# Business Continuity and Disaster Recovery Policy

*The purpose of this Policy is to define the requirements and processes that enable Florp to resume normal business operations in the event of a business interruption. This Policy also provides guidance on how Florp will communicate internally and externally during a business interruption.*

## Scope

This Policy applies to only Florp data and equipment used to conduct Florp business or interact with internal networks and business systems.

This Policy applies to Florp employees with access to Florp data or systems ("Covered Individuals"). All Covered Individuals are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Florp policies and standards as well as applicable laws and regulations.

## Business Continuity Program

Every five years, a Business Impact Analysis (BIA) may be conducted across business areas to identify critical business processes. A BIA should define the Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO) values for each critical business process. The BIA should also identify business continuity risk and add any findings to the risk register.

Our Florp app data should be backed up every 3 months at the latest. Backups should be securely stored on the same system to provide fast recovery opportunities, as well as in a secondary location in the event of a system having issues.

Business Continuity Plans must be documented and maintained for critical business processes. Plans should outline the steps necessary to resume critical functions within the time frame required to meet recovery time objectives set forth in the BIAs.

## Business Continuity Plan Requirements

After a BIA is conducted for a critical process, a Business Continuity Plan (BCP) should be created that formalizes the procedures for restoring normal operations. A BCP should include the following items:

- Critical Business Process Background Information
- Key Stakeholders and their contact information
- Critical Assets, Service Providers, and Sub Process with defined RPO, RTO, and MTD
- Downstream processes that will be affected and links to corresponding BCPs
- Procedures requiring post-mortem report and lessons learned discussion
- Procedures outlining the methods to update the plan after it has been executed

All BCPs should be printed and stored at the home of the CTO who can provide security. Each BCP should be reviewed every five years.

## Disaster Recovery

A Disaster Recovery Plan should be created for Florp in the event of a physical disruption which denies access to the primary core production infrastructure (the Florp App). A Disaster Recovery Plan should include the following items:

- Key Stakeholders and their contact information
- Roles and Responsibilities of the Recovery Team
- Passwords of all admin accounts
    - Contacts of the personnel who know how to rebuild the systems
- Procedures requiring post-mortem report and lessons learned discussion

In the event of a force majeure event, obligations of the service provider are not excused. The Business Continuity and Disaster Recovery Policy should be followed to restore all necessary systems in accordance with the agreement as well as following the recovery time/point objectives.

Backup restoration and failover testing should be tested every five years. The Disaster Recovery Plan should be documented in a central repository accessible by all relevant business stakeholders and the Recovery Team. The plan should be reviewed and approved every five years.

## Testing Exercise

1. A business continuity testing exercise is conducted every 2 years. All actions taken are recorded via screen and keystroke recording software and a post-mortem discussion is conducted. All identified areas of enhancement during the exercise will be incorporated into the BCP.
2. A disaster recovery testing exercise is conducted by Florp annually. All actions taken are recorded via screen and keystroke recording software and a post-mortem discussion is conducted. All identified areas of enhancement during the exercise will be incorporated into the DRP.

## Glossary

- **Recovery Time Objective (RTO)** - The targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. For example: The length of time that Florp can continue regular operations without a critical system or location.
- **Recovery Point Objective (RPO)** - The maximum targeted period in which data or transactions might be lost from an IT service due to a major incident. For example: The length of time that Florp data could afford to not be recovered to maintain business operations.
- **Maximum Tolerable Downtime (MTD)** - The total amount of time that a business process can be disrupted without causing any unacceptable consequences.