



Business Continuity Policy

Ensuring Resilience and Recovery

This policy outlines our approach to business continuity and disaster recovery.

Table of Contents

1. Introduction.....	2
2. Scope and Objectives.....	2
2.1. Scope.....	2
2.2 Objectives	3
2.3 Critical Functions.....	3
2.4 Risk Assessment.....	3
2.5 Recovery Strategies	4
2.6 Testing and Maintenance	4
2.7 Emergency Response	5
2.8 Recovery Procedures.....	5
2.9 Communication Plan	5
2.10 Training and Awareness.....	5
2.11 Plan Update And Maintenance	6
3. Recovery Procedures.....	6
3.1 IT Systems Recovery.....	6
3.2 Customer Service Recovery.....	7
3.3. Recovery Priorities	11
3.4 Roles and Responsibilities.....	15
3.5. Training and Testing	20
4. Appendices	30
Appendix A: Emergency Contact List.....	30
Phone Tree Backup.....	31
Appendix B: Emergency Contact List.....	31
5. Next Update.....	31



1. Introduction

Document Title	Business Continuity Plan
Version	1.0
Date	14.05.2025
Reviewer	Jean Pierre Hartl
Date Approved	2025-03-14

This section provides an overview of the business continuity plan.

- The plan outlines procedures for maintaining business operations during disruptions.
- It includes roles and responsibilities for key personnel.

2. Scope and Objectives

This section defines the scope and objectives of the business continuity plan.

- Ensure critical business functions can continue during disruptions.
- Minimize the impact of disruptions on business operations.

2.1. Scope

The scope of this plan covers all critical business functions.

- IT systems and infrastructure
- Customer service operations
- Financial operations



2.2 Objectives

The objectives of this plan are to ensure business continuity.

- Maintain critical business functions during disruptions.
- Ensure timely recovery of operations.
- IT Minimize downtime
- Protect critical data
- Ensure communication channels remain open

2.3 Critical Functions

Critical business functions are.

- Customer service
- Financial operations
- IT infrastructure

Each critical function has a designated owner.

Recovery procedures are documented for each function.

2.4 Risk Assessment

This section outlines the risk assessment process:

- Risks are identified and evaluated based on their impact and likelihood
- Mitigation strategies are developed for high-risk scenarios
- Regular risk assessments are conducted
- Risk matrix is used to evaluate risks
- Mitigation strategies are reviewed annually



2.5 Recovery Strategies

This section details recovery strategies for critical functions:

- Recovery strategies are developed for each critical function
- Strategies are tested regularly to ensure effectiveness
- Backup systems are maintained
- Alternative work locations are identified
- Communication plans are established

2.6 Testing and Maintenance

This section covers testing and maintenance procedures:

- Regular testing ensures the plan remains effective
- Maintenance procedures keep the plan up to date
- Annual testing of recovery procedures
- Quarterly review of contact information
- Monthly backup testing

Test Type	Frequency	Responsible Party
Full Recovery Test	Annually	IT Department
Contact List Review	Quarterly	HR Department
Backup Testing	Monthly	IT Department

Training is provided to all staff.



2.7 Emergency Response

Emergency response procedures are activated immediately upon detection of a disruption:

- Assess the situation
- Key personnel are notified according to the contact list
- Activate emergency procedures

2.8 Recovery Procedures

Detailed procedures for restoring critical functions, e.g. for IT systems:

- Restore from backups
- Verify system functionality
- Document recovery process

2.9 Communication Plan

Clear communication is essential during disruptions:

- Communication channels are established for different scenarios
- Internal communication via e-mail, team meetings, status updates

2.10 Training and Awareness

Regular training ensures staff are prepared for disruptions and inform them about their roles:

Training Type	Frequency	Participants
General Awareness	Annually	All Staff
Role-Specific	Quarterly	Key Personnel
Emergency Procedures	Monthly	All Staff



2.11 Plan Update And Maintenance

Maintenance of the Business Continuity Plan is the responsibility of the VP of Technology & special projects. The Phantom Compliance Business Continuity Plan will be distributed to the following departments and/or individuals:

Team	Title	Location	Person Responsible
Executive	Chief Operating Officer	Calgary	Manny Bains
Operations	Operational Compliance	Edmonton	Alex Beisel

3. Recovery Procedures

This section outlines recovery procedures for critical functions.

