Georgetown University
Information Services

POLICY: Information Systems Contingency Plan Policy

STATEMENT:

This policy is created to protect the ability to conduct business and maintain the availability of university information. Information Systems Contingency Plans (ISCP) are required for all information technologies (for example, applications, servers, and infrastructure) and from all university technology service providers (TSP) within and outside University Information Services (UIS).

APPLICABILITY:

This policy applies to all technology service providers responsible for the management of information technology.

GUIDING PRINCIPLES/PURPOSE:

A formal, documented contingency planning process provides a framework for setting information systems contingency objectives. Each plan addresses purpose, scope, roles, responsibilities, management commitment, and coordination among technology service providers within and external to UIS. All technology service providers are required to develop, record and annually review a comprehensive Information Systems Contingency Plan for university assets under their management.

ADMINISTRATION AND IMPLEMENTATION:

In order to insure ongoing availability of university services and data, all technology service providers are required to develop and maintain an Information Systems Contingency Plan for each service under their management.

RESPONSIBILITIES:

Members of the Georgetown University community with specific responsibilities governed by this policy are listed below.

Technology service providers, including UIS staff, are responsible for:

- Maintaining a current list of all services under the provider's management.
- Preparing and submitting an Information Systems Contingency Plan.
- Amending plans as required by the Director, IT Systems - Business Continuity/ Disaster Recovery (BC/DR).
- Participating in assigned test exercises of the Information Systems Contingency Plan.
- Updating existing Information Systems Contingency Plans based on test exercises, lessons learned or changes to services as required, but at least annually.
- Responding to disasters or interruptions in business continuity in accordance with Information Systems Contingency Plans.

Director, IT Systems Business Continuity and Disaster Recovery is responsible for:

- Maintaining the technology service provider BC/DR program on behalf of the University.
- Reviewing Information Systems Contingency Plans and working with providers to ensure complete, accurate, and effective planning.
- Planning, preparing for, conducting, and reviewing test exercises of the Information Systems Contingency Plans.
- Providing support and assistance to technology service providers with regard to Information Systems Contingency Planning.
- Working in close coordination with the Risk Management Office and other university departments to maintain and support University-wide Business Continuity/Disaster Recovery processes.

COMPLIANCE:

Technology service providers are expected to comply with this policy. Non-compliance may result in delayed recovery for critical systems and services, and low prioritization for services not covered.

RESOURCES:

Relevant policies, resources, and procedures supporting this Policy include:

- Georgetown University Information Security Policy for TSPs, SNAs, and DISOs

- ISO/IEC 22301 - Requirements for Business Continuity Management Systems

- NFPA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs

- ISO 22313 - Guidance for Business Continuity Management Systems

- ISO 27031 - Guidelines for Information and Communication Technology Readiness for Business Continuity

- NIST SP 800-34 - Contingency Planning for Federal Information Systems

REVIEW CYCLE:

This policy will be reviewed and updated as needed, but at least annually, unless changes in institutional policy or relevant law or regulation dictate otherwise.

Reviewed and approved: Date:

Feb 9, 2016

Interim Vice President
and Chief Information Officer