Disaster Recovery* Plan

↘ Summary

The Disaster Recovery Plan at Machina exists to enable quick recovery of essential network services which will support ongoing business operations during system failures and cyberattacks and natural disasters and site outages. The plan establishes full network connectivity through WAN connections which maintains accurate data and continuous operations between all sites.

↘ Plan Overview

The Machina Disaster Recovery Plan establishes a systematic approach to recover network operations and data accessibility and business functionality when disruptions occur. The solution works for all sites that connect through WAN networks including headquarters and manufacturing facilities and warehouses and retail locations. The plan details response methods and recovery sequence and communication protocols for different disaster types including hardware breakdowns and cyber threats and electrical blackouts and natural catastrophes. The system protects Machina operations through complete security and continuous connectivity and operational resilience during all situations.

Goals	**Objectives**
Ensure Business Continuity	Maintain critical operations and connectivity during and after an outage or natural disaster.
Minimize Downtime	Restore essential WAN services within defined RTO (Recovery Time Objective) targets.
Protect Data Integrity	Prevent data loss through scheduled backups, replication, and secure cloud storage.
Establish Redundancy	Utilize the Dallas DR site as a secondary hub to support network failover and continuity.
Define Clear Procedures	Provide step-by-step recovery processes for IT staff to follow during incidents.
Assign Roles and Responsibilities	Clarify who leads, manages, and executes recovery tasks.
Regular Testing and Updates	Conduct periodic drills and updates to ensure readiness and effectiveness of the plan.

↘ Risks and Plans of Operations

The section reveals potential risks to Machina's WAN network infrastructure while demonstrating operational procedures to reduce service disruptions and achieve quick system recovery.

Risks	Description	Operations
Cyber Attack	Unauthorized access, ransomware, or data breach affecting network operations or ERP systems.	0–1 hour: The system needs to identify intrusions while it separates compromised systems from all other network components. 1–3 hours: The organization needs to start its incident response system while it blocks malicious IP addresses and brings back its firewall and access control systems. 3-6 hours: The system will perform a restoration from its last clean backup which contains both database information and system setup details during this time period. 6–12 hours: The network should return to normal operation through the DR site for WAN traffic while staff monitor for any remaining security threats.
Natural Disaster	Severe weather (flood, storm, fire) causes physical damage or power loss at HQ.	0–2 hours: Declare disaster; shift operations to DR site (Dallas). 2–4 hours: The system activates backup servers while DR routers redirect WAN traffic. 4-8 hours: The system will enable all remote branches to access ERP and POS functions during this time period.

		8–24 hours: The system needs complete validation of all its functions while verifying HQ backup data replication occurs.
Power Outage	Complete or partial power loss at primary or branch site	0–30 mins: The UPS backup system turns on while the IT team tracks the system status. 30-90 mins: The system will redirect traffic to the DR site for 30–90 minutes while power remains offline and backup DNS/DHCP systems become active. 1.5–3 hours: The team verified that all critical systems including ERP and database and authentication functions were operational through the DR link. 3–6 hours: The system will restore power to synchronize DR data with HQ servers.
Hardware Breakdown	Router, switch, or server failure disrupting connectivity or operations.	0–1 hour: The NOC alerts and logs help identify which component failed. 1–3 hours: The system performs backup hardware operations and virtual device configuration changes to execute operation rerouting and replacement. 3–6 hours: Restore configurations from stored router/switch backups.

		6–12 hours: The system needs to perform a full connectivity test to enable default network routes.

Recovery Strategy Section

Machina’s Disaster Recovery Strategy operates network operations through continuous data protection which protects all operational sites from extended system disruptions. The section of the document defines Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical systems which determine how fast services can be restored and what amount of data loss is acceptable during system failures.

