Cyber Resilience Planning Workshop

Cyber Recovery Plan Template

READIVERSE

Commvault

TABLE OF CONTENTS

DOCUMENT CONTROL & EMERGENCY INFORMATION 3
Revision History 3
Executive Summary 3
Purpose of this Plan 3
Activation Criteria 3
Plan Authority 4
Alternate Authority | if Primary Authority is Unreachable 4
Emergency Contact List 4
Document Access & Storage 5
Physical Hard Copy Location 5
Encrypted Offline Copy Location 5
Vault / Safe Access Procedure 5
GOVERNANCE, ROLES, AND OBJECTIVES 6
Purpose, Scope, and Assumptions 6
Cyber Recovery Team (CRT) 6
Authority & Decision Rights 6
PLAN ACTIVATION & COMMUNICATION 7
Plan Activation Checklist 7
Internal Communications Protocol 7
Employee Communications Cadence 7
Executive Briefing Cadence 7
External Communications 8
Legal Contact 8
Insurance Notification Timeline 8
Regulatory Notification Triggers 8
AS-BUILT AND CRITICAL ASSET INVENTORY 10
Business Impact & Prioritization 10
System Prioritization Matrix 11
Backup Environment Architecture Diagram 11
Critical Credentials and Licensing 11
CYBER RECOVERY PROCEDURES 12
Isolated Recovery Environment (IRE) Setup 12
Critical Credentials and Licensing 12
Core Infrastructure Restoration 12
Security Hardening and Verification 13
Testing, Maintenance, and Post-Recovery 13
Testing and Exercise Schedule 13
Maintenance and Update Schedule 13
Post-Incident Review (Lessons Learned) 14
Plan Maintenance 14
Frequency to Review and Update 14
Ownership 14
Post-Incident Review (Lessons Learned) 15
Appendix A: Cyber Insurance & Legal Considerations 15
Appendix B: Regulatory & Compliance Mapping 15

DOCUMENT CONTROL & EMERGENCY INFO

REVISION HISTORY

Version	Date	Author	Summary of Change
1.0			Initial Draft

EXECUTIVE SUMMARY

PURPOSE OF THIS PLAN

Describe the organization's intent to recover from a cyber-specific disruptive event (e.g., ransomware, wiper malware, insider threat).

ACTIVATION CRITERIA

This plan is invoked when:
- Malware or ransomware is confirmed or suspected
- Identity systems are compromised
- Backup integrity is in question
- Business operations are materially disrupted
- Other:

DOCUMENT CONTROL & EMERGENCY INFORMATION

PLAN AUTHORITY

This Role is authorized to activate this plan:

PLAN AUTHORITY: *(Include name, title, email, cell phone and alternative cell or email)*

ALTERNATE AUTHORITY | IF PRIMARY AUTHORITY IS UNREACHABLE:

(Include name, title, email, cell phone and alternative cell or email)

EMERGENCY CONTACT LIST *(Hard Copy Required: Input all from RACI model)*

Role	Name	Phone	Email	Out-of-Band Contact	Notes
IT Director					
Security Lead					
Legal Counsel					
Cyber Insurance					
Forensic Partner					
Law Enforcement					

DOCUMENT CONTROL & EMERGENCY INFORMATION

DOCUMENT ACCESS & STORAGE

PHYSICAL HARD COPY LOCATION:

ENCRYPTED OFFLINE COPY LOCATION:

VAULT / SAFE ACCESS PROCEDURE:

GOVERNANCE, ROLES, AND OBJECTIVES

PURPOSE, SCOPE, AND ASSUMPTIONS

(Include name, title, email, cell phone and alternative cell or email)

- This plan focuses on recovery, not detection
- Assumes perimeter defenses may be bypassed
- Assumes identity compromise is possible

CYBER RECOVERY TEAM (CRT)

(Clearly outline CRT organizational chart: Includes CRT Team Lead, Crisis Management Team, and Technical Teams involved in cyber incident)

Role	Responsibilities	Primary Contact	Alternate Contact
IT Director	Overall ownership, recovery approval		
Security Director	Breach assessment, threat validation		
Recovery Lead	Technical recovery execution		
Forensics Lead	Cleanliness validation		
Communication Lead	Internal & external comms		

AUTHORITY & DECISION RIGHTS

(Who has authority to disconnect/restore systems/sign off on recovery costs)

