Title: ITS Systems Disaster Recovery		Code Number: IT.007.02
Functional Category: Information Technology Services	Issuing Department: Information Technology Services	Effective Date: 10/01/2018

1.0 PURPOSE

1.1 This policy specifies the requirements for creating and maintaining disaster recovery plans for all critical business processes that utilize Information Technology (IT) systems, to ensure that the Board can continue operations if a disaster occurs.

2.0 DEPARTMENTS / PERSONS AFFECTED

2.1 All Board departments.

3.0 POLICY

3.1 The following activities must be performed to help minimize the impact of a disaster on ITS systems:

3.1.1 Perform a risk assessment.

3.1.2 Perform a business impact analysis.

3.1.3 Establish recovery time, recovery point objectives, and maximum tolerable period of disruption (MTPD).

3.1.4 Establish recovery plans.

3.1.5 Establish training, testing, and maintenance protocols.

3.2 **Exceptions.** Exceptions to this policy require the approval of the Vice President of ITS and the Chief Financial Officer with concurrence of the Executive Vice President of Administration and Diversity. Requests for exceptions, along with sufficient justification, must be submitted in writing by the requesting department head to the Vice President of ITS. Each subsequent request for an exception must stand on its own merit and circumstances without regard to prior exceptions granted**.**

4.0 PROCEDURE

4.1 **Risk Assessment.**

4.1.1 Risk assessments must be performed on all business processes that utilize an IT system, to identify threats to process continuity, IT system availability, and IT data integrity.

4.1.2 The risk assessment must include the following components for each threat:

4.1.2.1 Identification of IT programs/systems.

4.1.2.2 Threat description.

4.1.2.3 IT systems impacted by the threat.

4.1.2.4 Existing mitigating controls against the threat.

4.1.3 The risk assessment must be reviewed annually with the Information Technology Services (ITS) and Risk Management (RM) departments and updated as necessary. The final risk assessment report shall be provided to the Security Incident Response Team (SIRT) to ensure data/system coverage and continuity of interrupted loss coverage.

4.2 **Business Impact Analysis.**

4.2.1 A business impact analysis must be performed on all business processes that utilize an IT system. The end user groups will provide input into the critical nature of the system with respect to their individual departmental needs.

4.2.2 IT systems that are critical dependencies for other systems must inherit the business impacts of these dependent systems.

4.2.3 A business impact analysis for each business process that utilizes an IT system shall be conducted the earlier of every three years or as significant system modifications or upgrades occur.

4.3 **Recovery Time and Recovery Point Objectives.**

4.3.1 Recovery time and recovery point objectives must be:

4.3.1.1 Established for each IT system based on the business impact analysis.

4.3.1.2 Coordinated with the department head responsible for each business process/system.

4.4 **Disaster Recovery Plans:**

4.4.1 Must exist for all systems/applications that support critical processes.

4.4.2 Must be accessible (onsite and from a remote location) to the parties that will be responsible for implementation of the plans.

4.4.3 Should include the following information:

4.4.3.1 Conditions under which the plan is to be executed.

4.4.3.2 Required personnel and external vendors required to execute the plan.

4.4.3.3 Prerequisites that must exist before the plan can be executed.

4.4.3.4 Detailed steps required to execute the plan.

4.4.3.5 Criteria that will be used to determine if the plan was executed successfully.

4.5 **Testing Recovery Plans.**

4.5.1 The ITS Department must develop and document testing procedures for each disaster recovery plan.

4.5.2 Testing recovery plans should be performed by the business unit in coordination with the designated ITS representative, as specified in the Disaster Recovery Plan.

4.6 **Disaster Recovery Plan Maintenance.**

4.6.1 Disaster Recovery Plans must contain current and accurate information.

4.6.2 Backup strategies must comply with defined and approved recovery time and point objectives. Backup strategies must be reviewed on an annual basis.

4.6.3 All backup media must be precisely labeled and accurate records of backups and the backup set to which they belong must be maintained.

4.6.4 Backup media supporting critical business processes must be tested semi-annually for integrity and reliability of the backup data.

