BRANDON & CLARK

DISASTER RECOVERY PLAN

Version 1.0 | [07/22/2025]

TABLE OF CONTENTS

1. Executive Summary
2. System Inventory and Criticality Assessment
3. Recovery Objectives (RTO/RPO)
4. SpringPoint ERP Recovery Procedures
5. Active Directory Recovery Procedures
6. File Server Recovery Procedures
7. SQL Server/IIS Recovery Procedures
8. Network Infrastructure Recovery
9. Communication Procedures
10. Testing and Maintenance
11. Vendor Contact Information
12. Recovery Team Roles and Responsibilities
13. Step-by-Step Recovery Procedures
14. Post-Recovery Verification
15. Appendices

1. EXECUTIVE SUMMARY

PURPOSE:
This Disaster Recovery Plan provides detailed procedures for recovering Brandon & Clark's critical IT systems and data in the event of a disaster that impacts the primary office location or technology infrastructure.

SCOPE:
This plan covers all critical business systems, including SpringPoint ERP, Active Directory, file servers, and supporting infrastructure necessary to maintain business operations.

ACTIVATION CRITERIA:
Primary office building inaccessible
Critical system failure affecting business operations
Network infrastructure failure
Cybersecurity incident affecting multiple systems
Natural disaster impacting facilities

RECOVERY STRATEGY:
Brandon & Clark's disaster recovery strategy leverages cloud-hosted SpringPoint

ERP, off-site Active Directory replica, and cloud backup services to ensure rapid recovery of critical business functions.

2. SYSTEM INVENTORY AND CRITICALITY ASSESSMENT

2.1 Critical Systems Overview

System	Function	Criticality	Hosting Location	Recovery Method	RTO Target	RPO Target
SpringPoint ERP	CRM, Job Tracking, Invoicing, Purchasing, Quoting, Inventory, Accounting, Finance, Operations	CRITICAL	AWS Cloud	SpringPoint DR procedures	[2 hours]	[15 minutes]
Active Directory	User authentication and access control	CRITICAL	Primary office + Off-site replica	Failover to replica DC	[1 hour]	[15 minutes]
File Server	AutoCAD files, pre-2023 job images, engineering documents	HIGH	Primary office	Restore from Cove cloud backup	[8 hours]	[24 hours]
SQL Server 2022/IIS	Legacy data, non-business critical applications	MEDIUM	Primary office	Restore from backup	[48 hours]	[24 hours]

2.2 System Dependencies

Primary System	Dependencies	Impact of Dependency Failure	Workaround Available
SpringPoint ERP	Internet connectivity, DNS, user authentication	Complete business system unavailable	Mobile hotspot, alternate internet
Active Directory	Network connectivity, DNS	User login failures, file access issues	Local user accounts, cached credentials
File Server	Active Directory, network connectivity	Engineering file access unavailable	Local file copies, cloud access

3. RECOVERY OBJECTIVES (RTO/RPO)

3.1 Business Impact Analysis

Business Function	Supporting System	Maximum Tolerable Downtime	Financial Impact per Hour	Recovery Priority
Customer Service/Dispatch	SpringPoint ERP	2 hours	[$ amount]	1 - Critical
Field Service Management	SpringPoint ERP	2 hours	[$ amount]	1 - Critical
Invoicing/Accounting	SpringPoint ERP	4 hours	[$ amount]	1 - Critical
Engineering Design	File Server, AutoCAD	8 hours	[$ amount]	2 - High

Historical Data Access	SQL Server/Legacy systems	48 hours	[$ amount]	3 - Medium

3.2 Recovery Time and Point Objectives

CRITICAL SYSTEMS (RTO 2 hours):
SpringPoint ERP: 2 hours RTO, 15 minutes RPO
Active Directory: 1 hour RTO, 15 minutes RPO
Internet connectivity: 30 minutes RTO

HIGH PRIORITY SYSTEMS (RTO 8 hours):
File Server: 8 hours RTO, 24 hours RPO
Engineering workstations: 4 hours RTO
Email systems: 2 hours RTO

MEDIUM PRIORITY SYSTEMS (RTO 48 hours):
SQL Server/IIS: 48 hours RTO, 24 hours RPO
Legacy applications: 48 hours RTO
Non-critical workstations: 24 hours RTO

