FivePaths

Anatomy of an Information Technology Disaster Recovery Plan

What public agencies should consider when planning for disaster recovery in information technology.

www.fivepaths.com | info@fivepaths.com | 415 - 326 - 3483

The following are elements agencies should consider in an information technology disaster plan.

Goals

Goals can differ across organizations. For public agencies, consider including goals that focus on the following aspects of disaster recovery:

- Minimizing interruptions to normal operations.
- Limiting the extent of disruption and damage.
- Minimizing the economic impact of an interruption.
- Establishing alternative means of operating in advance of an interruption.
- Training personnel about emergency procedures.
- Providing a workflow for smooth and rapid restoration of service.
- Communicating clearly to the public all necessary information and alternative means for accessing services.

Personnel

This section identifies the key personnel who have the knowledge and access to technology systems and managers and executives with budgetary and decision-making authority. Consider identifying the following personnel:

- Staff with Data Processing Responsibility
- Staff with Technology Hardware and Software maintenance
- Critical outside contractors who hold access and knowledge of foundational information systems
- Chief Information Officer or similar person with director-level responsibility for technology and the ability to allocate budget and resources
- Crisis Communications Team or Marketing/Communications personnel

It is critical to update this portion of the plan regularly to ensure every person listed has the properly updated contact information - email and mobile numbers at a minimum. These people will be responsible for understanding disaster recovery and executing the plan in the event of a disaster. It is helpful to include a staff org chart so that anyone referencing the disaster recovery plan understands the reporting relationships for faster execution of the plan.

Application Profile

This section of the plan provides important detail about the critical software applications your agency chooses to include as part of disaster recovery planning. Consider tracking the following about each application:

- Application name
- Is it critical? This is a way to prioritize what to focus on in recovery responses.
- Vendor name and contact information
- Key staff maintainer (make sure they are on your personnel list!)
- Describe what information the application manages.
- Backup process: Reference the backup process you use with this system. If you don't have one, now is a great time to establish a backup workflow!

The key to disaster recovery is to not waste time identifying what applications to focus on and who to contact to execute recovery.

Inventory Profile

This section of the plan provides important detail about the critical hardware and other physical assets vital for information management that your agency chooses to include in the disaster recovery plan. Consider the following hardware:

- Laptops & mobile devices
- Desktop computer hardware
- Backup servers and hardware
- Data servers, network servers
- Network routing and firewall hardware
- Printers & scanners
- Physical files storage

For each hardware device, include an ID/tracking number and who the user or maintainer is for each system.

Information Services Backup Procedures

Many agencies lack strong backup procedures. Consider describing the following:

- Identify how each application listed in the previous section is primarily backed up. Include the

frequency of backup, how long backups are maintained, and where they are located.
- Identify alternative backup locations and workflows that are used in addition to the primary.
- Identify which hardware or service is used for the backups. Include the name and contact information for any backup service in the personnel section.

For hardware, what is the process for replacing these systems? For example, are redundant systems available, or do you have access to a replacement warranty service?

Disaster Recovery Procedures

This section provides your workflow for executing a recovery process in the event of an information technology disaster. Consider including the following:

- Plan Initiation: This is a list of steps describing how the disaster plan gets started. Be sure to follow a streamlined workflow but also one that includes the proper authoritative sign-off required to initiate disaster recovery. This section should also list the steps of engaging a disaster recovery team, analyzing the scope and significance of the disaster, and communicating with staff and the public.
- Plan Steps: This should include all the steps for executing the plan. This could include providing transportation, housing, and emergency cash for staff to minimally continue operations; providing for emergency office supplies and rental and replacement equipment; accessing backups; notifying insurers; and staff and public communications.

The goal is to have a series of steps that allow for the fast execution of a plan without debating the process itself. It can be helpful to run disaster scenarios to ensure the plan will truly work, asking teams to follow through on tasks. This can identify pitfalls in the process early, before disaster strikes.

Record of Plan Changes

This section simply records when updates are made to the plan. Ideally, add the date of the update and the information updated. This way, over time, the team responsible for maintaining the plan can see what sections have not been updated regularly or recently and focus on those sections ensuring that the whole plan gets regular attention.