Recovery Objectives Table (RTO / RPO)

System / Function	RTO (Max Downtime)	RPO (Max Data Loss)	Priority
ERP / Supply Chain System	4 hours	1 hour	High
Point-of-Sale (POS) Systems	2 hours	30 minutes	High
Email & Collaboration	8 hours	2 hours	Medium
DNS / DHCP / Authentication	1 hour	15 minutes	**Critical**
Web & E-Commerce Services	6 hours	2 hours	High
Design File Storage	6 hours	2 hours	Medium

↘ Testing & Maintenance

To ensure the continued effectiveness of Machina's Disaster Recovery Plan, regular testing and maintenance activities are performed across all network sites. These activities confirm that recovery procedures work reliably and data remains intact while staff members demonstrate readiness. The system achieves continuous improvement through regular review sessions and simulation tests and system audit procedures.

Testing Procedures

- **Quarterly Recovery Drills:**
  The organization runs simulated disaster recovery exercises four times per year to verify system failover operations and data restoration procedures and network communication systems. Results are documented and reviewed by IT management to identify any gaps or delays.

- **Semi-Annual Network Failover Tests:**
  The system performs tests on SD-WAN and routing configurations to verify their ability to automatically switch between HQ and the Dallas DR site in case of failure. The tests show how long it takes for route convergence and how fast VPN tunnels recover from failures and evaluate

network bandwidth performance under heavy traffic conditions.

- **Annual Full-System Test:**
  The recovery test includes all necessary components which run once annually to verify backup restoration and user authentication and ERP system recovery and application performance.

Maintenance Activities

- **Plan Review and Updates:**
  The DR Plan undergoes semi-annual reviews to verify its current alignment with system configurations and vendor data and organizational guidelines while major network infrastructure updates occur.

- **Backup Validation:**
  Weekly verification process checks backup files for completeness and corruption while confirming their ability to restore data. The system checks Cloud and offsite storage logs for accuracy to ensure they meet all required retention standards.

- **Hardware and Software Patching:**
  Network devices, servers, and security appliances are patched regularly to prevent vulnerabilities that could impact recovery operations.

- **Staff Training:**
  All IT personnel receive DR awareness training and participate in at least one recovery simulation per year to maintain familiarity with roles and escalation procedures.

↘ Success Criteria

Success Criteria & Performance Metrics

The Disaster Recovery Plan of Machina undergoes evaluation through performance metrics and post-incident assessment procedures. The established criteria help recovery processes meet operational needs by minimizing system downtime and protecting data precision. Success Criteria

Success Criteria

- **Recovery Time Objective (RTO) Met:**
  The defined RTO thresholds for ERP POS and authentication services have been met through the restoration of all critical systems.

- **Recovery Point Objective (RPO) Met:**
  The data retrieval process from backup systems stays within the established RPO limits which

define the maximum amount of data that can be lost.

- **Business Continuity Maintained:**
  Core essential network operations, communication systems, and user access remain functional throughout recovery events.

- **Zero Data Corruption:**
  There's no corrupted or lost data is identified during restoration or synchronization between HQ and DR sites.

- **System Reliability:**
  All of the network services resume normal performance levels without packet loss, latency, or configuration drift after recovery.

Performance Metrics

Metric	Target	Frequency of Review
WAN Failover Time	< 5 minutes	Quarterly
ERP System Recovery Time	< 4 hours	Quarterly
Backup Success Rate	100% verified backups	Weekly
DR Drill Completion	100% participation	Quarterly
Data Restoration Accuracy	99.9%	Monthly
Incident Resolution Time	≤ 24 hours	As Occurred

Evaluation and Reporting

The team creates a complete **After-Action Report (AAR)** for every DR test and actual incident to assess system performance and staff reaction and DR Plan execution. The research team documents their results before showing them to Executive Leadership for policy modification and resource distribution and development of enhanced disaster recovery systems.

Roles & Responsibilities

This section defines the key personnel and their responsibilities during disaster recovery operations. The recovery process depends on these roles to maintain coordinated response and fast service restoration and secure communication systems.

Roles	Responsibility
IT Manager	Declare disaster, oversee recovery, communicate with executives.
Network Engineers	Restore WAN connectivity and routing.
Server Administrators	Activate and sync DR systems (ERP, DNS, authentication).
Security Officer	Ensure data integrity and enforce access policies.
Executive Leadership	Approve DR actions and manage external communications.

↘ Communication Plan

Purpose

The communication plan ensures that all stakeholders are informed, coordinated, and updated during each phase of the disaster recovery process from incident detection to full restoration.

