LAST UPDATE DATE	04-10-2025
OWNER	JEFF LILLIBRIDGE
STATUS	APPROVED

BUSINESS CONTINUITY POLICY

Approval History

Version	Approved By	Approved On
1.0	Not Present	04-10-2025

Purpose

The purpose of this policy is to outline objectives, plans, and, procedures put in place by City of Madeira Beach to ensure that it minimizes disruption to the Company's key business activities caused by a major security incident or a natural disaster.

Scope

Business Continuity policy applies to following

- All Information Systems
- Operation teams and support personnel
- Senior management

Background

City of Madeira Beach continuously aims for the preservation of critical business operations and essential functions to deliver key products and services. This policy outlines how City of Madeira Beach ensures this continuity.

- This policy puts in place a structure and authority to ensure business resilience of operations and information systems.
- This policy puts in place a plan to manage business operations through the disaster period and the effort it will take to get back to normal operations
- This policy defines a disaster recovery plan containing a set of human, physical, technical, and procedural resources to return to a normal level of operation, within a defined time and cost, in case of an emergency or disaster.

Policy

City of Madeira Beach must establish, implement and maintain procedures for the continuity of operations and ensure the availability of information systems and resources during adverse conditions. As a result, the company must create a **contingency and recovery plan** which must

- Identify essential information systems and critical business functions that must operate normally or in a limited fashion despite a system disruption, compromise, or failure;
- List associated contingency requirements for each one of the identified systems.
- Provide recovery objectives, restoration priorities, and metrics for each system.
- Define roles, responsibilities, and assigned individuals with contact information for each system.
- Create procedures for obtaining access to sensitive data during other-than-normal or emergency conditions.
- Create an inventory of recovery documents and operation procedures for each system. The steps should contain
    - Assets impacted
    - Custodian
    - Backup procedures
    - Restoration procedures
    - Testing / Validation steps
    - Recovery time and recovery point objectives for each asset
    - Escalation structure during the disaster period
    - Communication steps
- The recovery steps must be in the following order of priority.
    - Critical operations during disaster
    - Minimal operations after recovery
    - Full recovery and normal operations

Reviewing and maintaining the plan

- The contingency plan must be reviewed at least annually.
- The contingency plan must be reviewed and approved by company management.
- After each review, the necessary changes must be applied to the plan
- Key personnel must be notified of the changes
- Distributing copies of the contingency plan to key contingency personnel.
- Asset custodians and data owners are required to be trained in their contingency roles and responsibilities for systems.

Testing the plan

- A contingency plan must be tested once per year
- The contingency plan test results are document
- Asset owners and custodians of the information systems are responsible for the testing of the plan.
- Asset owners and custodians of the information systems are responsible for making any corrective actions in the plan as a result of the test exercises.

Enforcement

Business Continuity policy is enforced by the Senior Management team along with information security team and in some cases the business operation teams such as IT support teams.