

Information Technology Disaster Recovery Plan

Purpose

Provide business continuity for IT services
Comply with State of Maryland audit requirements

Core document

Objective

To ensure the continues operation of our business by providing the ability to successfully recover computer services in the event of a disaster.

Team Descriptions

Emergency Response Management Team

To establish and direct plans of action to be followed during an interruption or cessation of computer services caused by a disaster.

Operations Team

To ensure the resumption of computer services.

Applications Team

To ensure the proper functioning of the applications and to coordinate with users how their applications should be maintained during the contingency period.

Hardware Team

Repair or replace computer hardware; install and test.
Hardware contingency planning.

Facilities Team

Restore or replace the Data Center and other data processing facilities.

Logistical Support Team

Administrative support to the recovery effort; arrange Transportation, housing, expense advances, shipping, etc

Networking and Telecommunications Team

Restore or replace the Data and Telecommunications systems.

Help Desk Team

Serve as a customer focused, single point of contact for information about IT services and support to the campus.

Communications Team

Serve as communications liaison to the University
Emergency Response Teams; partnering with University
Relations, disseminate emergency information concerning
IT infrastructure, services and support to the public.

General Procedures for Potential Interruptions

Fire, flood, electricity, network failure

Policies for Reducing Risk

Computer data backup procedures
Backup recovery

Recovery Procedures, Notifications and Activations

Initial procedures, notification of teams, activation of
contingency site.

Testing and Maintenance

Testing verifies that all facets of the Plan have been
implemented and have been found to be accurate and
sufficient and achievable.
Periodic review and updating

Appendices

Unit specific sensitive blueprint for restoration of services
Critical Applications
Business Continuity Plan (Hot Site)
Emergency Contact List
Applications and Hardware Recovery Plans
Facilities Recovery Plan
Contingency Site Descriptions
Networking and Telecommunications Recovery Plan
Operations Recovery Plan
Logistical Support Plan
Help Desk Recovery Plan

Next Steps

RFP for Business Continuity (Hot Site)
Testing and Maintenance