4. SPRINGPOINT ERP RECOVERY PROCEDURES

4.1 SpringPoint System Overview

SYSTEM DETAILS:
Hosting: AWS Cloud Infrastructure
Access Methods: Web browser, RDP
Business Functions: CRM, Job Tracking, Invoicing, Purchasing, Quoting, Inventory, Accounting, Finance, Operations
Vendor: SpringPoint Solutions
Service Level Agreement: [Service Level Agreement details]
DR/BCP: Provided by SpringPoint Solutions

DEPENDENCIES:
Internet connectivity
DNS resolution
User authentication
Compatible web browsers/RDP clients

4.2 SpringPoint Recovery Procedures

SCENARIO 1: SpringPoint Service Outage

IMMEDIATE ACTIONS (0-30 minutes):
1. Verify outage scope (all users affected vs. isolated).
2. Check SpringPoint status page: [URL].
3. Test internet connectivity from multiple locations.
4. Contact SpringPoint support: [Emergency phone number].
5. Notify management and affected departments.
6. Activate manual processes for critical functions.

WORKAROUND PROCEDURES (30 minutes - 2 hours):
1. Switch to mobile data/alternate internet connection.
Implement paper-based job tracking forms
2. Use manual dispatch procedures.
3. Route customer calls to field supervisors.
4. Postpone non-critical invoicing and purchasing.
5. Document all manual activities for later entry.

ESCALATION PROCEDURES:
1. After 1 hour: Contact SpringPoint account manager.
2. After 2 hours: Escalate to SpringPoint management.
3. After 4 hours: Activate extended manual procedures.
4. After 8 hours: Consider alternate software solutions.

4.3 SpringPoint DR Activation

SPRINGPOINT DISASTER RECOVERY ACTIVATION:

According to SpringPoint's DR/BCP documentation:
1. Contact SpringPoint Emergency Support: [Phone number].
2. Reference Brandon & Clark account: [Account number].
3. Request Disaster Recovery (DC) site activation.
4. SpringPoint RTO commitment: [Time from their BCP].
5. SpringPoint RPO commitment: [Data loss timeframe].

B&C RESPONSIBILITIES DURING SPRINGPOINT DR:
1. Provide alternative internet connection if needed.
2. Coordinate user communications.
3. Test system functionality upon restoration.
4. Document any data loss or system issues.
5. Verify all integrations are working properly.

5. ACTIVE DIRECTORY RECOVERY PROCEDURES

5.1 Active Directory Infrastructure

CONFIGURATION:
1. Primary Domain Controller: [Server name/IP at main office]
2. Secondary Domain Controller: [Server name/IP at off-site location]
3. Domain Name: [domain.local]
4. Replication Schedule: [Replication frequency]
5. Off-site Location: [2 miles from main office]

FSMO ROLES DISTRIBUTION:
1. Schema Master: [Primary/Secondary DC]
2. Domain Naming Master: [Primary/Secondary DC]
3. PDC Emulator: [Primary/Secondary DC]
4. Infrastructure Master: [Primary/Secondary DC]
5. RID Master: [Primary/Secondary DC]

5.2 Active Directory Failure Scenarios

Failure Scenario	Impact	Recovery Procedure	Estimated Recovery Time
Primary DC Failure	Authentication issues, policy updates unavailable	Promote secondary DC, transfer FSMO roles	30 minutes
Secondary DC Failure	No AD redundancy	Rebuild secondary DC, restore from backup	4 hours
Both DCs Failed	Complete authentication failure	Restore from system state backup	8 hours
Network Connectivity Loss	Replication failure	Restore network, verify replication	2 hours

5.3 Active Directory Recovery Procedure

PRIMARY DC FAILURE RECOVERY:

STEP 1: Assess Failure (0-15 minutes)
1. Verify primary DC is truly offline.
2. Check network connectivity to primary site.
3. Test authentication from secondary DC.
4. Document failure symptoms and time.

STEP 2: Activate Secondary DC (15-30 minutes)
1. Log into secondary DC at off-site location.
2. Verify AD services are running.
3. Check replication status and last sync time.
4. Transfer FSMO roles to secondary DC:

```
netdom query fsmo Move roles using Active Directory Users
and Computers or PowerShell: Move-
ADDirectoryServerOperationMasterRole
```

STEP 3: Update Infrastructure (30-60 minutes)
1. Update DNS to point to secondary DC.
2. Update DHCP to reference new DC.
3. Modify firewall rules if necessary.
4. Test user authentication.
5. Verify group policy application.
6. Test file server access.

