Infinit Technology Solutions

Disaster Recovery – When all else fails!

IT Planning Notes

Your network's life insurance plan!

Infinit Technology Solutions | www.infint-tech.com | 877-825-8340 (Toll Free)
7037 Fly Rd. | East Syracuse, NY 13057 | 315-432-1323 (Corporate Office)
201 Main Street | East Rochester, NY 14445 | 585-425-0668 (Rochester Office)

Recovering from a disaster involves developing a business continuity plan (BCP). This outlines all the steps, processes, and procedures in preparing as best you can. It is a lengthy and detailed process with countless questions, requiring a great deal of consideration, information, and documentation. Some elements to consider are as follows.

Emergency action steps to take in an incident.

- Have a section in your plan that outlines your incident response procedures.
- Include contact information for the following teams.
    - **Emergency Team**
    - Primary employees notified when an emergency occurs. They will be responsible for all aspects of recording and monitoring the incident.

    - **Incident Response Team**
    - Employees considered the "first responders". You may want to have employees with some first aid and emergency response training on this team.

    - **Emergency Management Team**
    - Company executives to be contacted and kept informed.

    - **Technology Team**
    - IT and/or production employees to be contacted and kept informed. They may need to respond to the incident as well.

    - **Damage Assessment Team**
    - Employees who will review the aftermath of the emergency and provide an impact analysis and/or utilize 3rd-party resources to assist in that process.

Emergency action steps to take in an incident.

- Include contact information for Key Customers and Stakeholders.
- Indicate the primary and alternate assembly areas where employees will meet following an evacuation. Include emergency phone numbers for all public services.

Types of incidents that could launch the BC plan.

Be specific in identifying internal and external situations serious enough to launch a Business Continuity plan.

Not all events may warrant the launching of your Business Continuity plan, which is why you have Incident Response and Damage Assessment Teams.

Lists of key business processes to protect.

These are business processes that must be recovered and returned to normal operation as quickly as possible. There needs to be a prioritized list across the company as not all processes are created equal.

Lists of critical technologies to protect.

These are the mission-critical systems, data and databases, and technology resources needed by each process needed to restore operations.

Lists of recovery time objectives and recovery point objectives.

You will want to outline the following, as these help identify and prioritize recovery activities:

- Recovery Time (elapsed time before a disrupted process needs to be operational again
- Recovery Point Objectives (point in time to which data must be recovered)

Lists of key vendors, stakeholders, regulators and other third parties.

These are key business impactors you will want to contact quickly. Their support and/or guidance will be critical to maintaining business partner relationships and meeting your legal obligations.

Step-by-step procedures for various activities.

Use these to provide the appropriate sequence of actions

- damage assessment
- initial response activities
- disaster declaration criteria
- how to access a notification system
- building evacuation
- staff relocation to an alternate work site
- how to respond to specific kinds of incidents (i.e., power outages, water damage, floods, or severe weather)
- recovering and restarting business operations
- returning to the original (or new) work location and resuming business operations

Procedures for obtaining emergency funds.

Include a list of banks and other financial institutions with which you do business. Include specific instructions for engaging them and obtaining cash. Only authorized people should
have this data.

Use of Credit Cards.

Company credit cards can be used by authorized employees for which they may be specific dollar limits. Personal credit cards may also be used, but employees should be preapproved, and there should be a dollar limit and a reimbursement plan in place.

Lists of vital records the company needs to operate.

Paper documents, especially this required to be kept by law, should be stored appropriately. Some may need to be stored in a fire-proof cabinet and scanned and stored electronically.

References to other activities.

Be mindful you also need to plan

- awareness and training activities
- periodic reviews and audits
- periodic updating of plans, strategies, procedures, and processes .

Other Areas to Consider in Your Backup Planning

What to Include

- Mission Critical Applications
- Data
- Devices
  - Desktops
  - Laptops/Notebooks
  - Tablets
  - Servers
  - Cellphones

Occurrences

- Full All data (Recommended Weekly)
- Incremental Only data that has been changed (Recommended Daily)
- Differential Data changed since the last Full backup (As Necessary)

Scheduling Considerations

- Manual
- Semi-Automated
- Automated

Storage Considerations

- On Premise Media based
- Offsite Media based
- Cloud Storage

Retention Considerations

- Business
- Legal
- Financial
- Tax

Disposal Methods

- Disintegration
- Shredding (Disk Grinding)
- Incineration

Email Limitations and Archival Requirements

- User Quotas
- Business vs. Personal
- Legal

Like anything else, disaster recovery planning is a process that takes time and attention to detail. You may want to consider a team consisting of line-of-business managers along with folks from IT. This will help get the work done and raise awareness for the importance the plan should take with everyone.