Communication Objectives

- Maintain clear, real-time communication between technical teams and leadership.
- Provide consistent updates to employees, clients, and partners.
- Ensure accurate documentation of all actions and recovery milestones.

Key Contacts

Role	Responsibility	Primary Contact Method
IT Manager	Declares disaster, leads recovery coordination	Phone, Email, Teams
Network Engineers	Report network and connectivity status	Slack/Teams, Incident Log
Server Administrators	Report system, DNS, ERP, and backup status	Email, System Dashboard
Security Officer	Reports on breaches or threats	Secure Messaging
Executive Leadership	Approves external statements, client communication	Email, Phone

Communication Channels

- **Internal:** Microsoft Teams, Slack, and internal email groups
- **External:** Customer email notices, website status page, vendor contact lines
- **Backup Channel:** SMS alerts or phone tree if network is unavailable

Reporting Frequency

Phase	Frequency	Description
Incident Detection	Immediate	IT Manager notifies all stakeholders of the event.
Active Recovery	Every 2 hours	Progress updates shared via Teams and logs.
System Validation	Upon completion	Confirm systems restored and data integrity verified.
Post-Recovery Review	Within 24-48 hours	Send final incident report and improvement actions.

↘ Budget & Resource Allocation

Estimated DR Budget Breakdown

Category	Description	Estimated Annual Cost (USD)
Hardware & Infrastructure	Redundant routers, switches, UPS units, and backup servers at the Dallas DR site.	$18,000
Software & Licensing	Backup management software, cloud storage licenses, SD-WAN, and security suite renewals.	$9,500
Cloud & Offsite Backup	Monthly encrypted data replication to AWS/Azure for ERP, POS, and authentication systems.	$7,200
Testing & Drills	Quarterly DR drills, simulations, and maintenance of test environments.	$3,000
Personnel & Training	IT staff training, certification renewals, and cross-site coordination expenses.	$5,000
Power & Environmental Systems	Generator fuel, UPS battery maintenance, and climate control for DR equipment.	$2,800
Contingency Fund (10%)	Reserved for unplanned hardware failure or emergency vendor services.	$4,500

Total Estimated Annual DRP Budget ~ $50,000

Resource Allocation

- **Primary Responsibility:** IT Manager and Network Engineers oversee DR infrastructure, testing, and vendor coordination.

- **Backup Operations Site:** Dallas DR facility acts as the recovery hub for all WAN services.

- **Vendor Partnerships:** Cisco, AWS, and Microsoft Azure provide network hardware, backup, and cloud services.

- **Training Cadence:** Bi-annual internal DR workshops and one external certification opportunity per staff member.

Budget Review Cycle

The DRP budget receives annual review during Q4 through collaboration between Machina's Finance and IT departments adjustments are made based on:

- New site expansions or hardware refresh cycles.
- Shifts in vendor pricing or licensing terms.
- Post-incident cost analysis or recovery audit findings.

Machina Network Infrastructure Budget Estimate

Category	Item Description	Quantity	Estimated Unit Cost (USD)	Total (USD)
Routers	Cisco 2911/4331 Series (Core + Branch Routers)	6	$1,200	**$7,200**
Switches	Cisco 2960/2975 Series 24-Port Gigabit	8	$900	**$7,200**
Servers	Dell PowerEdge R740 (Corporate + Backup)	2	$4,000	**$8,000**
Laptops / PCs	Department Workstations (Design, Sales, Mfg, Marketing, Supply)	12	$800	**$9,600**
Rack Equipment	Network rack, patch panels, cable management	1	$1,500	**$1,500**
Power Systems	UPS + Power Distribution Units (2)	2	$1,200	**$2,400**
Cabling & Accessories	Ethernet, fiber, labeling, connectors	Bulk	—	**$1,500**
Backup Storage	NAS / Cloud backup system	1	$2,000	**$2,000**
Licenses & Config Tools	Packet Tracer, Cisco SmartNet, management software	Bundle	—	**$1,800**
Contingency (10%)	Unexpected hardware or replacements	—	—	**$4,020**

↘ Contact Information

For any inquiries on this project, reach out to:

Aaron Foster
Project Manager