CSNP
CYBERSECURITY NON-PROFIT

Backup & Disaster Recovery Plan Template

A comprehensive framework for protecting your organization's critical data and ensuring business continuity. Developed by the Cybersecurity Non-Profit (CSNP).

CHAPTER 1

Plan Overview & Core Objectives

Purpose

This disaster recovery plan establishes procedures to protect, backup, and restore your organization's critical systems and data in the event of hardware failure, cyberattack, natural disaster, or other disruptions.

Key Goals

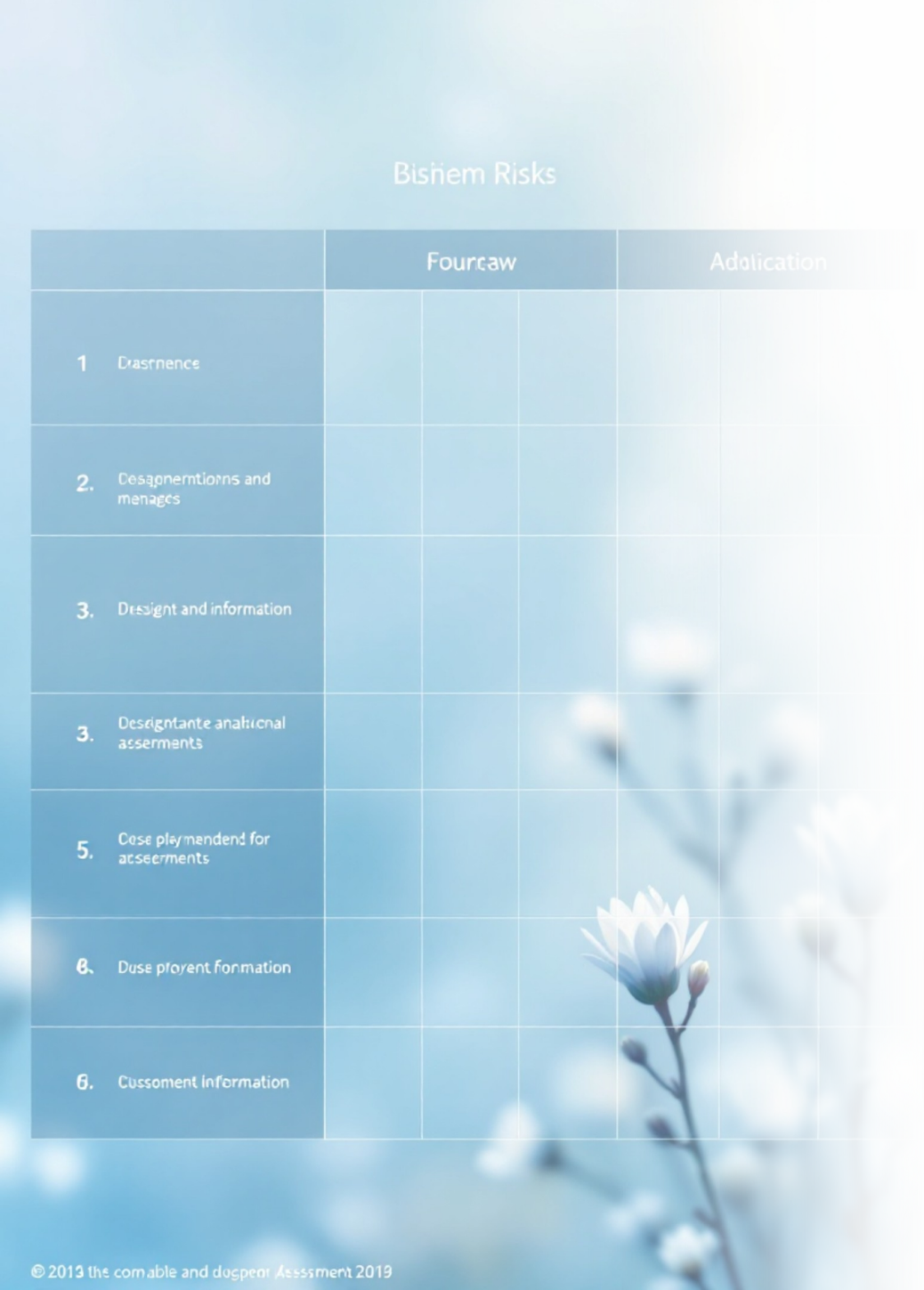
- Minimize data loss and downtime
- Ensure rapid recovery of operations
- Protect against financial and reputational damage
- Maintain compliance with regulations