STEP 4: Notify Users and Monitor
1. Send notification that AD services are restored.
2. Monitor for authentication issues.
3. Plan primary DC rebuilding/replacement.

6. FILE SERVER RECOVERY PROCEDURES

6.1 File Server Configuration

SERVER DETAILS:
Server Name: [File server name]
Location: Primary office
Operating System: [Windows Server version]
Storage Capacity: [Total TB]
File Types: AutoCAD files, pre-2023 job images, engineering documents

BACKUP CONFIGURATION:
Local Backup: Synology NAS drives
Cloud Backup: Cove Backup service
Backup Frequency: [Daily/Hourly]
Retention Period: [Days/Months]
Test Restore Frequency: [Monthly/Quarterly]

6.2 File Server Recovery Scenarios

Scenario	Recovery Method	Recovery Source	Estimated Time	Data Loss
Hardware Failure	Restore to new hardware	Cove cloud backup	8-12 hours	Last backup (24 hours max)
Corrupted Files	Selective file restore	Synology local backup	2-4 hours	Last backup point
Ransomware Attack	Full system restore	Clean Cove backup	12-24 hours	To clean backup point
Building Inaccessible	Restore to alternate location	Cove cloud backup	6-8 hours	Last backup (24 hours max)

6.3 File Server Recovery Procedure

COMPLETE FILE SERVER RECOVERY:

PHASE 1: Assessment and Preparation (0-2 hours)
1. Assess extent of file server failure.
2. Determine recovery location (primary office or alternate).
3. Procure replacement hardware if needed.
4. Contact Cove support for restore assistance.
5. Prepare recovery environment.

PHASE 2: System Recovery (2-6 hours)
1. Install base operating system on replacement hardware.
2. Install Cove backup client.
3. Configure network connectivity.
4. Join server to Active Directory domain.
5. Configure appropriate security permissions.

PHASE 3: Data Restoration (6-12 hours)
1. Initiate full restore from Cove cloud backup.

```
Priority Order: 1. AutoCAD files (engineering department)
2. Recent project folders 3. Historical job images 4.
Administrative documents 5. Other files
```

2. Monitor restore progress.
3. Verify file integrity during restore.
4. Document any restoration issues.

PHASE 4: Verification and Testing (12-14 hours)
1. Verify all critical files are restored.
2. Test file share access from workstations.
3. Confirm AutoCAD can open engineering files.
4. Verify user permissions are correct.
5. Test backup system functionality.
6. Update DNS records if server name changed.

COVE BACKUP CONTACTS:
Support Phone: [Cove support number]
Account Manager: [Name and contact]
Account Number: [Account reference]
Emergency Escalation: [Emergency contact]

7. SQL SERVER/IIS RECOVERY PROCEDURES

7.1 SQL Server/IIS Configuration

SYSTEM SPECIFICATIONS:
SQL Server Version: Microsoft SQL Server 2022
IIS Version: [IIS version]
Server Location: Primary office
Primary Function: Legacy data hosting, non-business critical applications
Recovery Time Objective: 48 hours (non-critical)
Recovery Point Objective: 24 hours

BACKUP CONFIGURATION:
Database Backup: [Daily/Weekly full, hourly differential]
Transaction Log Backup: [Every 15 minutes]
IIS Configuration Backup: [Weekly]
Backup Location: [Local NAS and cloud]

7.2 SQL Server Recovery Procedure

SQL SERVER 2022 RECOVERY (RTO: 48 hours):

PHASE 1: Hardware and OS Preparation (0-8 hours)
1. Install/configure replacement server hardware
2. Install Windows Server operating system
3. Install SQL Server 2022 (same edition and version)
4. Install IIS with required features
5. Apply necessary Windows and SQL updates
6. Join server to Active Directory domain

PHASE 2: SQL Server Configuration (8-16 hours)
1. Configure SQL Server services and accounts.
2. Restore master database from backup.
3. Restore MSDB database (contains backup history).
4. Restore model database.
5. Configure SQL Server security and permissions.

PHASE 3: Database Restoration (16-32 hours)
1. Restore all user databases from most recent backups.
2. Apply differential backups if available.
3. Apply transaction log backups to minimize data loss.
4. Verify database consistency (DBCC CHECKDB).
5. Update database statistics.

