both fiber paths utilize DWDM technology for high-capacity transport. At the network layer, we employ BGP and ECMP to provide automated failover. In the event of a fiber cut or path degradation, traffic automatically reroutes to the secondary path with sub-second convergence time, maintaining synchronous data replication between sites. The Lumen and Ciena paths operate in an active-active configuration, providing combined capacity of 480 Gbps.

Monitoring and Alerting Systems

- **DC Facilities Team**: Siemens & ASCO systems for HVAC, fire suppression, UPS, batteries
- **Observability Team:** Swift Environmental system for temperature/humidity/fluid detection
- **Network Operations Center:** Hardware equipment monitoring

Physical Security, Access, and Safety Systems

Both datacenters employ the following:

- **Identity and Access Management (IDAM) systems**
  - The centralized frameworks and software used to verify a user's identity and determine their permission levels.
- **Building access controls and badging**
  - The physical hardware and protocols used to restrict entry to facilities, such as

RFID card readers, biometric scanners, and turnstiles.

- **Security monitoring and surveillance**
  - The use of CCTV cameras, motion sensors, and intrusion detection systems to maintain real-time visibility of a facility.
- **Emergency access procedures**
  - The pre-defined protocols that override standard security measures during a crisis, such as "fail-safe" locks that automatically open during a power outage. It should be noted that the Data Center fail-safe mode is doors locked.
- **Fire suppression procedures and systems**
  - The automated hardware designed to detect and extinguish fires, such as smoke detectors, water sprinklers, and clean agent gas systems for server rooms.

Service Levels

See Appendix E

This section details how the data center is structured to support the following maximum tolerable downtime thresholds, organized by system tier.

AnonCo Tier 2 Data Center

The existing AnonCo critical system infrastructure was originally designed as a Tier 2 facility with dual pathway components of a Tier 3 configuration. Tier 2 facilities cover redundant capacity components for power and cooling that provide better maintenance opportunities and safety against disruptions. These components include:

- Engine generators
- Energy storage
- Chillers
- Cooling units
- UPS modules
- Pumps
- Heat rejection equipment
- Fuel tanks
- Fuel cells

The distribution path of Tier 2 serves a critical environment, and the components can be removed without shutting it down. As such the infrastructure is set up to support the critical environments detailed below by System Tier.

By System Tier

See Appendix E

- **Tier 0 Prime (Foundational IT Core Services):** Critical IT Infrastructure *(Recovered with or prior to mission critical services)*
- **Tier 1 Prime (Mission Critical):** Mission clinical applications for supporting core healthcare operations *(Up to 4 hours)*
- **Tier 1 (Critical):** Critical business function that is life/safety or revenue impacting *(Up to 8 hours)*
- **Tier 2 (Moderately Critical):** Business applications, administrative systems *(Up to 24 hours)*

- **Tier 3 (Low Criticality):** Internal systems *(Up to 72 hours)*
- **Tier 4 (Non-Critical)**: Internal departmental systems, test *(Best effort basis)*

Response Procedures

See Appendix B for response procedures

Incident Protocol

Major incidents affecting datacenter operations are tracked and managed through AnonCo's System Incident Response (SIR) process. Incidents potentially meeting enterprise-level impact criteria are escalated through the Hospital Incident Command System (HICS) to coordinate organizational response actions.

Data Protection

- Automatic replication from Middletown to Lyndhurst
- All data files backed up regularly
- Continuous monitoring of replication status

Site Resilience

- **Primary-Secondary Configuration**: Geographic separation for disaster isolation
- **Independent Infrastructure:** Separate utility feeds and environmental systems
- **Redundancy:** N+1 for critical systems

Power Continuity

- N+1 redundancy for critical systems
- Automatic transfer switches (ATS) for seamless power transition
- Generator fuel management for extended outages

Response Teams

This section defines internal and external response team structure for managing disasters and emergencies.

Data Center Management

- **Director, Enterprise Technology Services (ETS) Hosting**
  - Provides executive decision making and strategic direction for response
  - Business liaison and SLT communications
- **Data Center Infrastructure Manager**
  - Directs restoration of core IT infrastructure at datacenter
- **Data Center Facilities Team**
  - Core technical team and support for datacenter activities
  - anonymized@example.com

Vendor List

See Appendix A

- Managed by Data Center Facilities team

Facilities Management

This section establishes regular testing cadence (monthly to annually), training, and maintenance windows.

Infrastructure Systems Testing

- **Monthly**
  - Power management testing and capacity verification
- **Quarterly**
  - UPS battery testing and capacity verification
  - HVAC Preventive Maintenance and system testing
- **Semiannual**
  - UPS Inspection
- **Annually**
  - Datacenter Tabletop exercise
  - BCP documentation review

Operations Training

See Appendix E

- Governed by AnonCo policy governing training and exercising.

Maintenance Windows

See Appendix E

- Coordinated through Change Advisory Board (CAB)

Appendices

Appendix A

Vendor Management

2023 LDC.MDC Emergency Contact.xls

Appendix B

Response Procedures

Data Center

- Data Center Alternative Operations
- Data Center Power Failure Response Procedures
  - UPS Failure
  - Emergency Generator Failure
- Fire Suppression Failure
- Precision Cooling Failure

IT

- Downtime Resources

Emergency Management

- Emergency Resources
- Utilities Emergency Response Guide
- Plumbing/ Flooding
- Communications Failure
- Evacuation Procedures
- Fatality Management

Appendix C

Emergency Processes

- AnonCo Emergency Management
- Incident Management Support
- HICS IMT
- AnonCo Emergency Management Contacts
- SIR Process Chart
- Fire Safety Manual

Appendix D

Risk Reports

Engineering Evaluation Study

- *AnonCo LDC Engineering Evaluation Study -10-5-2022 r3.pdf*
- *AnonCo MDC Engineering Evaluation Study - 9-15-2022 (final).pdf*

Audit Report

- *2025 IT New Jersey Data Centers Audit Report_Final.pdf*

Testing

- *Infrastructure Systems Testing Records*

Appendix E

AnonCo Governance

- Support Annexes and Documents for Emergency Operations Plans
- Business Continuity Program Management (ECSE-8002)
- Emergency Management (ECSE-8001)
- Mass Notification System (MNS) Policy
- Enterprise Command and Control (ECC)
- Training and Exercising (ECSE-8003)
- IT Technology and Recovery, Resilience
- Uptime Institute Tier Definitions
- Change Control Policy (IT-1001)

Compliance and Standards

Maps the plan to industry standards including NIST 800-53, ISO 22301, ANSI/TIA-942, and other regulatory requirements like HIPAA.

NIST 800-53 Controls

- **CP-1:** Contingency Planning Policy and Procedures
- **CP-2:** Contingency Plan development and maintenance
- **CP-4:** Contingency Plan Testing
- **CP-6:** Alternate Storage Site
- **CP-7:** Alternate Processing Site

ISO 22301 Requirements

- **Business Impact Analysis:** Documented and regularly updated
- **Risk Assessment:** Integrated with organizational risk management
- **Incident Response:** Structured approach with defined roles
- **Testing and Exercising**: Regular validation of plan effectiveness

Additional Standards

- **ANSI/TIA-942:** Telecommunications Infrastructure for Data Centers

- **Uptime Institute Tier Standards**
- **ISO 27001:** Information Security Management
- **SSAE 18** (SOC Reports)
- **HIPAA, GDPR** (where applicable)
- **New York SHIELD Act**
- **New Jersey Data Breach Statue Section 56:8-163**