Plan Scope

This template covers all critical business systems, applications, and data repositories essential to your organization's daily operations.

Success Metrics

- Recovery Time Objective (RTO) achievement
- Recovery Point Objective (RPO) compliance
- Regular testing completion rates
- Stakeholder awareness levels



CHAPTER 2

Risk Assessment Framework

1

Identify Threats

List potential disasters: ransomware, hardware failure, fire, flood, power outage, human error, insider threats.

Action: Document all relevant risks for your organization.

2

Assess Impact

Evaluate the potential business impact of each threat on operations, revenue, reputation, and compliance.

Action: Rate each risk as Low, Medium, High, or Critical.

3

Prioritize Response

Focus resources on mitigating the highest-impact, most likely risks first.

Action: Create a prioritized list of risks requiring immediate attention.

CHAPTER 3

Critical Systems Inventory

Document all systems, applications, and data that are essential to your business operations. This inventory forms the foundation of your recovery priorities.

System/Application	Criticality Level	Dependencies	Recovery Priority
Example: Email System	Critical	Internet, Authentication	Tier 1 (Immediate)
Example: CRM Database	Critical	Network, Storage	Tier 1 (Immediate)
Example: File Server	High	Network, Backup System	Tier 2 (Within 4 hours)
Example: Accounting Software	High	Database, Network	Tier 2 (Within 8 hours)
[Your System]	[Fill in]	[Fill in]	[Fill in]

CHAPTER 4

The 3-2-1 Backup Strategy

3 Copies

Maintain at least three copies of your data: one primary and two backups. This protects against single points of failure.