Define Who Can:	Primary Contact	Alternate Contact
Disconnect production systems		
Declare backups unsafe		
Approve restore to production		
Approve extraordinary spend		

PLAN ACTIVATION & COMMUNICATION

PLAN ACTIVATION CHECKLIST

Triage steps to confirm a full recovery as necessary

- □ Incident validated as cyber-related
- □ Identity compromise assessed
- □ Backup integrity questioned
- □ Executive notification complete

INTERNAL COMMUNICATIONS PROTOCOL:

EMPLOYEE COMMUNICATIONS CADENCE:

EXECUTIVE BRIEFING CADENCE:

EXTERNAL COMMUNICATIONS

Legal approval required before external communications.

LEGAL CONTACT:

INSURANCE NOTIFICATION TIMELINE:

REGULATORY NOTIFICATION TRIGGERS:

Vendor Type	**Company Name**	**Contact Name, Phone & Email Address**	**Contract Notes *(Include: account number and any relvant access code details for your account)***
Backup & Recovery			
Cloud Provider			
MSSP / IR Firm			

AS-BUILT AND CRITICAL ASSET INVENTORY

BUSINESS IMPACT & PRIORITIZATION

Application	Business Function	RTP	RPO	Priority

AS-BUILT AND CRITICAL ASSET INVENTORY

SYSTEM PRIORITIZATION MATRIX

Order of recovery for all critical applications and infrastructure.

Application / System Name	Order to Recover	Application or System Owner

BACKUP ENVIRONMENT ARCHITECTURE DIAGRAM

(Add Visio/CAD images for each bullet)

- Production environment
- Backup storage tiers
- Cyber Vault / IRE
- Clean Room tooling

CRITICAL CREDENTIALS AND LICENSING

(Secure location/retrieval procedure for OS keys, application licenses, administrative passwords, certificates)

Credential Type	Location	Access Method	Rotation Plan

CYBER RECOVERY PROCEDURES

ISOLATED RECOVERY ENVIRONMENT (IRE) SETUP

(Step-by-step to bring up the Clean Room, including networking and analysis tools)

Checklist:
- Backup storage tiers
- Cyber Vault / IRE
- Clean Room tooling

CRITICAL CREDENTIALS AND LICENSING

(Secure location/retrieval procedure for OS keys, application licenses, administrative passwords, certificates)

□ Isolated network established
□ No trust relationships with production
□ Logging & monitoring enabled

CORE INFRASTRUCTURE RESTORATION

(Detailed, step-by-step runbooks for the foundational systems: Clean Active Directory, Clean DNS/DHCP, Network Configuration)

Restore order: 1. Clean Identity (AD / IAM) 2. DNS / DHCP 3. Network services

Document validation steps after each restore.

Critical Application	Restore Method	Validation Owner	Functional Test Steps

CYBER RECOVERY PROCEDURES

SECURITY HARDENING AND VERIFICATION

(Steps to patch, change all passwords, and verify system security before returning to production)

□ MFA enforced
□ EDR deployed
□ Vulnerability scan completed

TESTING, MAINTENANCE, AND POST-RECOVERY

Describe forensic approval process before promotion to production.

TESTING AND EXERCISE SCHEDULE

(Required frequency for tabletop and full technical recovery testing)

MAINTENANCE AND UPDATE SCHEDULE

(When the plan/runbooks are reviewed and updated)

POST-INCIDENT REVIEW (LESSONS LEARNED)

(Checklist for gathering data and conducting a formal review after recovery)

PLAN MAINTENANCE

FREQUENCY TO REVIEW AND UPDATE

OWNERSHIP:

POST-INCIDENT REVIEW (LESSONS LEARNED)

Checklist:

□ Timeline created
□ Control gaps identified
□ Plan updates captured

METRICS & READINESS KPIS

- Time to clean restore
- Backup integrity confidence
- Test success rate

APPENDIX A: CYBER INSURANCE & LEGAL CONSIDERATIONS

- Policy notification timelines
- Ransom payment decision authority
- Evidence preservation requirements

APPENDIX B: REGULATORY & COMPLIANCE MAPPING

Map recovery requirements to:
- NIST CSF
- ISO 27001
- DORA / SEC / HIPAA (as applicable)

Commvault®

commvault.com | 888.746.3849

© Commvault – Cyber Resilience Workshop CR Plan Template 2026