3.1 IT Systems Recovery

This section details IT systems recovery procedures.

Staffing

This section outlines staffing requirements during disruptions.

- Plane crash or other accident with key staff impacted
- Major transit incident prevents staff from accessing office(s)
- Flu, or similar, epidemic strikes
- Employees go on strike
- Key staff quit/are terminated without succession planning



Infrastructure

This section details infrastructure requirements.

- Building fire at primary office(s)
- Incident leads to loss of power in one or more location
- Potential gas leak at primary office(s)
- Theft of office hardware including computers and telephony
- Third party service providers suffer a critical event/outage
- Disgruntled employee damages or sabotages equipment
- Disgruntled employee assaults or kills other staff
- Civil unrest or terrorism damages the building or impedes access to it
- Access to internet is lost either at primary office or broadly

Data Management

This section covers data management procedures.

- Theft of all employee's personal information
- Data breach/compromise
- Data security/system intrusion event

3.2 Customer Service Recovery

This section outlines customer service recovery procedures.

3.2.1 Communication Plan

This section details the communication plan for customer service.

It also helps to highlight the gaps that may limit Phantom in achieving optimal recovery in the event of a business disruption, while identifying those resources required to resume operations speedily. BIA provides the Management of



Phantom with the information to devise a recovery strategy and recovery prioritization. It also provides supporting data to define an appropriate Disaster Recovery program budget.

Below is the list of parameters covered in the BIA:

- Identifies the critical processes and dependencies within an organization.
 - Internal – IT systems, suppliers, customers, shareholders.
 - External – government departments, regulators, trade bodies, competitors.
- Evaluates recovery priorities and time scales.
- Determines the criticality of each function to business survival.
- Assesses the potential cost of the disaster.
- Direct and indirect costs of loss of service capability.
- Identifies the high-risk areas of the existing infrastructure
- Identifies the Single points of failure
- Recovery time limitations (For IT systems in particular)

3.2.2 Customer Support

This section outlines customer support procedures.

The three potential risk factors that will be addressed include Natural and environmental threats, Man-made threats and Technical Threats. The resultant exercise will produce the following in a clearly documented format:

The diagram below known as (Risk Matrix) illustrates the appropriate form of Risk Management for different combinations of frequency and severity of the damage.

- Register potential threats.
- Identify essential operations that must be restarted as quickly as possible after a disaster has taken place.
- Identify cost-effective measures that could be introduced to prevent risks or lessen their impact, and
- Provide input for managing risk



Likelihood	Severity				
	Insignificant	Minor	Moderate	Major	Significant
Certainty					
Highly Likely					
Likely					
Unlikely					
Highly Unlikely					

Risk Definition	Low Risk	Medium Risk	High Risk
Colour Code			

3.2.3 Service Level Agreements

This section covers service level agreements.

- Constituting various Emergency Response teams in the event of a disaster.
- Determining an internal contact command tree; and defining emergency evacuation processes for staff.
- Defining and equipping alternative work locations for staff.
- Classification of staff based on priority to initiating and completing processes identified in the BIA
- Internal and external resource management (including third party services) for the speedy resuscitation of time-sensitive processes for crisis communication and incident management.



3.2.4 Recovery Time Objectives

This section outlines recovery time objectives.

The qualifying criteria for determining the criticality of these processes/services and their recovery needs include but are not limited to the following:

- The data, processes and services required for continuing the business functions.
- Services dependent on External Sources and Vendors.
- Dependency on other Business activities and their extent.
- Annual Maintenance Contracts (AMCs) and Service Level Agreements (SLAs) for continuity of Business Functions.
- System Backup Requirements.
- Resource requirements to meet recovery needs.

The Recovery of these functions is quantified in terms of:

Recovery Time Objective (RTO)

This is the maximum permissible outage time after which the function must be back in operation.

Recovery Point Objective (RPO)

This is the furthest point to which data loss is permissible. The Recovery Point Objective (RPO) determines what proportion of data under threat can be recovered.

3.2.5 Recovery Point Objectives

This section details recovery point objectives.

