FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions

(Seventh Edition)

(including supplement to the seventh edition)

March 2006
(Supplement to the seventh edition: March 2007)

The Center for Financial Industry Information Systems (FISC)

FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions (Seventh Edition)

(including supplement to the seventh edition)

Table of Contents

Buildings
Environment

Applicable location			
Center	Head	Affiliate	Direct
○			

F1	Avoid setting up a compute center in a place subject to disasters or failures.

To reduce the influence of a disaster on a computer center, it is recommended to avoid setting up a computer center in a place subject to disasters and failures.

1. Disasters and failures include fire, lightning strike, tsunami, storm surge, floods, earthquake, electric/magnetic disturbances, air pollution, excessive salt damage, and vibration.

2. It is recommended to avoid setting up a computer center at a site subject to disasters and failures. In the case where a computer center building has already been built or must be built at a site subject to disasters or failures, appropriate measures must be taken against each disaster or failure.

   Refer to materials on disasters published by the government offices concerned and each local government.

   (Note) Reference materials include the following:
   - "Study on Estimation of Possible Earthquake Damage in Tokyo" ("Tokyo Disaster-Prevention Conference", August 1997)
   - "Report on the Degree of Danger Concerning Earthquakes for Each Area" ("Tokyo Urban Planning Department", October 2002)
   - "Report on Estimation of Possible Earthquake Damage in the Western Part of Kanagawa Prefecture" ("Kanagawa Prefecture Disaster-Prevention/Fire-Defense Department", March 1999)

   For information on studies of earthquake damage for other areas, please refer to the report on estimation of possible earthquake damage for the particular area.

3. Fire

   The following lists sites subject to fire:

   (1) Sites with many wooden houses close together
   (2) Sites where a facility for large amounts of flammable materials is located
   (3) Sites where a dangerous substance is stored, which may explode when exposed to fire

4. Lightning strike

   Among disasters that cause damage to computer systems of financial institutions, lightning strikes are the most frequent.

   When determining a location for a computer system, it is recommended to refer to published data on the number of thunder/rainy days per year.

5. Tsunami

   (1) A tsunami is a wave that may span over a long period, triggered by the movement of the seabed due to an earthquake, etc. It travels toward coasts, where its size increases in shallow areas.

Establishment of management systems
Security management and definition of responsibility

Applicable location					Reference Item
Common	Center	Head	Affiliate	Direct	Out-of-scope
◎					※

O1	Documentation should be prepared with concrete definitions of security management methods.

Documentation that concretely specifies security management methods and defines responsibilities should be prepared in order to execute appropriate security management.

1. The appropriate execution of security management requires formulation of a security policy, which is a basic policy regarding the appropriate protection of company (or organization) information resources, and preparation of security-related documentation, including security standards (in-house company standards), manuals, and procedural instructions, which describe concrete measures for implementing that policy. The kinds of security-related documentation can be classified as shown below.

   (1) Security policy (basic policy)
   Basic company-level security policy that defines the information resources requiring protection, the reasons for protection, and the responsibilities for protection.

   (2) Security standards (in-house company standards)
   Concrete measures for implementing security policy (basic policy); it can be prepared by each unit of the company.

   (3) Manuals and procedural instructions
   Application of security policy (basic policy) and security standards in concrete operational procedures; it can be set for each unit of the company or individual system.

   Top management must participate in the revision, which may greatly impact on the policy and measures of security management for the entire company (or all organizations).

2. It is necessary to make security-related documentation known to all officers and employees (including outsourcee's staff) and to educate them appropriately according to their functions and responsibilities regarding security measures within the organization. In connection with security training, refer to [O80].

3. There are three main items that should be defined in security policy documents, as follows:

   (1) Information resources that require protection
   (2) Reasons why protection is required
   (3) Definition of responsibilities for protection

4. Points that should be given attention when preparing security-related documentation include the following:

   (1) The formulation of security management implementation plans begins with determination of the importance of the information handled in the computer system in question, and definition of the priority assigned to the services provided by the computer system. This requires an examination of all the information being handled, and decisions about the level of protection that the company (or organization) should assign to the information.

   Management of important information resources must be carried out in accordance with security policy, and appropriate protection must be provided for their levels of importance with consideration for the confidentiality, integrity, and availability of the information.

Measure to improve hardware reliability
Protection against hardware failure

Applicable location					Reference Item
Common	Center	Head	Affiliate	Direct	Out-of-scope
	◎	◎			※

T1	Perform preventive maintenance of hardware.

To prevent hardware failure, perform preventive maintenance of hardware regularly or when necessary depending on the characteristics or importance of the devices.

1. To enhance the reliability of computer systems, it is important to improve the reliability of system hardware firstly, therefore it is necessary to perform preventive maintenance to minimize any occurrence of hardware failure.

2. The following shows specific examples of preventive maintenance. Refer to [O59].

   (1) Regular maintenance

   In regular maintenance, inspection items and inspection intervals are predetermined depending on the characteristics or importance of the devices. Regular maintenance is performed to prevent failure, and takes the following two forms:

   1) Overall maintenance
      Comprehensive preventive maintenance performed when all system are shut down.
   2) Individual maintenance
      Preventive maintenance which is performed on a per-device basis so that it will not affect operations even when the system is running.
      Note that cleaning of devices, which is performed by operators prior to operation hours, is also an important maintenance item.

   (2) Occasional maintenance

   In occasional maintenance, the usage of each device, conditions under which failures occurred, and error log are collected and analyzed to estimate the possible occurrence of failure for its prevention. Occasional maintenance is performed as required. For example, open-system devices are likely excepted from regular maintenance and therefore may be subject to occasional maintenance.

3. For systems with long uninterrupted operations, such as 24-hour operated systems, it is necessary to perform appropriate preventive maintenance according to the function and restrictions of each system.