Microsoft 365 Disaster Recovery Plan Template

Purpose and Scope

Purpose: To ensure rapid recovery and continuity of Microsoft 365 services following a disruptive event (cyberattack, outage, misconfiguration, accidental deletion, etc.)

Scope:

- Covers all M365 workloads (Exchange, Teams, SharePoint, OneDrive, Entra, etc.)
- Applies to both cloud-only and hybrid environments
- Provides tenant-wide and workload-specific recovery steps

1. Key Contacts

Role	Name	Email	Phone	Backup Contact
M365 Admin Lead				
Security Officer				
CoreView Support	N/A	support@coreview.com	N/A	N/A
Incident Response				

2. Risk Assessment and Impact Analysis

- Risk assessment and impact analysis
- Identify critical workloads (e.g., Exchange, SharePoint, Teams)
- Document dependencies (on-prem AD connectors, identity sources)
- Assess business impact for downtime of each service

3. Disaster Senarios

- Ransomware or cyberattack
- Accidental massive deletion or misconfiguration
- Service outage (Microsoft cloud or sync failure)
- Configuration drift causing privilege escalation

4. Recovery Objectives

- RTO (recovery time objective), e.g., restore core email service within two hours of incident
- RPO (recovery point objective), e.g., data/configuration loss limited to max one hour

5. Backup and Restore Procedures

Configuration Backup:

- Use CoreView or equivalent tools to back up M365 configuration regularly (daily/weekly)
- Store backup securely offsite or in a secondary tenant

Restoring Configuration:

- Use configuration “rewind” to restore affected workloads or entire tenant
- Validate rollback does not introduce new risks
- Document restore points for audit

Data Backup and Restore:

- Confirm all critical mailboxes, SharePoint sites, and OneDrive accounts are included in backup scope
- Follow Microsoft documented restore methods for files, mail, and sites

6. Incident Response

- **Detection:** Use CoreView, Defender to detect drift, get policy alerts, and forensic analysis
- **Containment:** Disable affected accounts, segment network, apply least-privilege controls, revoke external access
- **Eradication and recovery:** Remove threats, restore configuration/data, validate operations
- **Post-incident review:** Audit, document actions, update policies as needed.

7. Communication Plan

- Notify stakeholders, IT, executives, and affected users per crisis escalation matrix
- Provide regular updates as recovery progresses

8. Testing and Review

- Schedule regular disaster recovery exercises (at least twice per year)
- Review plan after each exercise or major incident
- Update contact details and procedures quarterly

9. Role of Coreview in Disaster Recovery

- Unified visibility across all M365 tenants and workloads
- Backup and restore of entire tenant configuration
- Virtual tenant segmentation for rapid containment and least-privilege response
- Automation of recovery tasks
- Audit trail and reporting

10. Documentation and Resources

- Store all logs, restore records, and proofs of testing in compliance repository
- Reference Microsoft and CoreView documentation for procedure details

11. Approvals

Name	Role	Signature

For more information about CoreView's disaster recovery and automation capabilities, get in touch.