PHASE 4: IIS and Application Recovery (32-48 hours)
1. Restore IIS configuration from backup.
2. Restore web application files.
3. Configure application pools and websites.
4. Test database connectivity from web applications.
5. Verify SSL certificates are properly configured.
6. Test all legacy applications' functionality.

8. NETWORK INFRASTRUCTURE RECOVERY

8.1 Network Infrastructure Overview

Component	Primary	Backup/Redundancy	Recovery Method	RTO
Internet Connection	[Primary ISP/Speed]	[Secondary ISP/Speed]	Automatic failover	5 minutes
Firewall	[Primary firewall model]	[Backup firewall]	Configuration restore	2 hours
Core Switch	[Switch model/location]	[Backup switch]	Hardware replacement	4 hours

Wireless Network	[WiFi infrastructure]	[Backup APs]	Controller restore	2 hours

8.2 Network Recovery Priorities

RECOVERY PRIORITY ORDER:

PRIORITY 1 - Internet Connectivity (0-30 minutes):
Verify primary internet connection.
Activate secondary ISP if needed.
Configure basic routing.
Test SpringPoint ERP access.

PRIORITY 2 - Internal Network (30 minutes - 2 hours):
Restore core switching infrastructure.
Configure VLANs and basic routing.
Restore Active Directory connectivity.
Test internal file server access.

PRIORITY 3 - Wireless Network (2-4 hours):
Restore wireless controllers.
Configure access points.
Test mobile device connectivity.
Verify guest network isolation.

PRIORITY 4 - Advanced Services (4-8 hours):
Restore VPN connectivity.
Configure network monitoring.
Implement security policies.
Test all network services.

9. COMMUNICATION PROCEDURES

9.1 Disaster Declaration and Notification

DISASTER DECLARATION AUTHORITY:
Primary: [Senior Partner Name/Title]
Alternate: [Operations Manager Name/Title]
Emergency: Any member of Crisis Management Team

NOTIFICATION SEQUENCE (within 1 hour of disaster declaration):
1. Crisis Management Team
2. All employees
3. Key customers and clients
4. Critical vendors and suppliers

5. Insurance carrier
6. SpringPoint support
7. Other stakeholders as needed

9.2 Communication Templates

INITIAL NOTIFICATION TEMPLATE:

Subject: URGENT - Brandon & Clark System Outage Notification

Dear [Recipient],

Brandon & Clark is currently experiencing [brief description of outage]. We are working to restore full operations as quickly as possible.

Current Status:
1. Estimated restoration time: [time estimate]
2. Alternative contact method: [phone/email]
3. Services affected: [list affected services]
4. Services still available: [list available services]

We will provide updates every [frequency] until full service is restored.

For urgent matters, please contact: [emergency contact information].

Thank you for your patience.

Brandon & Clark Management Team
[Contact information]

9.3 Communication Channels

Communication Method	Primary Use	Backup Method	Contact Information
Email	Formal notifications, updates	Personal email accounts	[Backup email addresses]
Phone/SMS	Immediate notifications	Personal cell phones	[Emergency contact list]

Company Website	Public status updates	Social media accounts	[Website/social media accounts]
Radio/Walkie-Talkie	Field team coordination	Cell phone calls	[Radio frequencies]

10. TESTING AND MAINTENANCE

10.1 Regular Testing Schedule

Test Type	Frequency	Scope	Success Criteria	Responsible Party
SpringPoint Access Test	Monthly	Verify ERP accessibility from multiple locations	100% access success	[IT Manager]
Active Directory Failover	Quarterly	Test secondary DC promotion	Seamless authentication	[IT Manager]
File Restore Test	Monthly	Restore sample files from Cove Backup	Complete file recovery	[IT Manager]
Communication Test	Quarterly	Test all communication channels	All channels functional	[Crisis Manager]
Full DR Exercise	Annually	Simulate complete disaster scenario	Meet all RTO/RPO targets	[Senior Management]

10.2 Plan Maintenance

PLAN REVIEW SCHEDULE:
1. Monthly: Contact information updates
2. Quarterly: Procedure verification and testing results
3. Semi-annually: Technology inventory and dependencies
4. Annually: Complete plan review and update

TRIGGERS FOR PLAN UPDATES:
1. System configuration changes
2. Vendor changes or new service providers
3. Organizational changes
4. Test failures or identified gaps
5. Actual disaster recovery events
6. Regulatory or compliance changes