Function	Name	RTO
Tier 1	Critical Functions or Business	1 to 3 hours
	Impact Rating	Massive or Major



Tier 2	Essential Functions or Business	24 to 72 hours
	Impact Rating	Moderate
Tier 3	Desirable Functions or Business	Not exceeding 120 hours
	Impact Rating	Minor

3.2.6 Testing Procedures

This section outlines testing procedures.

Function	Name	RPO
Tier 1	Critical Functions or Business	90% within 1-3 hours and
	Impact Rating of Massive/Major	100% within a day
Tier 2	Essential Functions or Business	90% within 24 hours and
	Impact Rating of Moderate	100% within 72 hours
Tier 3	Operations	50% within 24 hours and
	Desirable Functions or Business	100% within 120 hours

3.3. Recovery Priorities

This section outlines the testing frequency for the business continuity plan.

3.3.1 High Level Priorities

- Ensure all employees/staff present at the site are accounted for and, where possible, safe
- Notify all relevant parties including:



- Onsite employees
- Remote employees
- Management and executives
- Key staff employed by related entities
- Local emergency response staff where necessary
- Clients affected
- Building/site management staff
- Assess impact of the disaster:
 - Can backup locations be accessed and used to mitigate impact?
 - Has anyone suffered physical injury or death as a result of the incident?
 - Any client/staff/customer data stolen or compromised?
 - Has this incident impacted third party service providers such as Slack, Google, or processing banks?
 - If key staff are unaccounted for or deceased can their job functions be carried out by a designated second?
 - If partner banks suffer an incident, the same or unrelated, that is critical to their services the recovery time objective may not be met
- Are any members of the ERT affected? Can a second fulfill the role?
- Identify the Emergency Response Team (ERT)
 - Is the ERT available and trained for the scenario?
 - Has communication with relevant parties been successful?
- Identify the correct response:
 - Where infrastructure is affected can teams/staff work from backup location(s)?
 - What mitigating/remediating steps are contained within the plan?
- Carry out the incident response plan
- Confirm that critical services have been restored
- Restore remaining outstanding services



3.3.2 Relocation Strategy And Alternate Business Sites

- In the event of a disaster or disruption to office facilities the strategy is to recover operations by relocating to alternate business sites. Short term strategies (for disruptions lasting 2 weeks or less) which have been selected include:

Primary Location	Alternate Business Site
Unit 410 Bow Valley Square 3, 255 5 Ave SW, Calgary AB T2P 3G6	Employees to work from home

- In the event of a long-term disruption the short-term strategies/locations above will be employed until such time as a new office space similar in size and location to the one destroyed can be located.
- Where employee homes have been impacted/are not accessible an appropriate location will be determined

3.3.3 Recovery Plan Phases

Activities required to recover from a facilities disaster are divided into four chronologically sequential phases:

- Disaster Occurrence
 - This phase commences with the occurrence of a disaster event and continues until management activates the recovery plan. Major activities in this phase include:
 - Emergency response measures
 - Notification of all relevant parties
 - Damage assessment
 - Declaration of disaster



- Plan Activation
 - In this phase the Business Continuity Plans of individual teams are enacted. This phase will continue until such time as fallback locations are occupied, critical business activities have resumed, and Phantom Compliance staff have resumed business as usual. Major activities in this phase include:
 - Notification and assembly of recovery team
 - Implementation of interim procedures
 - Relocation to backup sites
 - Re-establishment of communications
- Alternate Site Operations
 - This phase consists of the duration of time that business operations are conducted from the fallback/alternate locations. Primary recovery activities in this phase include:
 - Transition to Primary Site
 - This phase includes any and all remaining activities to resume business functions at the primary office location

3.3.4 Vital Record Backup

- All vital records and business information is maintained and stored in servers administered by Google. Google maintains data centers in numerous locations throughout the world ensuring that location risk is minimized, and the impacts of any local disasters are mitigated. Similarly, email and drive storage are provided by Google and maintained in the same fashion.
- Where physical records are produced within the normal course of business during a disaster these records will be transported to the primary business location at close of disaster by the employee that produced them. All business



records are subject to organizational confidentiality and document retention practices.

- Employees are expected to use cloud and communal storage for documents to mitigate risks of hardware loss or inaccessibility.

