

# JIPDEC

1996

## Informatization

## Quarterly



*Information Security*  
*—The Present and Future—*

**JIQ No. 103**



# JIPDEC Informatization Quarterly

1996

*JIPDEC Informatization Quarterly* (JIQ) is published quarterly by the Japan Information Processing Development Center (JIPDEC), Kikai Shinko Kaikan Bldg., 3-5-8 Shibakoen, Minato-ku, Tokyo 105 Japan.

Publisher: Hiroshi Ikawa, President  
Editor: Yuji Yamadori, Director  
Research & International  
Affairs

JIPDEC is a non-profit organization founded in 1967 with the support of the Ministry of International Trade and Industry, the Ministry of Posts and Telecommunications and related industry circles for the purpose of promoting information processing and the information processing industry in Japan.

NOTE: The opinions expressed by the various contributors to the JIPDEC Informatization Quarterly do not necessarily reflect those views held by JIPDEC.

Copyright 1995 by Japan Information Processing Development Center.

No part of this publication may be reproduced without written permission of the publisher.

Translated and Printed by The Translation Institute of Technology, Science & Culture  
Printed in Japan, January, 1996.

## CONTENTS

* From the Editor .....	1
* I. Information Security -The Present and Future- .....	4
* II. Computer Virus Prevention Guidelines (Tentative translation) .....	11
* III. THE STANDARDS FOR INFORMATION SYSTEMS SAFETY MEASURES (Tentative translation) .....	25
* IV. System Audit Standards (Tentative translation) .....	50

KEIRIN

00

This work was subsidized by the Japan  
Keirin Association through its Promo-  
tion funds from KEIRIN RACE.

No. 103



## From the Editor

With advances in networking and downsizing, information systems are exposed as never before to risks of deliberate or accidental harm by individuals, faults in information systems themselves, and the threat of disasters and the like. In an instant, the earthquake that struck southern Hyogo Prefecture in January 1995 dealt an annihilating blow to the Hanshin and Awaji districts, and many information systems were destroyed in Kobe, a major city representative of the Kansai region. This was one of the main factors that drove business activities of the region to a standstill.

At the same time, there is a resurgence of awareness of the importance of security measures against theft of secret information or abuse of information systems by people with bad intentions, simply because information systems have become the infrastructure for corporate and enterprise activities.

Since there have not been that many incidents of damage that have had a serious impact on company activities

in Japanese companies and enterprises, up until now awareness of the importance of security has not been that strong. Furthermore, occurrence of such incidents notwithstanding, company investments to prepare for such threats have been weak because there are no tangible returns for the investments. That is, though management may feel the need for security measures to some extent, there are extremely few firms that are actually plunging into such investments programs, because of the relatively high costs and recent recessions. This tendency stands out conspicuously in the results of the surveys JIPDEC has conducted up until now.

However, though incidents have not been that numerous of late in comparison to major European countries and the U.S., the number of willful criminal incidents of hacking, computer viruses, and the like in Japan has shown a tendency to increase. Among these incidents, not a few have exercised a serious influence on company activities. Because of this, MITI has formulated standards such as the "Anti-Computer Virus Guidelines,"

the "Standards for Information Systems Safety Measures," and the "System Audit Standards." JIPDEC has played the central role in drawing up the explanatory documents for these. Of special note are the "Standards for Information Systems Safety Measures," an all-encompassing set of standards that includes disaster countermeasures. Their worth was proven in the recent earthquake, when computer centers that had cleared the highest level under these standards sustained no damage whatsoever. However, a relatively long period has passed since some of these standards were determined. A drastic revision of these standards was executed starting in the spring of 1995, to reflect the recent rapid advances in information technology and grounded in the security guidelines drawn up by the OECD. Meetings will be held in locations around the country as suitable to explain the final results of the revision, and JIPDEC is playing the central role in issuing new explanatory documents.

