

IT Disaster Recovery Checklist

An IT disaster recovery checklist for small and mid-sized teams: priorities, backups, runbooks, incident response, recovery and testing.

Scope and Priorities

- ☐ List every critical system, application and data store
- ☐ Map which business processes depend on each system
- ☐ Set a recovery time objective (RTO) for each system
- ☐ Set a recovery point objective (RPO) for each system
 - The RPO sets your backup frequency: a one-hour RPO needs at least hourly backups or replication.
- ☐ Rank systems into recovery tiers, with dependencies first
 - Identity, DNS and networking usually have to come back before the applications that rely on them.
- ☐ Get management sign-off on the targets and the budget they need

Backups and Data Protection

- ☐ Follow the 3-2-1 rule: three copies, two media types, one off-site
- ☐ Keep at least one immutable or offline backup copy
 - Ransomware commonly targets connected backups first, so an offline or immutable copy is your last line of defense.
- ☐ Back up cloud and SaaS data, not just on-premises servers
- ☐ Encrypt backups and store the keys separately
- ☐ Use separate credentials with MFA for backup administration
- ☐ Monitor backup jobs and alert on failures

Recovery Environment

- ☐ Choose a recovery site: cloud, secondary data center or hot, warm or cold standby
- ☐ Document network, firewall and DNS settings needed to fail over
- ☐ Keep spare hardware or a replacement plan for key devices
- ☐ Store licenses, installers and configuration exports off-site

Runbooks and Contacts

- ☐ Write step-by-step recovery runbooks for each tier-one system
- ☐ Assign a recovery owner and a backup person for each system
- ☐ Keep a contact list for staff, vendors, ISP, insurer and cloud providers
- ☐ Store the plan where you can reach it if your systems are down
 - Keep a printed copy and a copy outside your own network, since the plan is useless if it lives only on the systems that failed.
- ☐ Prepare message templates for staff and customers

During an Incident

- ☐ Declare the incident and name an incident lead
- ☐ Contain the problem: isolate infected or failing systems
- ☐ Preserve logs and evidence before wiping anything in a security incident

- ☐ Notify management, insurers and any regulators that require it
- ☐ Log every decision and action with a timestamp

Recovery and Validation

- ☐ Restore systems in tier order, starting with dependencies
- ☐ Check restored data is complete and from a clean point in time
- ☐ Have system owners confirm each service works before go-live
- ☐ Reset passwords and keys if credentials may be compromised
- ☐ Watch restored systems closely for errors or reinfection

Testing and Review

- ☐ Run a test restore of sample files every month
- ☐ Run a full disaster recovery test or tabletop exercise every year
- ☐ Measure actual recovery times against your RTO and RPO
- ☐ Hold a lessons-learned review after every test or real incident
- ☐ Update the plan after major system, staff or vendor changes