3.3.5 Online Access To Phantom Compliance Systems

- Systems are maintained and stored on cloud servers with multiple backups. Staff should be able to access systems as normal from their own home machines or laptops provided by IT in the event of a disaster. Where a key staff member of Phantom Compliance is unable to perform their regular duties as a result of the disaster their designated second will perform these duties remotely from their homes or a backup location if the disaster is global in scope.
- If a 3rd party software product goes offline and is required for Business Critical services, backup providers are listed in Appendix B. This list assumes that client's customer data is available through Google, Dropbox or other file sharing services and clients maintain their own backup of this data as required.

3.3.6 Mail And Report Distribution

- Communication will continue via slack and email if available, otherwise by SMS or phone calls.

3.4 Roles and Responsibilities

This section outlines the roles and responsibilities of team members during a business continuity event.



3.4.1 Purpose And Objective

- This section outlines who participates in the recovery process for Phantom Compliance Business Continuity Plan. The Team Leader oversees coordinating efforts, delegating tasks to the team members, and assisting team members as required. Further, the Team Leader reports to executives as required regarding ongoing status and expected timeframe for resumption of normal business activities.

3.4.2 Roles, Responsibilities & Contact Information

- **Chief Operating Officer & special projects:** responsible for coordinating the recovery effort, notifying the executives of situation status and relevant updates, delegating tasks to team members, and assisting with performing tasks as required
 - **Information Technology Recovery Team**
 - The Information Technology Team(s) has its own disaster recovery policy that covers physical disasters as well as data security related events. At a high level, their responsibilities include:
 - Activating the Incident Response Plan
 - Mobilizing and managing IT resources
 - Co-ordinating any communications with technical service providers such as cloud servers, data warehouses, telephony, PC, LAN support, and other technology related vendors
 - Assisting with acquisition and installation of equipment at recovery and backup sites
 - Participating in the testing of new/backup systems and networks
 - Coordinating telephone and network setup at backup locations
 - Keeping Leadership Team apprised of recovery status



- **Business Continuity Coordinator and Team Leader**

- Liaising with the Leadership Team to officially declare a disaster and commence enacting this plan and act as the point of contact for management until disaster is declared over
- Assist in the development of any required statements to media, public outlets, and clients
 - Note that statements may be made by the CEO or staff specified by the CEO only
- Monitor the progress of business continuity efforts on a daily basis
- Report on progress to all staff on a daily basis
- Liaise with, and coordinate efforts between, various team leaders as required
- Ensure an accurate record of all disaster related expenses is maintained and preserved

- **Communications**

- Preparing any communications and status updates intended for an external audience with the CEO's guidance and approval
- Coordinating the distribution of updates and communications to:
 - Vendors
 - Clients
 - Media
 - Government bodies
 - Regulatory agencies
 - Insurance companies
 - Other stakeholders

- **Human Resources**

- Providing information regarding the disaster and recovery efforts to employees/their immediate families as required



- Arranging for cash advances/expenses coverage if travel is necessary
- Notifying designated emergency contacts of employee injury or fatality
- Processing life and health insurance claims

- **Administration**

- Ensuring adequate supplies are available to the recovery team
- Assisting with clerical tasks and errands as required
- Arranging any necessary employee travel
- Tracking costs and expenses as they relate to recovery efforts
- Contacting vendors to arrange for site repairs
- Taking action to safeguard physical assets from further damage
- Co-ordinating the removal of furniture, documents, supplies and other physical materials as required
- Supervising salvage and clean up activities
- Assisting with relocation to backup sites
- Coordinating relocation to primary site when possible
- Where necessary, ensuring lodging and food is available to recovery personnel
- Notifying postal service of forwarding addresses

- **Emergency Response Team**

- Safety of employees
- Where possible inspecting physical structures and assessing damage
- Preparing and amending impact assessment documents
- Providing Leadership Team with damage assessment reports and recommendations

- **Account Management:**

- **Backup Team Leader**

- The Backup Team Leader should be familiar with the plan and able to take on the tasks of the Team Leader should they be incapacitated or otherwise unavailable due to the disaster



- The Backup Team Leader is expected to take a lead role in teams and assist the Team Leader with preparation and distribution of reporting, preparation of backup locations, and transporting of records as required
- The Backup Team Leader may be responsible for overseeing and reporting on one or more of the recovery functions
- **Team Member**
 - The Team Member is an employee of Phantom Compliance that is designated to participate in the recovery effort
 - The Team Member is expected to take direction from the Team Leader(s), perform normal job duties, and prepare summaries of work completed as required
 - Team Members are not expected to report to the Board/executive on activities and status in the event of a disaster

3.4.3 Personal Notification

- Communication will be conducted via telephone and email using the details noted in Appendix A – Employee Contact List. In general, the Emergency Response Team Leader will notify department heads and team leaders and they will notify their staff in turn. The phone tree is noted in Appendix A and is tested quarterly.
- Further, a backup communication tree is listed in Appendix A should phone lines be unavailable.