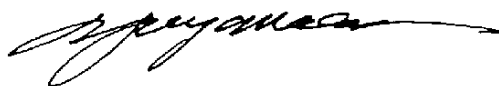
Meanwhile, with regard to how to deal with physical damage from disaster, using the lessons learned from the January 1995 earthquake, research is underway to study the issue of what forms robust security systems should adopt in order to be able to resist damage from such disasters

in the future, with a target for completion in March, 1996. Currently, surveys are underway to study conditions overseas as well as the effects on information systems exerted by the damage from the recent earthquake, and studies are also being performed by a committee of specialists established for that purpose.

In Japan, concern about privacy problems has not been very high in the past, perhaps partly because of the nature of our national character. Nevertheless, awareness of privacy protection issues has been gradually increasing in Japan recently because of the privacy guidelines drawn up by the OECD, the TDF (Transborder Data Flow) declaration, and the spread of electronic transactions involving information about individuals owing to advances in information systems. To respond to this, not only have preparations on the level of the legal system already been undertaken in the administrative sector regarding the handling of individual information, various investigations have since been carried out in the private sector as well. For example, JIPDEC is currently performing research regarding the formulation of a standard Compliance Program for protection of individual information in private enterprises and the establishment of a system for granting certifi-

cation marks to companies that carry out this program, with an operational target launch date of April, 1996.

In this issue, we will introduce information related to security and privacy issues in Japan, focusing on recent activities. I hope this information will be of service to our readers.



Yuji Yamadori  
Director  
Research & International Affairs

# **I. Information Security - The Present and Future -**

## **1. Japanese Standards related to Information Security**

In our country, information security measures are implemented based on the guidelines formulated and announced by the government authorities concerned. In particular, the Standards for Information Systems Safety Measures, handed down by the Ministry of International Trade and Industry (MITI), are widely used by public institutions and private corporations alike as a standard reference guideline on the safety of buildings and other information system hardware.

Security-related measures in our country

With the development of the GII environment and change in information systems resulting from advances in information technology, the MITI started work on revising the Anti-Computer Virus Guidelines, Standards for Information Systems Safety Measures, and Sys-

tem Audit Standards in the spring of 1995.

### **1.1 Anti-Computer Virus Guidelines**

(1) This Guidelines outline effective measures for protecting computers from computer viruses, detecting computer viruses, eradicating them and restoring computers affected by them to normal.

#### **(2) Elements of the Guidelines**

- System User Standards (18 items)
- The System User Standards describe the measures that system users can refer to for taking measures against viruses.
- System Administrator Standards (31 items)
- These standards describe the measures that people who introduce, maintain and control systems (system administrators) can refer to for taking measures against viruses.



• Software Supplier Standards (21 items)	1990 (April through December):	14
These standards describe the measures that people who develop, produce and supply software pro- grams and software products (soft- ware suppliers) can refer to for taking measures against viruses.	1991:	57
	1992:	253
	1993:	897
	1994:	1,127
	1995:	668

- Network Operator Standards  
(15 items)  
These standards describe the  
measures that operators who sup-  
ply information via personal com-  
puter communication networks  
(network operators) can refer to  
for taking measures against vi-  
ruses.

- System Service Operator Stand-  
ards (19 items)  
These standards describe the  
measures that operators who pro-  
vide system management services,  
system maintenance services,  
rental services and other services  
(system service operators) can re-  
fer to for taking measures against  
viruses.

The number of computer virus in-  
fections and the resulting damage  
are increasing because distributed  
processing (for example, the client-  
server architecture) is developing  
due to increased downsizing and  
more open systems in recent years  
and more non-technical users than  
ever before are using computers. In  
this situation, measures for protect-  
ing computers from viruses cannot  
cover all areas of computing, there-  
fore the scope of computer virus in-  
fection has expanded.

With the above situation in mind  
and understanding that antivirus  
measures more appropriate for the  
current information system environ-  
ment are needed, MITI has reviewed  
and revised the Anti-Computer Vi-  
rus Guidelines.