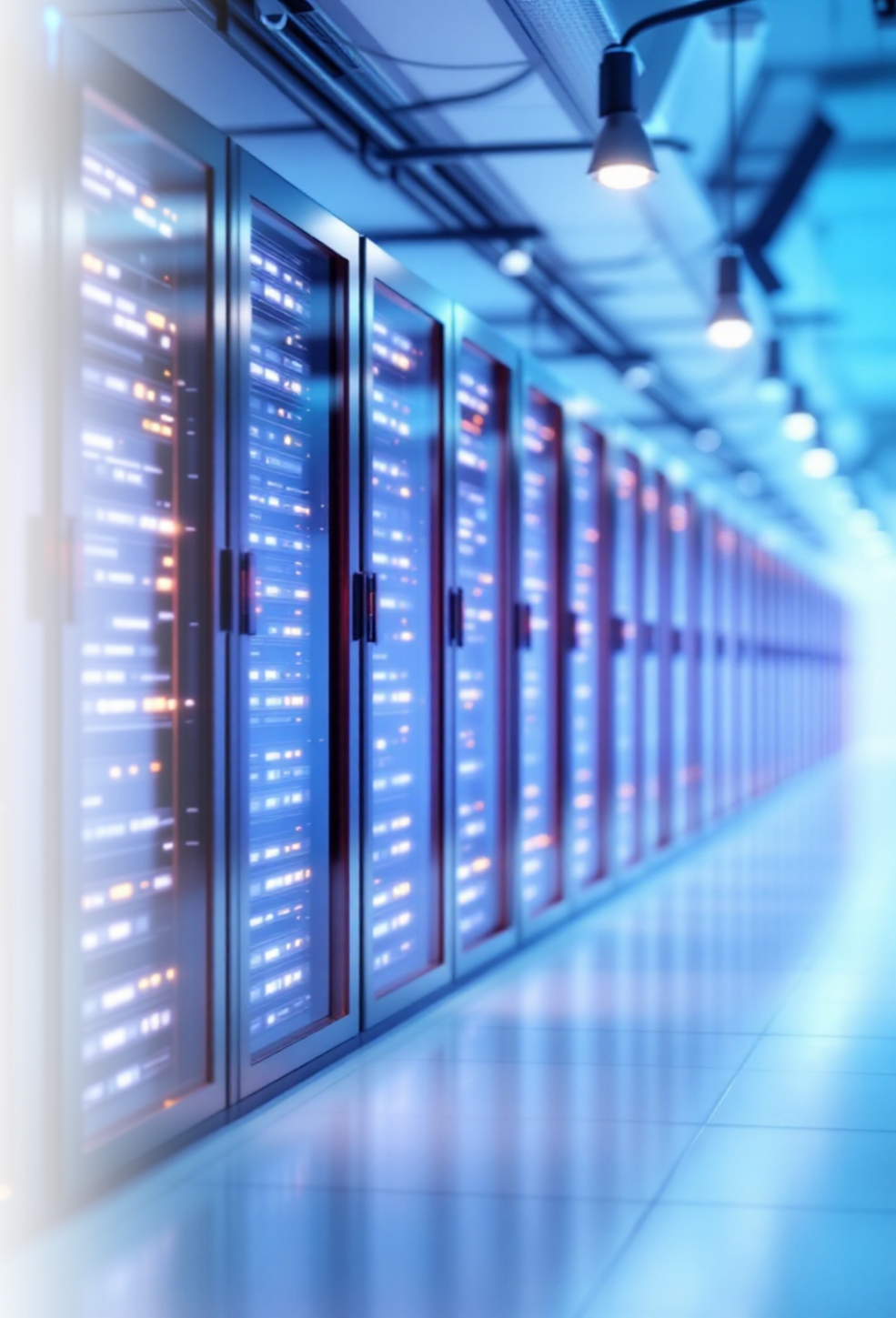
2 Media Types

Store backups on two different media types (e.g., local disk and cloud storage) to protect against media-specific failures.

1 Off-Site

Keep one backup copy off-site or in the cloud to protect against physical disasters at your primary location.

Best Practice: Encrypt all backup copies and test restoration regularly to ensure data integrity and accessibility.



CHAPTER 5

Backup Schedule & Retention

Recommended Backup Frequencies

Critical Systems

Continuous or hourly backups for mission-critical data and applications.

Important Data

Daily backups for essential business files and databases.

Standard Files

Weekly backups for less critical but important organizational data.

Archival Data

Monthly backups for historical records and compliance documentation.

Retention Policy Template

Define how long to keep each backup type based on business needs and compliance requirements.

Daily backups: Retain for 7-30 days

Weekly backups: Retain for 4-12 weeks

Monthly backups: Retain for 12-24 months

Annual backups: Retain for 3-7 years

Fill in retention periods based on your regulatory requirements and business needs.

CHAPTER 6

Recovery Objectives: RTO & RPO

Recovery Time Objective (RTO)

The maximum acceptable time that a system can be down after a disaster before business impact becomes unacceptable.

Example: Email system RTO = 2 hours
This means email must be restored within 2 hours of failure.

Define RTO for each critical system in your inventory.

Recovery Point Objective (RPO)

The maximum acceptable amount of data loss measured in time. How much data can you afford to lose?

Example: Customer database RPO = 15 minutes
This means you can lose no more than 15 minutes of data.

Define RPO for each critical system in your inventory.

Your backup frequency must be shorter than your RPO, and your recovery procedures must meet your RTO requirements.