3.4.5 External Contacts

- Emergency contact lists will be prepared and updated as warranted by the Team Leader. This list will include all key external contacts and include both daytime and emergency contact information. This list will be distributed amongst all team members (EMT and ERT) and available in the shared drive for all to review.



3.5. Training and Testing

This section outlines the training and testing procedures for the business continuity plan.

3.5.1 Purpose And Objective

- This section contains activities and tasks that may be employed/required in the recovery process to restore business-critical functions of Phantom Compliance. The procedures are organized according to the type of disaster scenario that has occurred. In general, the activities are assigned to teams and teams may, at their discretion, assign tasks to their employees as needed.
- In general tasks and activities are presented in the order in which they should be completed. Staff should familiarize themselves with this plan, however it is recognized that disaster scenarios are rarely uniform and as such some deviation from the plan is expected. Personal and team safety is the number one priority in any scenario and should not be foregone in favor of adherence to this plan.

3.5.2 Disaster Scenarios

- **Staffing Scenarios**
 - **Disaster Occurrence:**
 - Loss of key staff to illness, death or termination of employment
 - **Recovery Time Objective:** 1 – 2 business days
 - **Activity: Confirm employee(s) are not able to work**
 - **Activity Performed At:** Primary Office Location or at Employees Home
 - **Activity Performed By:** Business Continuity Coordinator



- Where a travel accident has occurred, confirm the employee is dead/incapacitated via contact with the airline/rail line/local law enforcement/hospital
- Inform HR to notify employee emergency contact
- Where possible, speak with the employee directly and obtain first-hand information regarding the duration of illness/incapacity
- Where an employee has quit/been fired – Confirm to disable all system access
- **Activity: Declare Disaster**
 - **Activity Performed At:** Primary Office Location or at Employees Home
 - **Activity Performed By:** Business Continuity Coordinator
 - Advise leadership team of disaster via phone/email
- **Activity: Locate Designated Backup Employee**
 - **Activity Performed At:** Primary Office Location or at Employees Home
 - **Activity Performed By:** Business Continuity Coordinator
 - Contact employee's direct supervisor or second in command
 - Advise them of employee loss
 - Advise them to activate their departmental disaster recovery plan
- **Activity: Identify What Job Role Documentation Exists**
 - **Activity Performed At:** Primary Office Location
 - **Activity Performed By:** Business Continuity Coordinator OR Employee Direct Supervisor
 - Consult team drive for any relevant processes and procedures
 - Ensure that external contact list is maintained and updated
 - Introduce designate to external/3rd party contacts
- **Activity: Ensure that Job Duties Continue with Minimal Interruption**
 - **Activity Performed At:** Primary Office Location
 - **Activity Performed By:** Business Continuity Coordinator OR Employee Direct Supervisor



- Follow up with internal and external stakeholders to ensure tasks are completed as normal
- Follow up with backup employee on a regular basis to ensure workload is manageable and their own duties are not impacted
- Liaise with direct supervisor to ensure non-critical and junior tasks of backup employee are reassigned or ceased until disaster over
- **Activity: Begin Succession Plan or Recruitment**
 - **Activity Performed At:** Primary Office Location or at Employees Home
 - **Activity Performed By:** Business Continuity Coordinator OR HR Manager
 - Promote internally or place job ads
 - Where a new hire is required follow standard HR procedure for recruitment
 - Initiate training for new role
- **Activity: Declare Disaster Over**
 - **Activity Performed At:** Primary Office Location or at Employees Home
 - **Activity Performed By:** Business Continuity Coordinator
 - Notify executives that disaster over
- **Infrastructure Scenarios**
 - **Disaster Occurrence:**
 - Loss of use of the primary office location or employees home due to fire, power outage, employee theft/sabotage, or human related impedance of access (terrorism, civil unrest, transit strike)
 - **Recovery Time Objective:** 1 – 2 business days
 - **Activity: Confirm Primary Location Inaccessible**
 - **Activity Performed At:** Primary Office Location OR Employee Homes
 - **Activity Performed By:** Business Continuity Coordinator
 - If on site at time of disaster, evacuate the building in as calm and fast a manner as possible