### (3) Purpose of the revision

The number of computer virus in-  
fections reported in our country is  
increasing rapidly each year:

### (4) Important points of the revision

- ① Adaptability to a new informa-  
tion system environment based

on distributed processing instead of centralized processing

- ② International coordination, which is important in an international network environment
- ③ Clarification of the purpose of each measure and improvement in the efficiency of applying one particular measure to one specific problem

## **1.2 Standards for Information Systems Safety Measures (formerly referred to as the Standards for Computer Systems Safety Measures)**

- (1) The purpose of these standards is to ensure the confidentiality, integrity and availability of information systems by enumerating measures to be executed by user, in order to prevent the destructive consequences of an abnormality such as natural disaster, hardware error, and deliberate or erroneous mistakes. In the event of the occurrence of such an abnormality, these standards minimize its impact and expedite the restoration of the affected system.

### **(2) Composition of the Standards**

- Installation Standards (100 items)  
These standards, relevant to the aspect of equipment and facilities installation, provide measures for physically protecting information systems, related equipment, disaster-prevention facilities and crime-prevention systems from natural disasters such as fire or earthquake, the failure of constituent elements, the harmful acts of intruders and other dangers.

- Technical Standards (26 items)  
These standards provide technical measures (both hardware and software) for allowing information systems to function smoothly and safely.

- Operating Standards (66 items)  
These standards provide measures for ensuring the safety and reliability of information systems through proper implementation of the Installation Standards and Technical Standards.

### **(3) Purpose of the revision**

Since MITI first formulated the standards in 1977, many corporations have considered them very valuable and used them to work out their own safety measures. In the information processing industry in particular, computer facilities com-

plying with the standards have been built and installed. Continuing effort has been made to enhance the level of safety so that their computer systems can receive the Business Establishment Certification under the Information Processing Service Industry Computer Systems Safety Measures. Considering the remarkable development of distributed processing, changes in the information processing environment and the effects of the Great Hanshin and Awa-ji Earthquake, MITI decided to revise the Standards to reflect these changes and update the content.

#### **(4) Important points of the revision**

- ① Adaptability to the latest information system environment (networking, downsizing, etc.)
- ② Current standards are based on an earthquake with the seismic intensity of 5 on the Japanese Scale. We revised them so that information systems can tolerate an earthquake with the seismic intensity of 7, or a direct-hit earthquake.
- ③ To make our country's security measures internationally acceptable, we considered the viewpoints given in the Guideline on

Information System Security formulated by OECD in 1992 and the Security Evaluation Standards now being discussed internationally at ISO and IEC.

### **1.3 System Audit Standards**

- (1) These standards outline the important points of system auditing, conducted to improve the reliability, safety and efficiency of information systems and thereby contribute to the sound development of an information-oriented society.

#### **(2) Composition of the Standards**

- General Standards (9 items)  
These standards provide the fundamentals of audit planning and the requirements of auditors.
- Implementation Standards (191 items)  
These standards provide specific audit items for planning of construction, operation processes, development, operation, maintenance and common operations of information systems to be audited.
- Reporting Standards (8 items)  
These standards provide requirements to consider when summarizing the results of a system audit

as well as the actions to take based on the results.

### **(3) Purpose of the revision**

In our country, system auditing came into wide practice, after the MITI announced System Auditing Standards in 1985 and System Auditors Examination was made part of the Information Technology Engineers Examinations in 1986. After 10 years, over 3,000 system auditors have passed the Examination and the number of corporations using the System Audit Standards is now showing a steady and stable increase.

The information system environment, however, has undergone considerable change in the past 10 years. Especially in recent years, changes have been happening markedly and some problems have been pointed out regarding the application of System Audit Standards. Against this background, MITI reviewed the contents of the standards to revise it appropriately.

