ARMORYFIVE

Disaster Recovery Checklist

A high-level guide for restoring critical systems and minimizing downtime during an outage or cyber incident.

1. Identify Critical Systems and Data

- List every system that supports day-to-day operations (servers, workstations, applications, cloud services, etc.).
- Classify them by priority: mission-critical, important, and non-essential.
- Document where each system's data lives (on-prem, cloud, backup, or hybrid).

Tip: The first step to recovery is knowing what matters most–and where it's stored.

2. Define Recovery Objectives

- Establish Recovery Time Objective (RTO) – how long each system can be offline before business impact occurs.
- Establish Recovery Point Objective (RPO) – how much data you can afford to lose between the last backup and the incident.
- Record these values in a simple table and align them with your backup and failover strategy.

3. Backups and Replication

- Confirm automated, tested backups exist for every critical system.
- Store at least one copy off-site or in the cloud, separate from production networks.
- Validate encryption, retention periods, and integrity (run periodic test restores).
- For virtual or cloud environments, confirm replication jobs and snapshot schedules are up to date.

If you've never tested a restore, you don't really have a backup.

4. Network and Infrastructure Recovery

- Document all IP addressing, VLANs, routing, VPNs, and firewall rules in a secure location.
- Keep an inventory of network devices, servers, storage arrays, and power systems with model numbers and configurations.
- Record where infrastructure backups (configs, exports) are stored and who has access.
- Ensure critical hardware spares, credentials, and recovery media are accessible during an outage.

5. Access and Authentication

- Maintain a secure copy of admin credentials for all core systems (servers, networking, cloud).

- Document domain controllers, identity providers, and MFA requirements.
- Plan how to restore identity systems first – they're often the key to accessing everything else.

6. Incident Response Integration

- Establish a clear process for triggering disaster recovery after a major incident.
- Document who declares a disaster, who communicates updates, and who coordinates technical recovery.
- Link your DR plan to your incident response playbook for ransomware, hardware failure, or natural disasters.

7. Restoration Procedures

- Define the order of recovery for servers and services (e.g., DNS, AD, file shares, databases, applications).
- Outline basic steps for restoring systems from backup or image.
- Verify system integrity and functionality before reconnecting to production networks.
- Maintain documentation for each recovery test or event.

8. Testing and Continuous Improvement

- Schedule at least one recovery test per year (tabletop or live).
- Review outcomes, note bottlenecks, and update documentation.
- Revisit your RTO/RPO and backup policies after any infrastructure or application change.

9. Communication and Documentation

- Store your DR plan in both digital and printed form (offline copy).
- Keep a contact list for key personnel, vendors, ISPs, and emergency services.
- Establish internal communication channels for downtime events.

10. Professional Review

Even the best documentation can't replace experience. A professional assessment ensures your plan is executable under real-world stress.
Armory5 offers tailored Disaster Recovery Consulting–covering plan design, infrastructure testing, and automated recovery validation.

Ready to move beyond a checklist? Schedule a consultation with our team to build a recovery plan that actually works under fire.