Presbytery of Geneva Information Technology Disaster Recovery Plan

This document delineates the Presbytery of Geneva's policies and procedures for an Information Technology (IT) Disaster Recovery Plan, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of people, systems, and data.

Our mission is to ensure information system operation, data integrity and availability, and business continuity.

Policy Statement

- The Presbytery's comprehensive IT Disaster Recovery Plan shall be reviewed annually by the Personnel Committee and kept up to date to take into account changing circumstances.
- The IT Disaster Recovery Plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key activities.
- Staff must be made aware of the IT Disaster Recovery Plan and their own respective roles.

Objectives

The principal objective of the IT Disaster Recovery Plan program is to develop, test and document a well-structured and easily understood plan which will help the Presbytery recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and operations. Additional objectives include the following:

- The need to ensure that employees fully understand their duties in implementing such a plan.
- The need to ensure that operational policies are adhered to within all planned activities.
- The need to ensure that proposed contingency arrangements are cost-effective.
- Disaster recovery capabilities are applicable to staff, vendors and others.

Plan Overview

- **Plan Documentation Storage**

  Hard copies of the plan will be stored in secure locations to be defined by the Presbytery Personnel Committee. Each member of the IT Disaster Recovery Team will be issued a hard copy of the plan and be asked to keep it offsite.
- **Prevention and Backup Strategy**

  All attempts are made to prevent or limit the impact of a disaster on the information systems of our Presbytery. Key business processes and the agreed backup strategy for each are listed below. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site and the backup site.

KEY BUSINESS PROCESS	BACKUP STRATEGY
Operations	Fully mirrored recovery in off-site location and cloud
Finance and Human Resources	Fully mirrored recovery site in off-site location and cloud
Email	Fully mirrored recovery site in off-site location and cloud
Disaster Recovery	Fully mirrored recovery site in off-site location and cloud

Emergency Response

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

- **Key trigger issues that would lead to activation of the IT Disaster Recovery Plan are:**
  - Total loss of all communications
  - Total loss of power
  - Flooding of the premises

  - Loss of the building
  - Other situations as needed
- Plan Invocation **When an incident occurs, the IT Disaster Recovery Plan may be implemented to:**
  - Respond immediately to a potential disaster and call emergency services;
  - Assess the extent of the disaster and its impact on the Presbytery;
  - Decide which elements of the disaster recovery plan should be activated;
  - Establish and manage disaster recovery team to maintain vital services and return to normal operation;
  - Ensure employees are notified and allocate responsibilities and activities as required.
- **IT Disaster Recovery Team** members include:
  - Linda Badger Becker – Transitional Leader
  - Alicia Alvarez – Office Administrator
  - Rev. Val Fowler – Stated Clerk
  - Lea Kone – Camp Director
  - Russ Kinch – IT and Technology Consultant

  The team's responsibilities include:
    - Establish facilities for an emergency level of service within 1 business day or as soon as possible;
    - Restore key services within 1 business day of the incident or as soon as possible;
    - Return to business as usual within 1 business day after the incident or as soon as possible;
    - Coordinate activities with disaster recovery team, first responders, etc.

- **Emergency Alert**

  The person discovering the incident calls the Transitional Leader, Office Administrator, or Stated Clerk, in order of availability. Then the IT Disaster Recovery Team will be informed that an emergency has occurred.
- **Personnel and Family Notification**

  If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

Media Contact

The Transitional Leader or designee, will coordinate with the media. Only the Transitional Leader or designee is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the Transitional Leader or designee.

- ***Media Strategies***
  - Avoiding adverse publicity
  - Take advantage of opportunities for useful publicity
  - Have answers to the following basic questions:
    - What happened?
    - How did it happen?
    - What are you going to do about it?

Recovery

- **Insurance**

  As part of the Presbytery's disaster recovery strategy, comprehensive liability coverage has been put into place. The Transitional Leader will contact the Insurance agency as soon as possible following the incident to apprise them of the incident.
- **Financial Assessment**

  The Treasurer and the Budget and Finance Committee of the Presbytery shall prepare an initial assessment of the impact of the incident on the financial affairs of the Presbytery. The assessment should include:
    - Loss of financial documents

    - Loss of cash and checks
- **Financial Requirements**

  The immediate financial needs of the Presbytery must be addressed by the Treasurer in consultation with the Transitional Leader. These may include:
    - Cash flow position
    - Temporary borrowing capability
    - Upcoming payments
    - Availability of Presbytery credit cards to pay for supplies and services required post-disaster
- **Legal Actions**

  The General Council will review the aftermath of the incident and may consult with an attorney to decide whether there may be legal actions resulting from the event.
- **IT Disaster Recovery Kit and Supplies**

  An IT Disaster Recovery kit, including the following items, will be located at the Presbytery Office and off-site:
    - Copy of the Presbytery's IT Disaster Recovery Plan
    - Copy of the telephone numbers and email addresses for all members of the IT Disaster Recovery Team.
    - Copy of telephone numbers with extensions and email addresses for all staff and the General Council.
- **IT Disaster Recovery Incident and Activity Report**
    - On completion of the initial IT disaster recovery response, the Office Administrator, in consultation with the Transitional Leader will prepare an incident report of the disaster and the activities undertaken.
    - The report should contain information on the emergency, who was notified and when, action taken by members of the IT Disaster Recovery Team together with outcomes arising from those actions.
    - The report will also contain an assessment of the impact to normal business operations and lessons learned
    - A copy of the report will be provided to General Council and the Personnel Committee of Presbytery.
    - The General Council will report the incident to the Presbytery.

Policy Approved by the Presbytery of Geneva on March 20, 2018