

**OLD DOMINION UNIVERSITY**  
**University Policies and Procedures**

**3513 - INFORMATION TECHNOLOGY CONTINGENCY PLANS**

**Statement:** Old Dominion University strongly believes in the effective planning and preparation for continuation of critical business functions in the event of a service disruption or disaster. Contingency plans also serve to minimize the effects of such disruptions by guiding staff and setting clear goals and objectives. With regard to critical business services and reliance upon information technology, Old Dominion University conducts a risk assessment analysis on a bi-annual basis. Although the University expects all departments to have a plan in place for the continuance of critical business functions and services should there be a computer/network outage, those departments identified as highly critical and high risk by the risk assessment are required to have a formal contingency plan on file with the Office of University Audit. The Office of Computing and Communications Services is required to have a comprehensive plan in place that deals with the primary computing and communications components that support the campus. Such plans shall be developed, maintained, reviewed and periodically tested.

Contingency planning is defined by Old Dominion University to include procedures, documentation, appropriate backups, file restoration and recovery issues in dealing with service outages, as well as protecting critical data and providing essential services via alternate methodologies when computing capacities have diminished or are non-existent.

The following list of safeguards may be augmented by additional items and methods where believed to be practical, reasonable and reflective of sound business practices.

1. Campus departments are expected to have documented contingency plans identifying what critical and essential services are performed by that department. These plans must include strategies and methodologies as to how the department will perform those services in a diminished computing capacity environment. These plans are to be placed on file with the Office of University Audit.
2. Based on the University Audit Risk Assessment, certain identified departments must complete and submit a more formal contingency plan for their operational area. This plan must be based on the Commonwealth's [ITRM Standard 95-1 document](#). This designation and request for a formal plan will be made by the Office of University Audit.
3. The Office of Computing and Communications Services is expected to have a comprehensive Contingency Plan on file with the Office of University Audit as directed by the Commonwealth's [ITRM Standard 95-1](#).
4. The Office of Computing and Communications Services will provide a standard outline to assist the departments in creating a contingency plan.

5. The Office of University Audit will conduct a bi-annual survey (Risk Assessment) of all departments to determine levels of risk and magnitude of loss relating to critical business functions performed by that department.
6. Contingency plan review, oversight of contingency plan submission, updating and testing are the responsibilities of the Office of University Audit.

**Responsibility:** Vice President for Administration and Finance

**Authorization:** James V. Koch, President

**Date:** July 1, 2000

**Effective Date:** July 1, 2000