Education and Workforce Development Cabinet
POLICY/PROCEDURE

Policy Number: EDU-21

Effective Date: 08/19/2010
Revision Date: December 20, 2012

Subject: Contingency Planning Policy and Procedures

Policy: The contingency planning policy must be reviewed at least annually to assure its relevance. Just as in the development of such a policy, a team that consists of management and personnel from the Division of Technology Services/Department of Workforce Investment (KYWI) should be assembled to review the contingency policy. The procedures for execution of such a capability shall be documented in a formal contingency plan by the Information Systems Contingency Plan (ISCP) Coordinator and must be reviewed annually and updated as necessary by the ISCP Coordinator. The plan must account for the FIPS 199 security categorization (low, moderate, high) and comply with the appropriate security controls.

Roles and responsibilities of the planning team should be as follows:

- Perform an initial risk assessment to determine current information systems vulnerabilities.
- Perform an initial business impact analysis to document and understand the interdependencies among business processes and determine how the business would be affected by an information systems outage.
- Take an inventory of information systems assets such as computer hardware, software, applications, and data.
- Identify single points of failure within the information systems infrastructure.
- Identify critical applications, systems, and data.
- Prioritize key business functions.

Division of Technology Services and KYWI agency personnel will carry out the following procedures in the implementation of a disaster recovery policy:

- Setup and maintain offsite facilities for data backup storage and/or electronic vaulting as well as redundant and reliable standby systems if necessary.

- Ensure that critical applications, systems, and data are distributed among facilities that are reasonably easy to get to but not so close that they could be affected by the same disaster.
- Establish written policies, contracts, and service level agreements with third party hosting, co-location, telecommunications, and Internet service providers that facilitate prompt recovery and continuity.
- Create an incident response team that consists of Division of Technology Services/**KYWI agency** personnel and other relevant personnel as needed.
- Define the roles and responsibilities of the incident response team.
- Obtain each incident response team member's contact information.
- Determine which methods the incident response team members will use to communicate in the event of a disaster.
- Create a public relations plan to assist with the effective handling of an incident.
- Assign a manager (such as an IT Manager) that has the responsibility and authority to make critical IT decisions.
- Develop testing standards.
- Document and distribute the disaster recovery plan.
- Distribute copies of the written plans to everyone involved and also store extra copies in an offsite location.

The following are ongoing procedures that must be followed:

- Continuously perform data backups (See EDU-6 for the Backup Policy and Procedures), store at least weekly backup's offsite, and test those backups regularly for data integrity and reliability.
- Test plans at least annually, document and review the results, and update the plans as needed.
- Analyze plans on an ongoing basis to ensure alignment with current business objectives and requirements.
- Provide security awareness and contingency planning education for all team members involved.
- Continuously update information security policies and network diagrams.
- Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
- Perform continuous computer vulnerability assessments and audits.

Timeline:
Review Date: November 26, 2012
Reviewed by: ISCP Coordinator

Enterprise Security and Policies
Cross Reference:

OTS Standards
Cross Reference:
EDU_06 **--** Backup Policy