IT Disaster Recovery Plan

Archived: 2026-04-05 18:34:56 UTC

Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential.

An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan. Priorities and recovery time objectives for information technology should be developed during the business impact analysis. Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the business recovery.

IT Recovery

Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective for the business function or process that depends on the IT resource.

Recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

Developing an IT Disaster Recovery Plan

Businesses should develop an IT disaster recovery plan. It begins by compiling an inventory of hardware (e.g. servers, desktops, laptops and wireless devices), software applications and data. The plan should include a strategy to ensure that all critical information is backed up.

Identify critical software applications and data and the hardware required to run them. Using standardized hardware will help to replicate and reimage new hardware. Ensure that copies of program software are available to enable re-installation on replacement equipment. Prioritize hardware and software restoration.

Document the IT disaster recovery plan as part of the business continuity plan. Test the plan periodically to make sure that it works.

Data Backup

Businesses generate large amounts of data and data files are changing throughout the workday. Data can be lost, corrupted, compromised or stolen through hardware failure, human error, hacking and malware. Loss or corruption of data could result in significant business disruption.

Data backup and recovery should be an integral part of the business continuity plan and information technology disaster recovery plan. Developing a data backup strategy begins with identifying what data to backup, selecting and implementing hardware and software backup procedures, scheduling and conducting backups and periodically validating that data has been accurately backed up.

Developing the Data Backup Plan

Identify data on network servers, desktop computers, laptop computers and wireless devices that needs to be backed up, along with other hard copy records and information. The backup plan should include regularly scheduled backups from wireless devices, laptop computers and desktop computers to a network server. Data on the server then can be backed up. Backing up hard copy vital records can be accomplished by scanning paper records into digital formats and allowing them to be backed up along with other digital data.

Data should be backed up frequently. The business impact analysis should evaluate the potential for lost data and define the “recovery point objective.” Data restoration times should be confirmed and compared with the IT and business function recovery time objectives.

Resources for Information Technology Disaster Recovery Planning

- Computer Security Resource Center - National Institute of Standards and Technology (NIST), Computer Security Division Special Publications
- Contingency Planning Guide for Federal Information Systems - NIST Special Publication 800-34 Rev. 1
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities – NIST Special Publication 800-84
- Building An Information Technology Security Awareness and Training Program - NIST Special Publication 800-50

Source: https://www.ready.gov/business/implementation/IT