PLAN DISTRIBUTION:
1. Crisis Management Team (complete plan)
2. Department managers (relevant sections)
3. IT team (technical procedures)
4. Key vendors (contact information updates)
5. Offsite storage (backup copies)

11. VENDOR CONTACT INFORMATION

11.1 Critical Vendor Contacts

Vendor	Service	Emergency Contact	Account Information	SLA Details
SpringPoint Solutions	ERP System	[24/7 Emergency Phone]	[Account # and Manager]	[RTO/RPO commitments]
Cove Backup	Cloud Backup Services	[Support Phone]	[Account # and Rep]	[Restore time commitments]
[Primary ISP]	Internet Connectivity	[Emergency Phone]	[Account # and Rep]	[Repair time commitments]

[Secondary ISP]	Backup Internet	[Support Phone]	[Account # and Rep]	[Activation procedures]
[IT Support Vendor]	IT Infrastructure Support	[Emergency Phone]	[Contract # and Manager]	[Response time commitments]

12. RECOVERY TEAM ROLES AND RESPONSIBILITIES

12.1 Crisis Management Team Structure

Role	Primary Person	Backup Person	Key Responsibilities
Crisis Manager	[Name/Contact]	[Name/Contact]	Overall disaster response coordination, communications, and decision making
IT Recovery Manager	[Name/Contact]	[Name/Contact]	Technical recovery coordination, vendor management, system restoration
Operations Manager	[Name/Contact]	[Name/Contact]	Business continuity, customer communications, field operations
Communications Coordinator	[Name/Contact]	[Name/Contact]	Employee notifications, customer updates, media relations
Finance/Admin Manager	[Name/Contact]	[Name/Contact]	Financial impact assessment, insurance claims, procurement

12.2 Recovery Team Activation

TEAM ACTIVATION PROCEDURE:
1. Crisis Manager declares disaster and activates plan
2. IT Recovery Manager assesses technical impacts
3. Operations Manager evaluates business impact
4. Communications Coordinator initiates notifications
5. Finance/Admin Manager coordinates financial aspects

TEAM COORDINATION:
1. Initial meeting: Within 30 minutes of activation
2. Status meetings: Every 2 hours during active recovery
3. Communication method: [Conference call/Teams meeting]
4. Documentation: All decisions and actions logged
5. Escalation: Senior management involved for major decisions

13. STEP-BY-STEP RECOVERY PROCEDURES

13.1 Complete Disaster Recovery Workflow

DISASTER RECOVERY ACTIVATION CHECKLIST:

IMMEDIATE RESPONSE (0-1 hour):
1. Assess scope and impact of disaster.
2. Ensure personnel safety.
3. Activate crisis management team.
4. Declare disaster and activate DR plan.
5. Notify key stakeholders.
6. Establish emergency communication.
7. Assess alternate facility needs.
8. Contact critical vendors.

CRITICAL SYSTEMS RECOVERY (1-4 hours):
1. Verify SpringPoint ERP accessibility.
2. Test alternate internet connections.
3. Activate secondary Active Directory.
4. Establish temporary user workstations.
5. Restore essential network connectivity.
6. Implement manual workarounds.
7. Coordinate with SpringPoint for DR activation.
8. Update customers on service status.

FULL RECOVERY PHASE (4-48 hours):
1. Complete SpringPoint ERP restoration.
2. Restore file server from Cove backup.
3. Rebuild Active Directory infrastructure.
4. Restore SQL Server/IIS systems.
5. Reinstall user workstations.

6. Verify all system integrations.
7. Test all business processes.
8. Return to normal operations.

13.2 Recovery Sequence Priority

RECOVERY PRIORITY MATRIX:

PHASE 1 - IMMEDIATE (0-2 hours):
1. Personnel safety and accountability
2. Emergency communications
3. SpringPoint ERP access verification
4. Basic internet connectivity
5. Active Directory failover

PHASE 2 - CRITICAL (2-8 hours):
1. Complete SpringPoint ERP restoration
2. File server recovery initiation
3. Network infrastructure rebuild
4. Essential workstation deployment
5. Customer service restoration

PHASE 3 - FULL RECOVERY (8-48 hours):
1. Complete file server restoration
2. SQL Server/IIS recovery
3. All workstation replacement
4. Full network services
5. Legacy system restoration

