Revision History

Version	Date
Business Continuity and Disaster Recovery Policy, 1.0	30 July 2021

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

I. Introduction

USEIC requires adequate protections to be established to assure the continuity and recovery of the Organization's business following the loss of Systems (as defined in the USEIC Data Protection Charter (the "Charter")) that are critical to the operations of the Organization (a "Key Business System"). This Policy defines acceptable methods for business continuity and disaster recovery planning, leveraging a risk-based analysis in order to prepare for and maintain the continuity of the Organization's operations in case of the loss of a Key Business System.

Capitalized terms used in this Policy without definition are defined in the Charter.

II. Policy

A. Business Risk Assessment and Business Impact Analysis

Each Executive Manager is required to perform a Business Risk Assessment and Business Impact Analysis for each Key Business System that is used in his/her area of responsibility. The assessment should identify and define the criticality of Key Business Systems and the repositories that contain the relevant and necessary Organizational Data for the Key Business System. The assessment should also define and document the Disaster Contingency and Recovery Plan (the "Contingency Plan") for his/her area of responsibility. Such Plan shall include the following:

- Key business processes;
- Applicable risk to availability;
- Prioritization of recovery;
- Recovery Time Objectives; and
- Recovery Point Objectives.

For purposes of this Policy, a "Recovery Time Objective" is the 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 and a "Recovery Point Objective" is the maximum tolerable period during which Data might be lost from an Information Resource.

B. Contingency Plans

Each Key Business System must have a Contingency Plan documented for when hardware, software or Networks become critically dysfunctional or cease to function (short term and long-term outages). This Plan should include an explanation of the magnitude of information or System unavailability in the event of an outage and the process that would be implemented to continue operations during the outage. In addition, the feasibility of utilizing alternative off-site computer operations should be addressed. Specifically, the Contingency Plan must include:

1. An Emergency Mode Operations Plan for continuing operations in the event of temporary hardware, software, or Network outage. This Plan should contain information relating to the end user process for continuing operations.
2. A Recovery Plan for returning functions and services to normal on-site operations when a disaster is over.
3. A procedure for periodic testing, review, and revision of the Contingency Plan for all affected Systems, as a group and individually as needed.

C. Data Backup Plans

Each System Owner and IT Custodian will implement a Data Backup Plan or document the decision to forgo a Plan with a risk-based analysis. Such Plan should define the following:

1. Who is responsible for taking reasonable steps to ensure the backup of Organizational Data, particularly Sensitive Data and Confidential Data;
2. A backup schedule;
3. The Key Business Systems that are to be backed up;
4. Where backup media is to be stored and workforce members who may access the stored backup media;
5. Where backup media is to be kept secure before it is moved to storage, if applicable;
6. Who may remove the backup media and transfer it to storage;
7. Restoration procedures to restore Key Business System Data from backup media to the appropriate System;
8. Test restoration procedures and frequency of testing to confirm the effectiveness of the Plan;
9. The retention period for backup media; and
10. A method for restoring encrypted backup media, including encryption key management.