4.6.5 ITS must maintain a single, comprehensive electronic inventory of all servers, network equipment, relevant configuration, model information, and the information they support.

4.6.6 The following maintenance activities must be conducted annually:

4.6.6.1 Review of Disaster Recovery objectives and strategy.

4.6.6.2 Update of internal and external contact lists.

4.6.6.3 Conduct a simulation desktop exercise.

4.6.6.4 Conduct an application recovery test.

4.6.6.5 Verify alternate site technology.

4.6.6.6 Complete Disaster Recovery Plan revisions within 30 days after the Disaster Recovery Plan is tested.

5.0 RESPONSIBILITIES

5.1 **Chief Financial Officer and Vice President of ITS**. Authorized to approve exceptions to this policy with concurrence of the Executive Vice President of Administration and Diversity; also responsible for ensuring Board-wide compliance with this policy.

5.2 **Department Heads**. Responsible for performing a risk assessment and business impact analysis with designated ITS representatives on all business systems that utilize an IT system; developing and maintaining disaster recovery plans for all “critical” business processes in the event of a failure of the related IT system; and conducting disaster recovery testing in coordination with designated IT representatives.

5.2.1 For non-IT managed systems, department heads shall be responsible for:

5.2.1.1 Facilitating the risk assessment, business impact analysis, and disaster recovery tests.

5.2.1.2 Establishing procedures and designing the proper safeguards to ensure that non-ITS managed systems are reliable.

5.2.1.3 In the event of a disaster, ensuring that written disaster recovery processes and procedures from IT vendors are in place to restore systems within appropriate recovery time and recovery point objectives.

5.3 **Information Technology Services Department (ITS).** Responsible for facilitating the risk assessment and business impact analysis, establishing policies and procedures, designing the proper safeguards to ensure that ITS managed systems are reliable, and participating in the disaster recovery tests.

5.4 **Risk Management Department (RM).** Responsible for ensuring that the identification of critical programs and software are scheduled annually to ensure asset (system) identification and criticality of business interruption, if applicable, is accounted for in the event of a loss.

5.5 **Business Users/End Users.** Responsible for providing input for business impact analysis and executing manual processes and procedures during a system outage until the service can be restored.

6.0 DEFINITIONS

6.1 **Critical Systems.** Defined according to the business impact of a loss of its availability. This measurement is used to determine the order of system recovery in the case of a large scale disaster, as well as to recommend appropriate controls to minimize business impact.

6.2 **Department Head.** Vice president or senior vice president of a department, or assistant vice president in those cases where the department is led by an assistant vice president.

6.3 **Disaster Recovery.** The processes and technology that are implemented to reduce the disruption caused by disasters and system failures to an acceptable level through a combination of preventative and recovery controls.

6.4 **Disaster Recovery Plans.** The processes and technology that are implemented to maintain operations within a section in the event of the failure of an IT system that is critical to that business unit.

6.5 **Maximum Tolerable Period of Disruption**. The duration after which the size of the impact on an organization caused by the non-delivery of a product or service becomes unacceptable.

6.6 **Recovery Point Objectives.** The target maximum time elapsed from the last time of the reliable data backup until the time of loss of data integrity.

6.7 **Recovery Time Objectives.** The target maximum duration to return the IT service to its operable state.

6.8 **Security Incident Response Team (SIRT).** Composed of both permanent and ad-hoc members. Members include, but are not limited to, Vice President of ITS, Senior Information Security Manager, Chief Financial Officer, Vice President of Human Resources, General Counsel, and Vice President of Public Affairs.

7.0 RESOURCES / FORMS

7.1 **Related Policies.**

7.1.1 Data Security Incident Response.

8.0 REVISION HISTORY

8.1 04/01/2007 – AA.008.00 – Original document.

8.2 04/01/2011 – IT.007.00 – Changed Issuing Department to Information Technology Services; added sections 4.2.6 and 6.3.

8.3 10/01/2015 – IT.007.01 – Substantive revisions.

8.4 10/01/2018 – IT.007.02 – Renamed from Disaster Recovery - Information Technology Services policy; other minor revisions.