****

**ITT-306 Company Systems Disaster Relief Plan**

# Austin Johns

# 31 January 2021

# Professor Kris Peters

# ITT-306

# Directions:

# Read the description of the company’s IT assets, software, physical locations, and key employees.

# Complete the following 7-point plan for ensuring that IT systems will continue operating in case of an interruption event.

# Section 1: Personnel

In case of the loss of IT services, what employees do you recommend be called into an emergency meeting? Justify your selection.

In the case of the loss of IT services, it’s important to get them back up and running. As the company is heavily online-based because of the number of online orders and the remote desktop connection runs the entire business. Therefore, the personnel recommended to handle this issue would be the CEO Norma, Fred, and George. Norma is an important role in this situation because, although she has little experience with IT, she must have the crucial points of contact for these issues. If extra help needs to be called in, she would be the communicator. Next, Fred and George are important roles in this situation because they are constantly working with the system. Most likely, they have worked with system bugs and found their way around the systems in the past. Therefore, these three are the right people to get the fixing started.

# Section 2: Application Profile

Using the table below, list the key business system applications and identify the purpose for each. Then, determine the Recovery Point Objective (RPO), how far back does a data system data need to be restored as well as the Recovery Time Objective (RTO), how quickly the system needs to be restored. Consider the following:

| **Application Profile** | | | |
| --- | --- | --- | --- |
| For each application in use at the company, describe its purpose and the estimated downtime tolerance in terms of RPO and RTO. How much downtime can the business tolerate? RTO How much data history loss can the business tolerate? RPO | | | |
| **Application Name** | **Purpose** | **Recovery Point Objective (RPO)** | **Recovery Time Objective (RTO)** |
| Screen Printer | Project management software. Handles inventory, schedules, and orders. | Beginning of loss of IT service | Requires internet connection, time taken to regain internet access. |
| Windows Server 2019 | To manage and maintain servers and data structures | When servers stop responding/the beginning of when data is lost | Time taken to restore or recover lost data |

# Section 3: Hardware Profile

| **Hardware Profile**  What are the critical pieces of hardware that operate the computer system?  What systems can be made more reliable through backups, failovers, mirrored services, multiple pathways, and failure resistance? | | |
| --- | --- | --- |
| **Device** | **Description** | **Redundancy Recommendations** |
| **3 Servers** | **Used to run screen printer, remote desktop services, and store documents** | **Multiple pathways and regularly scheduled backups would help with the reliability of the system’s connection and mitigate any possible loss of data.** |
| **Document Server** | **Used at each of the three locations to store business documents** | **A regularly scheduled backup of this system would mitigate any possible data loss.** |
| **Windows 10 PCs** | **Used as point-of-sale terminals and employee computers.** | **A failover system for these computers would be useful in the event of a temporary shutdown so business could continue.** |

# Section 4: Communications

Create a diagram of the network design this company needs. Take into consideration the central office, internet connectivity, and branch offices. Describe the components you recommend in the plan that would make communication more robust.

Diagram, Teams

Description automatically generated

To make the communication more robust, the backup is included for all parts of the system. The goal of creating a backup for each part of the system is to help mitigate the loss of data in the event of a failure. Furthermore, a failover is included in all POS computers with the goal of continuing consistent service during a failure. If the system were to fail, the failover system would recover the failed part of the system to retain service capabilities.

# Section 5: Backup Procedures

What is the current backup or data protection process?

From the provided information about the company, there is currently no backup process. For data protection, the data is transferred to a server for local safekeeping. However, there are no network protections included in the data transfer.

What changes to the current backup process would you make to ensure its effectiveness?

Multiple changes are necessary to secure the data transfer and to ensure that all data is stored safely. To begin, during a data transfer during a sale or document creation, the data being transferred must be encrypted using a private key. Once the data is safely delivered to the server, the data can be decrypted for storage. Furthermore, the data on each server must be regularly backed up on a reliable schedule. The company will need to purchase a local-only data storage device to store data every 12 hours. The data must be backed up every 12 hours to allow for the shortest and most realistic recovery point objective.

# Section 6. Relocate and Rebuild

Describe the process you would recommend in the case of the complete destruction of a site, evacuation, or natural disaster.

In the event of a disaster or complete failure, the company must first determine where the event is taking place. If it is a server issue, the company may need to restore the server from the local backup. If it is a connection issue, the company may need to contact the internet service provider to solve the issue. If it is a POS issue, the company may need to restore the individual computer from a backup or contact Screen Printer to debug the issue. In the case of a more drastic event, like total loss of service or a natural disaster, the company would need to replace any defective or damaged equipment and restore these equipment from a backup.

# Section 7. Testing the Plan

# What steps would you take to ensure that the plans you describe are effective?

To ensure that all above steps of the plan are effective, there must be a high level of quality control and attention to detail. For example, in the event of loss of data, it would require a high level of attention to detail to determine when exactly the loss of data took place. Then, if the loss of data was identified more than 12 hours after the first event, any possible data would need to be restored from a backup. Furthermore, there must be great quality control in this situation. For the store managers, they must create a culture of good IT quality in their stores. If the employees are taking good care of their devices and making good decisions when storing data, there will be fewer human-caused disasters.