PHASE 4 - OPTIMIZATION (48+ hours):
1. Performance optimization
2. Security hardening
3. Documentation updates
4. Lessons learned review
5. Normal operations resumption

14. POST-RECOVERY VERIFICATION

14.1 System Verification Checklist

SPRINGPOINT ERP VERIFICATION:
1. All users can access system via web browser
2. RDP access functional for power users
3. All modules operational (CRM, Job Tracking, Invoicing, etc.)
4. Data integrity verified (recent transactions present)
5. Integrations working properly
6. Reports generating correctly

7. Performance meets normal standards

ACTIVE DIRECTORY VERIFICATION:
1. All users can authenticate
2. Group policies applying correctly
3. File server access permissions working
4. Email access functional
5. Network drive mappings correct
6. Replication between DCs operational

FILE SERVER VERIFICATION:
1. All critical files restored
2. AutoCAD files accessible and functional
3. Historical job images viewable
4. Engineering documents accessible
5. File permissions correct
6. Backup system operational

NETWORK VERIFICATION:
1. Internet connectivity functional
2. Internal network communication working
3. Wireless network operational
4. VPN access available
5. Network security measures active
6. Monitoring and ensuring that systems are operational

14.2 Business Process Verification

BUSINESS FUNCTION TESTING:

CUSTOMER SERVICE OPERATIONS:
1. Incoming call routing functional
2. Customer database accessible
3. Work order creation working
4. Dispatch system operational
5. Field technician communication

FIELD SERVICE OPERATIONS:
1. Job tracking system accessible
2. Mobile device connectivity
3. Parts inventory lookup
4. Time tracking functional
5. Photo upload capability

ADMINISTRATIVE FUNCTIONS:
1. Invoicing system working
2. Purchase order processing
3. Financial reporting accessible
4. Payroll system functional
5. Email system operational

ENGINEERING OPERATIONS:
1. AutoCAD software operational
2. Engineering files accessible
3. CAD file sharing working
4. Project folder access
5. Drawing revision control

PERFORMANCE BENCHMARKS:
1. System response times within normal range
2. File access speeds acceptable
3. Network throughput adequate
4. User productivity levels restored
5. Customer service levels maintained

15. LESSONS LEARNED AND IMPROVEMENT

15.1 Post-Recovery Review Process

REVIEW TIMELINE:
1. Immediate hot wash: Within 24 hours of recovery
2. Detailed analysis: Within 1 week of recovery
3. Final report: Within 2 weeks of recovery
4. Plan updates: Within 1 month of recovery

REVIEW PARTICIPANTS:
1. Crisis Management Team
2. IT Recovery Team
3. Department managers
4. Key vendors (SpringPoint, Cove, etc.)
5. End users' representatives
6. Senior management

EVALUATION CRITERIA:
1. RTO/RPO performance vs. targets
2. Communication effectiveness
3. Vendor response performance
4. Team coordination efficiency
5. Cost impact analysis
6. Customer satisfaction impact
7. Identified improvement opportunities

15.2 Continuous Improvement Framework

IMPROVEMENT AREAS:
1. Technology redundancy and resilience
2. Recovery procedure optimization

3. Staff training and preparedness
4. Vendor relationship management
5. Communication process enhancement
6. Testing and validation procedures

ANNUAL REVIEW REQUIREMENTS:
1. Complete technology inventory update
2. Vendor contract and SLA review
3. RTO/RPO target reassessment
4. Budget allocation review
5. Training program evaluation
6. Insurance coverage assessment
7. Regulatory compliance verification
8. Plan distribution and access review

APPENDIX A: EMERGENCY CONTACT INFORMATION

A.1 Internal Emergency Contacts

Name	Title	Primary Phone	Secondary Phone	Email	Role in DR
[Name]	Senior Partner	[Phone]	[Cell]	[Email]	Crisis Manager
[Name]	IT Manager	[Phone]	[Cell]	[Email]	IT Recovery Manager
[Name]	Operations Manager	[Phone]	[Cell]	[Email]	Operations Manager
[Name]	Service Manager	[Phone]	[Cell]	[Email]	Field Operations
[Name]	Office Manager	[Phone]	[Cell]	[Email]	Communications

