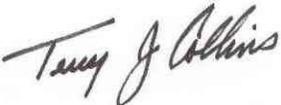


STATE OF OHIO



DEPARTMENT OF REHABILITATION  
AND CORRECTION

SUBJECT:	PAGE <u>1</u> OF <u>2</u> .
Disaster Recovery Planning	NUMBER: 05-OIT-13
RULE/CODE REFERENCE: State of Ohio Policy ITP-B.1; B.7.	SUPERSEDES: New
RELATED ACA STANDARDS: 3-3111	EFFECTIVE DATE: April 20, 2009
APPROVED:	

**I. AUTHORITY**

This policy is issued in compliance with Ohio Revised Code 5120.01 which delegates to the Director of the Department of Rehabilitation and Correction the authority to manage and direct the total operations of the Department and to establish such rules and regulations as the Director prescribes.

**II. PURPOSE**

The purpose of this policy is to ensure that Information Technology (IT) resource investments made by the Ohio Department of Rehabilitation and Correction (ODRC) are protected against service interruptions, including large scale disasters, by the development, implementation, and testing of disaster recovery/business resumption plans. For purposes of this policy, “disaster recovery/business resumption planning” includes, but is not limited to, the documentation, plans, policies, and procedures required to restore normal operation to the ODRC agency impacted by man-made or natural outages or disasters.

**III. APPLICABILITY**

This policy applies to persons employed by the Ohio Department of Rehabilitation and Correction, independent contractors providing a service to the department and volunteers who manage departmental data.

**IV. DEFINITIONS**

Disaster: An event, natural or man-made, which causes the loss of data in departmental data systems.

Risk Assessment: A process concerned with identifying, analyzing, and responding to IT security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events.

Service Interruption: The discontinuance of voice, data, or video telecommunications or computer services essential to the ODRC mission.

Telecommunications: The transmission, reception, and the switching of signals such as electrical or optical, by wire, fiber, or electromagnetic means.

## V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction to provide a plan to assess the risk of, prevent, and, if necessary, recover from a loss of departmental data through a disaster.

## VI. PROCEDURES

### A. Risk Assessment

1. The Bureau of Information Technology will conduct a Periodic Risk assessment on a three year schedule as part of routine IT maintenance procedures.
2. From this assessment, the Bureau of Information shall capture and disseminate incident lessons learned to reduce the possibility for similar incidents and thereby enhance the overall IT security posture.
3. A lesson learned analysis will be reported to the OIT SDD Enterprise Operations Security Office as defined in section 5.4 of Ohio Policy ITP-B.7.

### B. Disaster Recovery Plan

1. The Bureau of Information Technology will develop a Disaster Recovery/Business Resumption Plan. This plan will be reviewed and updated annually.
  - a. The Disaster Recovery/Business Resumption Plan will be tested annually and correct all deficiencies found during the test. The type and extent of testing adopted by the agency will depend upon:
    - i. Criticality of agency business functions
    - ii. Cost of executing the test plan
    - iii. Budget availability
    - iv. Complexity of information system and components
  - b. The Bureau of Information Technology will train employees to execute the Disaster Recovery/Business Resumption Plan.
2. In the event of a disaster occurring, departmental staff who own data will be responsible to cooperate with Bureau of Information Technology Staff in the identification of lost data.