CHAPTER 7

Step-by-Step Recovery Procedures

1. Assess the Situation

Determine the scope of the disaster, affected systems, and estimated downtime. Document all observations.

2. Activate Response Team

Notify key personnel according to your communication plan. Assign specific recovery responsibilities.

3. Secure Environment

Ensure the recovery environment is safe and ready. Address any immediate threats before restoration.

4. Restore Priority Systems

Begin restoration with Tier 1 critical systems according to your inventory priorities and RTO targets.

5. Verify & Test

Confirm all systems are functioning correctly. Test data integrity and application functionality thoroughly.

6. Resume Operations

Transition back to normal operations incrementally. Monitor systems closely for 24-48 hours post-recovery.

CHAPTER 8

Testing & Validation Schedule

Regular testing ensures your backup and recovery procedures work when you need them most. A plan that hasn't been tested is just a theory.

Testing Frequency

Monthly: Backup Verification

Verify that backups are completing successfully and data is accessible.

Quarterly: Partial Recovery

Test restoration of individual files and databases to ensure procedures work.

Annual: Full Recovery Drill

Conduct a complete disaster recovery exercise simulating a major system failure.

Testing Documentation

For each test, record:

- Date and time of test
- Systems/data tested
- Test results and timing
- Issues encountered
- Corrective actions needed
- Team members involved

Update your recovery procedures based on test results and lessons learned.

CHAPTER 9

Emergency Communication Plan

Internal Notifications

Establish a clear communication chain for alerting internal stakeholders during a disaster.

Key contacts: IT team, management, department heads, all staff

List primary and backup contact methods for each person.

External Communications

Define how and when to notify external parties about service disruptions.

Stakeholders: Customers, vendors, partners, regulatory bodies, media (if needed)

Prepare template messages for different disaster scenarios.

Status Updates

Establish regular update intervals to keep stakeholders informed during recovery operations.

Frequency: Every 2-4 hours during active recovery

Designate a single point of contact for official updates.

CHAPTER 10

Vendor & Service Provider Contacts

Maintain an updated list of all critical vendors and service providers who may be needed during recovery operations.

Vendor/Provider	Service Type	Emergency Contact	Account/Contract Info
Internet Service Provider	Connectivity	[Phone/Email]	[Account #, Support Level]
Cloud Storage Provider	Backup/Storage	[Phone/Email]	[Account #, SLA Terms]
Hardware Vendor	Equipment	[Phone/Email]	[Support Contract Details]
Software Vendors	Applications	[Phone/Email]	[License Keys, Support]
IT Support Partner	Technical Services	[Phone/Email]	[Contract Terms, SLA]
[Add More]	[Fill in]	[Fill in]	[Fill in]

Keep physical copies of this contact list in multiple secure locations, as digital systems may be unavailable during a disaster.

CHAPTER 11

Recovery Execution Checklist

Initial Response (0-2 hours)

- ☐ Assess and document the incident
- ☐ Activate disaster recovery team
- ☐ Notify key stakeholders
- ☐ Secure affected systems
- ☐ Begin impact assessment
- ☐ Initiate communication plan

Recovery Phase (2-24 hours)