A.2 External Emergency Contacts

Organization	Contact Person	Service	Phone	Email	Account Info
SpringPoint Solutions	[Account Manager]	ERP System Support	[Emergency Phone]	[Email]	[Account #]
Cove Backup	[Support Rep]	Cloud Backup Services	[Support Phone]	[Email]	[Account #]
[IT Support Company]	[Technical Lead]	IT Infrastructure	[Emergency Phone]	[Email]	[Contract #]
[Insurance Carrier]	[Agent Name]	Business Insurance	[Phone]	[Email]	[Policy #]

APPENDIX B: TECHNICAL SPECIFICATIONS

B.1 System Configuration Details

SPRINGPOINT ERP:
1. Cloud Provider: Amazon Web Services (AWS)
2. Access Methods: HTTPS web portal, RDP connection
3. URL: [SpringPoint access URL]
4. RDP Server: [RDP server address]
5. User Licenses: [Number of licenses]
6. Modules: CRM, Job Tracking, Invoicing, Purchasing, Quoting, Inventory, Accounting, Finance, Operations

ACTIVE DIRECTORY:
1. Domain: [domain.local]
2. Primary DC: [Server name/IP address]
3. Secondary DC: [Server name/IP address]
4. Forest/Domain Functional Level: [Level]
5. User Count: [Number of users]
6. Computer Count: [Number of computers]

FILE SERVER:
1. Server OS: [Windows Server version]
2. Storage: [Total capacity/Configuration]
3. Share Names: [List of shared folders]

4. File Types: AutoCAD files (.dwg), images (.jpg, .png), documents (.pdf, .doc)
5. Backup Schedule: [Frequency and retention]

SQL SERVER:
1. Version: Microsoft SQL Server 2022
2. Edition: [Standard/Enterprise]
3. Instance Name: [Default/Named instance]
4. Database Count: [Number of databases]
5. Size: [Total database size]
6. Applications: [List of applications using SQL]

APPENDIX C: RECOVERY CHECKLISTS

C.1 Quick Reference Recovery Checklist

DISASTER RECOVERY QUICK CHECKLIST:

IMMEDIATE ACTIONS (0-30 minutes):
1. Ensure personnel safety
2. Assess damage/impact scope
3. Activate crisis management team
4. Establish emergency communication
5. Notify key stakeholders

CRITICAL SYSTEMS (30 minutes - 2 hours):
1. Test SpringPoint ERP access
2. Verify internet connectivity
3. Check Active Directory status
4. Contact SpringPoint support if needed
5. Implement manual workarounds

RECOVERY PHASE (2-8 hours):
1. Complete SpringPoint DR activation
2. Failover to secondary AD controller
3. Begin file server restoration
4. Deploy temporary workstations
5. Restore critical network services

FULL RESTORATION (8-48 hours):
1. Complete file server recovery
2. Restore SQL Server/IIS systems
3. Rebuild network infrastructure
4. Deploy all user workstations
5. Verify all business processes

POST-RECOVERY:
1. Document lessons learned
2. Update DR procedures
3. Schedule follow-up testing

4. Review vendor performance
5. Update emergency contacts

C.2 Vendor Escalation Quick Reference

SPRINGPOINT ESCALATION:
Level 1: Support Portal + [Phone]
Level 2: Account Manager + [Phone]
Level 3: SpringPoint Management + [Phone]

COVE BACKUP ESCALATION:
Level 1: Support Portal + [Phone]
Level 2: Technical Support + [Phone]
Level 3: Account Manager + [Phone]

INTERNET SERVICE ESCALATION:
Level 1: ISP Support + [Phone]
Level 2: Business Support + [Phone]
Level 3: Account Manager + [Phone]

IT SUPPORT ESCALATION:
Level 1: Help Desk + [Phone]
Level 2: Senior Technician + [Phone]
Level 3: Manager + [Phone]

APPENDIX D: MANUAL PROCEDURES

D.1 Manual Job Tracking Procedures

EMERGENCY JOB TRACKING PROCESS:
(When SpringPoint ERP is unavailable)

CUSTOMER CALL INTAKE:
1. Use paper forms to record:
2. Customer name and contact info
3. Equipment type and issue description
4. Location and accessibility
5. Priority level (emergency/routine)
6. Preferred appointment time

DISPATCH PROCEDURES:
1. Assign technician based on location and expertise
2. Provide technician with:
3. Paperwork order form
4. Customer contact information
5. Basic equipment specifications
6. Parts list if known

