**Category: INFORMATION TECHNOLOGY**

# DISASTER RECOVERY POLICY

## I. PURPOSE

This policy defines the baseline Disaster Recovery Plan that will be used by SVCE. The Disaster Recovery plan will describe the process to recover IT systems, applications and data from any type of disaster that causes a major outage.

## II. SCOPE

This policy applies to all SVCE personnel and Information Technology (IT) systems, networks, and assets.

## III. DEFINTIONS

"Business continuity" – The degree to which an organization may achieve uninterrupted stability of systems and operational procedures.

"Information Technology Disaster" – A sudden, significant event that may result in the loss or destruction of Agency information and/or loss of service on SVCE's IT network.

## IV. POLICY

A. IT DISASTER RECOVERY PLANNING

SVCE assumes that a major disaster – environmental disaster, loss of utilities, large-scale equipment failure, a cyberattack, and so on will befall it eventually. To ensure the continuity of business, should a disaster occur, SVCE developed the Information Technology Disaster Recovery Plan (DRP).

SVCE shall implement the Plan, educate employees in their roles and responsibilities, test the Plan, to see if it will ensure rapid and full recovery, and fix flaws identified in testing, to better ensure the Plan will work when it is most needed.

The Director of Administration and Finance shall obtain and analyze information for development of the DRP, such as:

- Conducting an IT threat risk assessment

- Determining SVCE's current state of readiness for disaster by running a recovery capability test to establish a baseline
- Gathering IT industry information on best practices and technologies and identifying appropriate means of mitigating risk
- Identifying and assessing external resources and their capabilities
- Identifying mission-critical systems and services, determining how long each SVCE business unit can survive without those systems/services in operation (conduct a business impact analysis)
- Establishing recovery priorities

## B. IT DISASTER RECOVERY PLAN

IT Support shall ensure periodic backups of Agency information stores (databases, etc.).

IT Support shall periodically conduct a test of all backed-up data for integrity and recovery speed; frequency and extent of such testing shall be determined by mission criticality of the information.

In the event any employee knows of or suspects an Information Technology Disaster, the employee shall contact IT Support and the Director of Administration and Finance shall begin the response and recovery process in accordance with the Plan.

## C. IT DISASTER RECOVERY PLAN REVIEW

Subsequent to an actual disaster and recovery, the Director of Administration and Finance shall prepare a response and recovery report and submit it to the SVCE Board of Directors. The Board may recommend revisions to the Plan, based on the findings contained in the report.

The Director of Administration and Finance shall test Information Technology Disaster response and recovery at least once every 12 months.

The SVCE Board of Directors shall review the DRP every two years to determine if it continues to meet Agency, customer, and legal/regulatory requirements.

Periodically. the DRP shall be subjected to a third-party audit, to verify that the Plan is clear, sound, and continues to meet Agency, customer, and legal/regulatory requirements.

D. IT DISASTER RECOVERY PLAN REVISION

After any review of the DRP, the Director of Administration and Finance shall be responsible for updating the plan.

Within one month of any such update, the Director of Administration and Finance shall verify that the update is capable of providing the desired results by conducting a response and recovery tool.