- Where possible and safe to do so physically sight the location, confirm the normal office location is not safe for employee access
- Inform local emergency services where applicable
- Where possible, speak with any staff present at time of issue, confirm they are safe and able to reach home/a safe place
- Contact building/facilities management for further information
- **Activity: Declare Disaster**
 - **Activity Performed At:** Primary Office Location OR Employee Homes
 - **Activity Performed By:** Business Continuity Coordinator
 - Advise executives, board, and staff of disaster via phone/email
 - Confirm that employees are safe and accounted for
 - Where injury or fatality has occurred notify HR to advise emergency contacts
- **Activity: Confirm Backup Location(s) Are Accessible**
 - **Activity Performed At:** Primary Office Location OR Employee Homes
 - **Activity Performed By:** Business Continuity Coordinator
 - Contact staff and ascertain whether or not they can work from home
 - If staff cannot work from home contact Team Leaders to facilitate temporary coverage of duties
 - Confirm that staff have sufficient hardware to access systems and perform their jobs
 - Provide backup machines as necessary
 - Track expenses and report them to Finance
- **Activity: Confirm 3rd Parties Are Not Impacted**
 - **Activity Performed At:** Primary Office Location OR Employees Homes
 - **Activity Performed By:** Business Continuity Coordinator or Executive
 - Contact bank partners, vendors, and clients to assess impact of disaster on their operations



- Where the disaster has impacted banking partners notify Leadership Team
- Contact IT to obtain status of systems/data/servers
- Note any projected impacts to daily status reports
- **Activity: Ensure that Critical Functions Continue with Minimal Interruption**
 - **Activity Performed At:** Designated Backup Location(s) OR Employee Homes
 - **Activity Performed By:** Business Continuity Coordinator and Emergency Response Team
 - Follow up with internal and external stakeholders to ensure tasks are completed as normal
 - Notify executive of progress on a daily basis
 - Contact clients to confirm service is provided as normal
 - Produce reporting for Business Continuity Coordinator
 - Ensure that expenses are tracked and faithfully reported
 - Continue until such time as primary location or suitable replacement is available
- **Activity: Begin Transition Back to Primary Location OR Replacement Location**
 - **Activity Performed At:** Primary Office Location OR Replacement Location
 - **Activity Performed By:** Business Continuity Coordinator & All Staff
 - Transfer any hard copy records produced during disaster back to primary office per confidentiality and document retention policies
 - Confirm vendors and 3rd party partners are not experiencing current interruptions
 - Resume business as usual
 - Track performance carefully and escalate any issues
- **Activity: Declare Disaster Over**
 - **Activity Performed At:** Primary Office Location OR Employees Homes



- **Activity Performed By:** Business Continuity Coordinator
 - Notify executives and board that disaster over
- **Data/Server/Technology Scenarios**
 - **Disaster Occurrence:**
 - Event occurs that compromises the security, availability, or physical integrity of client data and/or production servers
 - **Recovery Time Objective:** 1 – 2 business days
 - **Activity: Confirm Disaster Occurrence**
 - **Activity Performed At:** Primary Office Location OR A Designated Backup Location
 - **Activity Performed By:** Business Continuity Coordinator
 - Contact CTO or IT team designate and confirm issue has occurred
 - Telephone is the preferred method of communication as other systems may be compromised/unavailable
 - **Activity: Declare Disaster**
 - **Activity Performed At:** Primary Office Location OR A Designated Backup Location
 - **Activity Performed By:** Business Continuity Coordinator OR Chief Technical Officer
 - Advise executives, and staff of disaster via phone/email
 - Advise all staff to change passwords on external accounts (banking, payment processing, email, fraud systems, data brokers) from a secure location
 - **Activity: Confirm Backup Location(s) Are Accessible**
 - **Activity Performed At:** Primary Office Location OR A Designated Backup Location
 - **Activity Performed By:** Business Continuity Coordinator
 - Contact facilities management at backup location
 - Contact staff and ascertain whether or not they can work from home



