

**Note: This document is not designed as a substitute for a comprehensive Disaster Recovery Plan; nor does it contain recovery procedures specific to your organization. This material suggests high level issues that you should consider if you are in response mode. SunGard Planning is providing this as a public service.**

## **Information Security Checklist**

### **Physical Security**

Control access to the building and/or data center. Ensure personnel identification (photo ID's) and authentication procedures for all personnel entering the building and/or data center are enforced.

Obtain a list of authorized individuals.

Control access to power plants if exterior to the building.

Protect critical documents at a secure off-site storage location.

- Network Topology
- Hardware/Software inventor
- Disaster Recovery Documentation

Implement security controls 24x7.

### **Security Administration**

Designate an individual to be responsible for security oversight.

Ensure that security policies and procedures are instituted and followed. Maintain security awareness and provide updates to personnel, as needed.

Manage all data security issues and continue system monitoring. All information should be based on a need to know basis.

### **Recovery Operations**

Verify security configurations on switches and routers.

Verify that the security configuration of each system is implemented.

Follow procedures for installing security-related patches.

Backup all systems and data on a daily basis and transport off-site to a secure location.

## **Access Control**

Coordinate user access control and emergency authorization of dial-in access, log-on identification and password setting. Ensure secure procedures for setting temporary user IDs and passwords are implemented and followed.

Use the following password security mechanisms:

- User authentication
- Password encryption
- Change passwords frequently
- Put limits on log-on attempts
- Automatic log-off after period of inactivity

Ensure that the network control center has the ability to, on request, automatically reduce the privileges of a particular user-ID/account or class of user-ID accounts.

Continue monitoring detection of security breaches and ensure the reporting of unauthorized attempts to gain access to system software and data.

Verify authentication and encryption of dial-up connections and connections from the Internet to the internal network?

Verify any and all open ports allowing two-way communication and determine level of security required. (i.e. close all open ports allowing external communication only).