Policy Statement (1-2 paragraphs)

First, detail how the business would be affected in the event of a disastrous threat.

In the event of a disastrous threat, the business would be affected severely as there have been High Turn-over of employees, employees working off-site, employees using the guest network to conduct business.

What are the main objectives of the Disaster Recovery plan for GeldCorp?

Our main objectives are to conduct employee Security Training (i.e. Tailgating, not clicking non-office email links, not using the guest network, working from the office, and not from home unless required (requires CISO approval) their access would be limited, removing Administrative Privileges from all non-essential personal)

Ensure that company data can only be accessed via a wired connection and not via a wifi connection (company intranet) A Wifi connection should only be established via CISO and the ability to change/view data would be restricted.

Due to the High Turnover Rate

1. Remove User Names/Passwords (Access) upon termination
2. Deny Access to Network upon leaving
3. Instruct employees to change their current password to new more secure one to prevent former employee access
4. Have Security Walk former employee out of the building

Moving the Server to a singular location can be only accessed from a singular direction. (accessible with CISO approval only)

Pending on budget available setup a Hot/Warm/Cold Site to protect data in case of disaster

Plan Overview

Indicate the following. You do not need to do a thorough BIA analysis, so be creative using what we have learned so far about GeldCorp.

MTD for information systems.

6 Days

RTO for information systems.

4 Days

RPO for information systems (i.e frequency of data and other systems backup)

Every 2 Days

What are the backup strategies that should be implemented?

Appoint (placeholder) in case a disastrous logical/physical event occurs, maintaining business operations.

Also, include necessary details for at least one of the following that senior management will need to be aware of. What should the activation procedures be?

Cold Site

Barebones server setup on a different location/Mobile recovery center, Workers can have a Work-From-Home policy in case of environmental disaster and office is rendered unusable to maintain business continuity.

Warm Site

Have backup drives, hardware with backup information, and officer-ware in case of physical/logical disasters for easy replacement.

Hot Site

Cloud storage solution for data backups has the same setup and architecture of the office in a different location for rapid deployment.

Explain how the business should prioritize its resources to recover from the reputation and operational damage of a catastrophic loss. Include any other people from the company you feel should be involved in this.  
  
Have a page setup displaying information and announcing downtime and why HR should send an email on how employees should proceed regarding business continuity. The business should focus its resources on maintaining services for consumers and company reputation.  
  
  
  
  
  
Plan Implementation and Testing

What will you need to do to implement your Disaster Recovery plan? Who are the

relevant stakeholders, who should be involved?

To implement our Disaster Recovery Plan we would need Human Resources, CFO, CISO, and the CEO.

We would need the CEO to approve any changes that we wish to implement.

We would need the CFO to approve a budget for the changes.

We would need Human Resources and CISO to conduct Security Training sessions and better computer practices with the employees.

We would need the CISO to manage the deployment of Hot/Warm/Cold sites, the moving of servers to a more secure location, and having his/her team conduct improved CyberSecurity checks.

Consider specifically how you will train your employees and how you will test critical

details of the plan.

Leverage your learnings in developing a training plan for the Security Culture Framework

exercises to help inform training and implementation for your DR plan.

Have Disaster Recovery training every 6 months for all involved employees, Have random drills and tests every year, making sure hardware backups, cloud backups, and running hardware and software are functional and being maintained.