Security Standard: Disaster Recovery

Scope
This Standard applies to:

- Process/function owners who use RIT Information Resources to perform their processes/functions (typically departments).
- Organizations that provide RIT Information Resources to support critical processes/functions (typically IT organizations).
- The standard does not apply to non RIT Information Resource restoration (e.g., staffing).

Continuity Classifications
Critical—Information or a process/function which if corrupted, lost, interrupted or made inaccessible during a disruption would pose a significant life, safety, financial, reputation, or other risk to RIT.

Non-Critical—Information or process/function which if corrupted, lost, interrupted or made inaccessible during a disruption would pose a minimal risk to RIT. The information or process/function could be supplied through alternate means during the disruption or delayed until after the disruption.

Requirements for Process Owners
The following security controls are required to be implemented:

1. Critical Processes Inventory and Recovery Time Objectives
   1.1. Every RIT organizational unit (department, division, etc.) should identify all critical processes/functions for which they are the process/function owner. Departments may use the continuity system for this purpose by coordinating with the Business Continuity Office, or may use the form located at http://www.rit.edu/fa/buscont/.
   1.2. For each critical process/function, departments will assign a Recovery Time Objective (RTO). An RTO is the minimum acceptable time a technology resource that is used to complete a process/function can be unavailable. Alternate methods of performing the process/function may be employed while the technology resource is being recovered.

2. Technology Resources and IT and Other Organizations
   2.1. Departments are responsible for identifying the technology resources that support each critical process/function. These resources include applications, software, hardware, and network (voice and data).
   2.2. Departments should identify IT and other organizations supporting critical processes/functions.
3. **Information and Recovery Point Objectives (RPO)**
   3.1. Departments should identify RIT electronic and non-electronic information created, used, and/or stored for each critical process/function.

4. **Documentation**
   4.1. Departments may use the recovery planning system for documenting critical processes/functions, RTOs, technology, IT Departments, RIT information, and RPOs by coordinating with the Business Continuity Office, or may use the form located at http://www.rit.edu/fa/buscont/. Forms should be provided to the Business Continuity Office for entry into the recovery planning system.

5. **Contingency Planning for Business Functions/Processes**
   5.1. To the extent possible, departments should establish contingency plans to continue critical business functions/processes to be used when normal mechanisms are unavailable.

6. **Training and Testing**
   6.1. Process/function owners should identify training requirements and determine appropriate training procedures.
   6.2. Training will include restoration and recovery procedures to return the process/function to its pre-disaster state.
   6.3. Departments should cooperate with supporting IT and other organizations to test restoration and recovery procedures on a periodic basis determined by the Divisional VP or Provost (Information Trustee).

7. **Review and Certification**
   7.1. Process/function owners should review all processes/functions and evaluate their criticality annually.
   7.2. Process/function owners should incorporate all new critical processes/functions into the Disaster Recovery Plan.
**Requirements for IT Organizations**
The following security controls are required be implemented:

8. **Documentation**
   8.1. IT organizations will retain an inventory of services in the Recovery Planning System that support critical processes/functions.

9. **Backup and Recovery/Restoration Procedures**
   9.1. IT organizations and business process owners will develop, maintain, and test backup and recovery/restoration procedures services (frequency of testing to be determined by process owner, IT organization, and contractual obligations) that support critical processes/functions to support academic/business unit recovery and disaster recovery.

10. **Alternate Site for Backup and Recovery/Restoration**
   10.1. IT organizations should determine an alternate site for back-up and recovery/restoration activities.
   10.2. Back-up and recovery/restoration activities should occur in a physically, environmentally, and logically secure location in compliance with RIT information security policies and standards.

**Effective Date:** January 23, 2016

**Standard History:**
November 11, 2013