Company System Disaster Recovery Plan

Ryan Scott

Grand Canyon University  
ITT-306 Information Security II

Prof. Christine Bakke

## Personnel

During a crisis such as this, it’s all hands on deck!

Norma, the CEO: In their capacity as the CEO of the organization, Norma will need to be informed of the situation and will be responsible for making key decisions regarding the company's responses to the loss of IT services.

Vince, the Accountant: As the loss of IT services could affect the company's finances, Vince must be involved in the emergency meeting. He is responsible for making decisions on how to mitigate any financial losses.

Molly, Sales: Molly will be involved since the company's ability to sell its products and services may be affected by the loss of IT services. She will be responsible for making decisions on how to communicate with customers and suppliers during the crisis.

Fred and George, the Site Managers: Fred and George are responsible for ensuring the continuity of business operations and communicating with employees at each store and will need to attend the emergency meeting.

IT Staff: IT staff will be responsible for the restoration of the IT services and data. They should be briefed on the situation during the emergency meeting.

## Application Profile

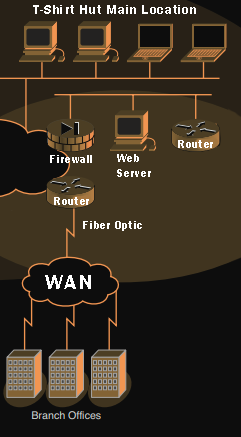
| **Application Name** | **Purpose** | **Recovery Point Objective (RPO)** | **Recovery Time Objective (RTO)** |
| --- | --- | --- | --- |
| **Screen Printer** | Managing inventory, employee schedules, and customer orders. | 0. Any data loss would cause significant business disruption. | 4 hours or less. The company needs to quickly restore this to resume operations. |
| **Amazon, eBay and Etsy** | Online selling portals for the company's products and services. | 1. The company can handle some data loss | 6 hours or less. Need to make money! |
| **Microsoft Office Applications** | Document creation and editing software | 2. Documents are pretty important, so don’t lose too many! | 8 hours or less. The company requires documents to function! |

# Hardware Profile

| **Device** | **Description** | **Redundancy Recommendations** |
| --- | --- | --- |
| **Employee Desktop** | In addition to facilitating employee work, employee desktops provide access to company applications and documents. | The use of a virtual desktop setup would allow employees to access their desktops remotely in case of an outage. |
| **Point of Sales Terminals** | This type of terminal is used to conduct transactions at the store and is essential to the revenue of the company. | The POS terminals can be made more reliable through backups, failovers, mirrored services and multiple pathways. |
| **Servers** | Responsible for running the database for Screen Printer, remote desktop sessions, and storing employee documents. | Failover mechanisms can enhance server reliability by allowing a backup server to take over when the primary fails. |

# Communications

The network design should connect all three locations together using a robust and reliable network, such as a fiber-optic connection. This will provide multiple pathways for data and ensure that connectivity is maintained during a disaster.



At the central office, there should be a firewall to secure the network and a router to manage the network traffic. The servers and employee desktops should be connected to the network through a switch. At each branch office, there should be a router to connect the office to the central office and a switch to connect the employee desktops and POS terminals to the network. To make communication more robust, the company should implement a Wide Area Network. This WAN will allow the branch offices to connect to the central office and ensure uptime at all locations.

## Backup Procedures

All important data, including the Screen Printer database, remote desktop sessions, and employee documents, should be backed up regularly and stored off-site. Automating and regularly testing the backup process should ensure that it is working properly and that all data is being backed up properly. Storing multiple copies of the backups in different locations is another excellent way to ensure that they are protected against disasters. Last but not least, encrypting the backups will ensure that they are protected against unauthorized access, (Emergency Preparedness for Business, n.d.).

## 

## Relocate and Rebuild

Response to an emergency: The first step is to activate the incident management plan, which requires contacting the appropriate personnel, including key employees and IT staff, and activating a communication plan for informing customers and suppliers of the situation.

Relocate to recovery site: The company should swiftly migrate its servers, applications, and personnel to the pre-established recovery site.

Data recovery: Once the backups have been recovered, the company should focus on restoring its data.

Rebuild: After the data has been recovered, the company should begin the process of rebuilding its IT systems and applications at the recovery site.

Resume operations: The company may temporarily resume operations at the recovery site once the IT systems and applications have been successfully rebuilt.

Return to primary location: Following the cleaning and restoration of the primary location, the company may resume operations there.

## Testing the Plan

Regular testing: To ensure effectiveness and familiarity with the disaster recovery plan, it should be tested on regularly.

Review and update: Disaster recovery plans should be reviewed and updated regularly to ensure they remain effective and take into account any changes in the company's operations or IT infrastructure.

Simulation: To identify and correct any weaknesses in the company's disaster plan, a simulation should be conducted of a disaster scenario.

Auditing: A periodic audit from a third party should be conducted to evaluate the disaster recovery plan and suggest improvements.

**References**

*Emergency Preparedness for Business*. (n.d.). The Hartford. <https://www.thehartford.com/claims/business-emergency-preparedness>