FIELD DOCUMENTATION:
1. Technician completes paper form with:
2. Time on site/time completed
3. Work performed description
4. Parts used (part numbers and quantities)
5. Customer signature
6. Photos with phone/camera

DATA ENTRY AFTER RECOVERY:
1. Enter all manual records into SpringPoint
2. Upload photos to appropriate job records
3. Generate invoices for completed work
4. Update inventory for parts used
5. Verify all manual data is accurately captured

D.2 Emergency Procurement Procedures

EMERGENCY PARTS ORDERING:
(When SpringPoint purchasing is unavailable)

AUTHORIZED PURCHASERS:
1. Service Manager: Up to $5,000
2. Operations Manager: Up to $25,000
3. Senior Partner: Unlimited

EMERGENCY VENDORS:
1. Primary Supplier: [Vendor name/phone]
2. Secondary Supplier: [Vendor name/phone]
3. Local Suppliers: [List of local vendors]

ORDERING PROCESS:
1. Verify part number and specifications.
2. Contact authorized vendor directly.
3. Place order with purchase order number.
4. Document order details on paper form.
5. Arrange delivery to job site or office.
6. Obtain receipt and shipping documentation.
7. Enter all emergency purchases into SpringPoint after recovery.

APPENDIX E: RECOVERY FORMS AND TEMPLATES

E.1 Disaster Declaration Form

BRANDON & CLARK DISASTER DECLARATION

Date: _____ Time: _____

Declared by: _____
Title: _____
Contact: _____

DISASTER TYPE:
1. Natural disaster (flood, fire, storm, etc.)
2. Technology failure (hardware, software, network)
3. Cybersecurity incident
4. Building/facility issue
5. Vendor/supplier failure
6. Other: _____

IMPACT ASSESSMENT:
1. SpringPoint ERP affected
2. Active Directory affected
3. File server affected
4. Network infrastructure affected
5. Building/facilities affected
6. Personnel affected

ESTIMATED RECOVERY TIME:
1. Less than 2 hours
2. 2-8 hours
3. 8-24 hours
4. More than 24 hours
5. Unknown at this time

INITIAL ACTIONS TAKEN:
1. Personnel safety ensured
2. Crisis team activated
3. Key vendors contacted
4. Backup systems activated
5. Manual procedures implemented
6. Stakeholders notified

Signature: _____ Date/Time: _____

E.2 Recovery Status Log

RECOVERY PROGRESS TRACKING LOG

Disaster Start: _____ Recovery Start: _____
Crisis Manager: _____ IT Manager: _____

Time	Action/Update	Person Responsible	Status	Next Steps

____	_____	_____	_____	_____
____	_____	_____	_____	_____
____	_____	_____	_____	_____
____	_____	_____	_____	_____

RECOVERY MILESTONES:
1. SpringPoint ERP restored: _____ (time)
2. Active Directory operational: _____ (time)
3. File server accessible: _____ (time)
4. Network fully functional: _____ (time)
5. All users working: _____ (time)
6. Business operations normal: _____ (time)

ISSUES/CONCERNS:
_____
_____
_____

FINAL RECOVERY CONFIRMATION:
Recovery Complete: _____ (date/time)
Confirmed by: _____
Signature: _____

DOCUMENT CONTROL

PLAN INFORMATION:
Document Title: Brandon & Clark Disaster Recovery Plan
Version: 1.0
Created: [Date]
Last Reviewed: [Date]
Next Review Due: [Date + 1 year]
Owner: [Crisis Manager name]
Approved by: [Senior Partner name]

DISTRIBUTION LIST:
1. Crisis Management Team (complete copy)
2. Department Managers (relevant sections)
3. IT Personnel (technical sections)
4. Offsite Storage (backup copy)
5. Key Vendors (contact sections)

REVISION HISTORY:

Version	Date	Changes Made	Approved By
1.0	[Date]	Initial creation	[Name]

IMPORTANT NOTICE:
This disaster recovery plan contains sensitive information about Brandon & Clark's technology infrastructure and business processes. Distribution should be limited to authorized personnel only. The plan should be reviewed and updated regularly to ensure accuracy and effectiveness. All personnel with access to this plan should be trained on their roles and responsibilities during a disaster recovery event.

END OF DISASTER RECOVERY PLAN

Brandon & Clark
Version 1.0 - [Date]
For questions or updates, contact: [Crisis Manager contact information]