- If staff cannot access backup location OR work from home contact Team Leaders to facilitate temporary coverage of duties
- Staff are not to carry out any job functions or otherwise access/modify systems until IT has confirmed incident resolution
- **Activity: Track Progress with IT**
 - **Activity Performed At:** Primary Office Location OR A Designated Backup Location
 - **Activity Performed By:** Business Continuity Coordinator or Executive
 - Stay in contact with IT to track issue progress
 - Note that IT has their own disaster recovery and incident response processes, Operational teams can assist as necessary to support the IT team
 - Track and report on all expenses
- **Activity: Ensure that Critical Functions Resume with Minimal Interruption**
 - **Activity Performed At:** Designated Backup Location(s) OR Employee Homes
 - **Activity Performed By:** Business Continuity Coordinator and Emergency Response Team
 - Resume business as usual when notified issue resolved by IT
 - Follow up with internal and external stakeholders to ensure tasks are completed as normal
 - Notify executive of progress on a daily basis
 - Contact clients to confirm service is provided as normal
 - Produce reporting for Business Continuity Coordinator
 - Ensure that expenses are tracked and faithfully reported
 - Continue until such time as primary location or suitable replacement is available
- **Activity: Declare Disaster Over**
 - **Activity Performed At:** Primary Office Location



- **Activity Performed By:** Business Continuity Coordinator or Chief Technical Office
 - Notify executives and board that disaster over
- **Environmental Scenarios**
 - **Disaster Occurrence:**
 - Loss of use of the Primary Office Location or Employees Homes due to extreme weather, natural disaster, proximal nuclear/chemical/toxic events
 - **Recovery Time Objective:** 1 – 2 business days
 - **Activity:** Confirm Primary Location Inaccessible
 - **Activity Performed At:** Primary Office Location OR Employees Homes
 - **Activity Performed By:** Business Continuity Coordinator
 - Evacuate any on site staff in as safe and expeditious a fashion as possible
 - Where possible and safe to do so physically sight the location, confirm the normal office location is not safe for employee access
 - Inform local emergency services where applicable
 - Where possible, speak with any staff present at time of issue, confirm they are safe and able to reach home/a safe place
 - Contact building/facilities management for further information
 - **Activity: Declare Disaster**
 - **Activity Performed At:** Primary Office Location OR Employees Homes
 - **Activity Performed By:** Business Continuity Coordinator
 - Advise executives, board, and staff of disaster via phone/email
 - Confirm that employees are safe and accounted for
 - Where injury or fatality has occurred notify HR to advise emergency contacts
 - **Activity: Confirm Backup Location(s) Are Accessible**



- **Activity Performed At:** Primary Office Location OR A Designated Backup Location
- **Activity Performed By:** Business Continuity Coordinator
 - If staff cannot access backup location OR work from home contact Team Leaders to facilitate temporary coverage of duties
 - Confirm that staff have sufficient hardware to access systems and perform their jobs
 - Provide backup machines as necessary
 - Track expenses and report them to Finance
- **Activity: Confirm 3rd Parties Are Not Impacted**
 - **Activity Performed At:** Primary Office Location OR Employees Homes
 - **Activity Performed By:** Business Continuity Coordinator or Executive
 - Contact bank partners, vendors, and clients to assess impact of disaster on their operations
 - Where the disaster has impacted banking partners notify Executive
 - Contact IT to obtain status of systems/data/servers
 - Note any projected impacts to daily status reports
- **Activity: Ensure that Critical Functions Continue with Minimal Interruption**
 - **Activity Performed At:** Designated Backup Location(s) OR Employee Homes
 - **Activity Performed By:** Business Continuity Coordinator and Emergency Response Team
 - Follow up with internal and external stakeholders to ensure tasks are completed as normal
 - Notify executive of progress on a daily basis
 - Contact clients to confirm service is provided as normal
 - Produce reporting for Business Continuity Coordinator
 - Ensure that expenses are tracked and faithfully reported