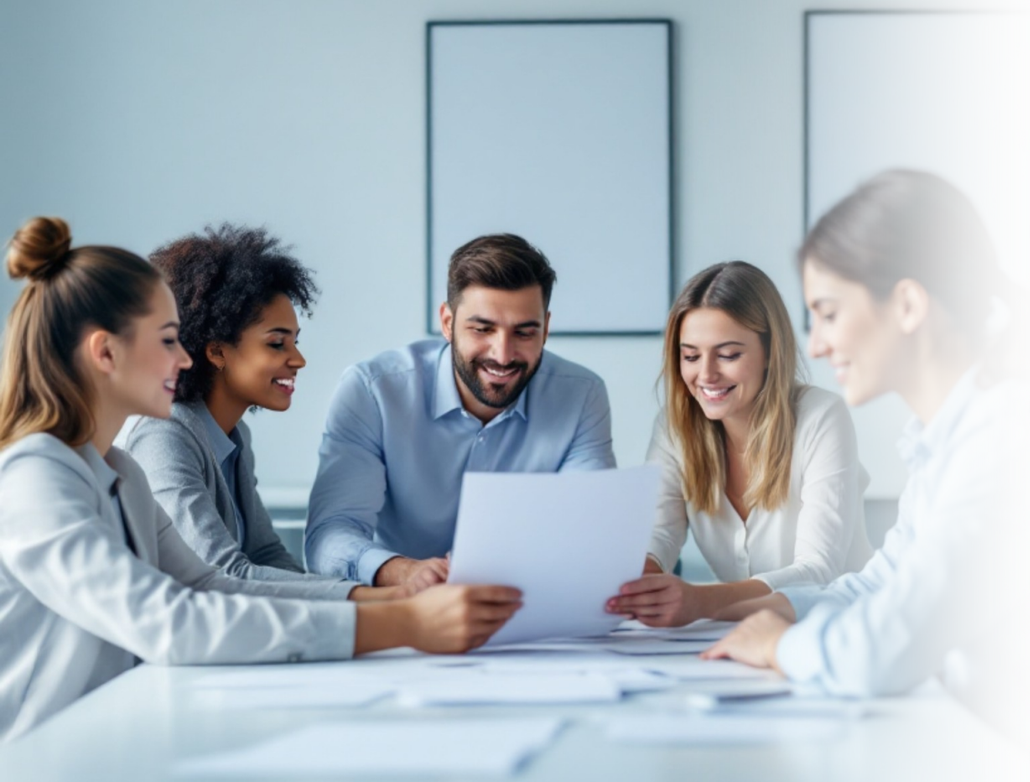
- ☐ Restore Tier 1 critical systems
- ☐ Verify backup integrity
- ☐ Test restored systems
- ☐ Document recovery actions
- ☐ Provide stakeholder updates
- ☐ Monitor system stability

Restoration Phase (24+ hours)

- ☐ Restore Tier 2 and 3 systems
- ☐ Complete data integrity checks
- ☐ Resume normal operations gradually
- ☐ Continue system monitoring
- ☐ Update stakeholders on status

Post-Recovery (1 week)

- ☐ Conduct post-incident review
- ☐ Document lessons learned
- ☐ Update recovery procedures
- ☐ Repair or replace damaged systems
- ☐ Strengthen backup procedures
- ☐ Brief team on improvements



CHAPTER 12

Plan Maintenance & Updates

Your disaster recovery plan is a living document that must evolve with your organization. Regular maintenance ensures it remains effective and relevant.

1

Quarterly Reviews

Review and update contact information, system inventories, and vendor contracts. Verify all documented procedures remain current.

2

Semi-Annual Audits

Conduct comprehensive audit of backup systems, test results, and recovery capabilities. Update RTO/RPO targets as needed.

3

Annual Revisions

Major plan review incorporating test results, technology changes, organizational updates, and lessons learned from incidents.

4

Trigger Updates

Update immediately when: new systems are deployed, personnel changes occur, vendors change, or after any disaster recovery event.

Version Control: Date each revision and maintain a change log documenting all updates to the plan.

About the Cybersecurity Non-Profit

> Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Our Programs for Everyone

Business & Non-Profit Security

Essential cybersecurity guidance for organizations of all sizes

Family Cybersecurity

Protecting your household in the digital age

Kids Safety

Age-appropriate online safety education for children

Senior Digital Safety

Empowering seniors to navigate technology safely

Women's Security

Specialized digital safety resources and support

Parents & Educators

Tools to teach and protect the next generation

Everything We Offer is Free

Access our complete library of resources, templates, and educational materials at no cost.

Connect With Us

Website: csnp.org
Resources: csnp.org/resources