- Continue until such time as primary location or suitable replacement is available
- **Activity: Begin Transition Back to Primary Location OR Replacement Location**
 - **Activity Performed At:** Primary Office Location OR Replacement Location
 - **Activity Performed By:** Business Continuity Coordinator & All Staff
 - Transfer any hard copy records produced during disaster back to primary office per confidentiality and document retention policies
 - Confirm vendors and 3rd party partners are not experiencing current interruptions
 - Resume business as usual
 - Track performance carefully and escalate any issues
- **Activity: Declare Disaster Over**
 - **Activity Performed At:** Primary Office Location OR Employees Homes
 - **Activity Performed By:** Business Continuity Coordinator
 - Notify executives and board that disaster over

3.5.3 Testing Frequency

- Work will be carried out initially offsite from the primary location to an alternative location such as the residential addresses of the employees in each office for a period of one week
- Phone tree and other communication methods tested quarterly
- To test the loss of key staff from the primary location, the day to day and critical functions of the roles will be carried out by the VP of Technology & special projects and the Financial Controller from their homes or office for a period of one week using employee manuals, policies and procedures already in place
- Results of the testing will be recorded in the first instance of determining whether it was possible for the key staff in the primary location to work from their residential location with the same level of access as they would have



from the primary location. Secondly, where the functions of the roles from the primary office have been passed on to the backup team, after the period of one week, all work will be checked over and analyzed to ensure it meets the normal standard of the work carried out from the key personnel in the primary location. Back up team can be found in Appendices

- Results will all be recorded within spreadsheets to confirm, advise or make recommendations whether the testing was successful or more needs to be done

4. Appendices

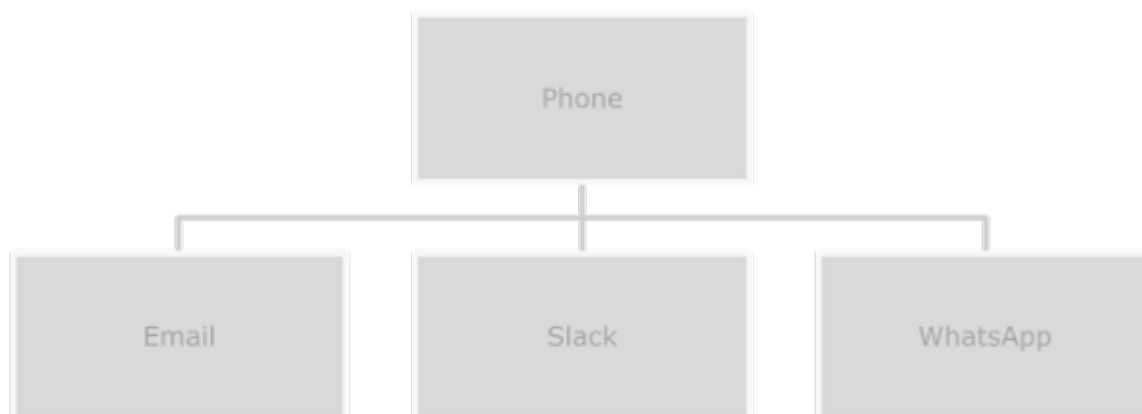
The following tables provide backup team information for disaster recovery scenarios.

Appendix A: Emergency Contact List

Ryan Mueller	Chief Executive Office	ryan@phantomcompliance.com	(403) 629-5763	(403) 473-8041
Manny Bains	Chief Operating Officer	manny@phantomcompliance.com	(403) 808-2267	
Kathy Chiu	Senior Administrator / Bookkeeper	kathy@phantomcompliance.com	(403) 831-2779	(587) 747-7976
Alexandria Beisel	Senior Compliance Analyst	atwilson+@live.ca	(204) 509-7670	
Emeka Nwaigbo	Senior Compliance Analyst	eemi4all@gmail.com	(587) 703-7893	
Michelle Matandani	Paralegal	simukaimatandani@gmail.com	(250) 619-7550	(587) 328-1422
Matthew Griffis	Compliance Analyst	matt.james142@gmail.com	(403) 829-4110	
Reia Gensaya	Social Media Ad Designer & Video Editor	reiagensaya@gmail.com	(09) 952-730699	



Phone Tree Backup



Appendix B: Emergency Contact List

The following tables provide backup team information for disaster recovery scenarios.

Function	Procedure	Responsible Party
IT Systems	Restore from backup	IT Department
Customer Service	Activate backup team	Customer Service Manager
Financial Operations	Switch to backup systems	Finance Department

5. Next Update

- 01-Feb-2026