### **(4) Important points of the revision**

- ① Expansion of the audit range in response to the increasing number of client/server systems

and to the remarkable changes taking place in the information environment

- ② Clarification of the responsibility and authority of system auditors and compatibility with OECD security guidelines to make the standards internationally acceptable
- ③ Addition of a number of audit items on the measures against disasters

## **2. Trends of Other Security-related Measures**

In addition to the standards related to information system security, the following subjects are being studied in our country after the G7 Ministerial Meeting held in Brussels in February 1995, which was attended by ministers in charge of information management.

### **2.1 Cipher and Authentication**

The Internet is being touted for commercial dealings. However, there is concern about data modification, wiretapping and other security-related issues. Encryption techniques are effective in solving these problems. Especially indispensable in

the world of electronic trading is an authentication technique that allows you to identify your counterpart (the company you are going to deal with) on the other end of a communication line via a station issuing a key. Considering the importance of this public key encryption system, MITI has studied the key control and management system.

After obtaining results on the studies MITI made of this system, the Initiatives for Computer Authentication Technology (ICAT) was established on March 20, 1995 to study and develop encryption techniques and related systems with the understanding that they are the basic technology needed to make electronic trade a reality. A total of 37 companies presently participate in the Initiatives and are studying technical and regulative aspects of systems which realize registration and control of public keys used for personal identification, indispensable for electronic commerce. They are also researching and studying encryption methods.

## **2.2 Protection of Privacy**

Personal information is sometimes used by others without the person's acknowledgement. As networking

advances and huge amounts of information, including personal information, are exchanged, chances are increasing that information will not only be used for unintended purposes but will travel further and faster than ever.

It is especially necessary for organizations that deal with personal information set limits on the use of that information and have a thorough understanding of the people concerned. MITI is studying how to set appropriate limits by referring to the EU directives given by the EC Commission. Practically, MITI is studying the following subjects and intends to start actual operation in April 1996.

- A standard compliance program (C/P), which private enterprises can use as a prototype for formulating C/P on personal information protection
- A system for issuing a certificate to private enterprises that formulate C/P and operate a proper personal information protection system

## **2.3 Dealing with Hackers and Computer Viruses**

With the expansion of networking

and the spread of personal computers, hacking, virus infection and other fraudulent acts will increase. Effective measures for eradicating such illegal acts must be established.

MITI has been working on preventive measures as well as damage recovery measures. Part of these preventive measures is the modification of Anti-Computer Virus Guidelines. Measures against illegal access for use by network opera-

tors, system users, and system administrators, are in preparation (to be completed in March 1996). MITI has been studying promotional activities for comprehensively protecting security environments and administrative measures to punish acts that interfere with system protection. In August 1995, Information-Technology Promotion Agency, Japan (IPA) established the illegal access (hacking) damage report system.

## II. Computer Virus Prevention Guidelines (Tentative translation)

### 1. Purpose

These Guidelines summarize effective computer virus prevention measures, including detection, eradication, and recovery measures.

### 2. Definitions of Terms

The main technical terms used in these Guidelines are defined below.

#### (1) Computer virus (hereinafter simply called "virus")

A program that is intentionally designed to cause damage to a third party's programs or databases and has at least one of the following functions:

##### ① Self-replication

The program can replicate itself or use another system function to infect other systems by copying itself into other programs.

##### ② Latency

The appearance of symptoms of virus infection are delayed by having the system wait for a spe-

cific point in time, a specific period of time, or a specific number of transaction executions.

##### ③ Destruction

The virus destroys program, data, or other files or causes systems to operate in a way not intended by the designers.

#### (2) Software

Programs such as system programs, applications, and utilities.

#### (3) System

Hardware, software or a network, or a combination of them.

#### (4) Vaccine

Software that includes virus inspection, prevention, or recovery functions.

#### (5) Back up

To record the contents of a program or data onto another medium.

### **(6) File**

A program or data recorded electronically or optically on a storage medium.

### **(7) Maintenance function**

A function for keeping a system in its normal condition.

### **(8) Security function**

A function for maintaining the security, integrity, and availability of programs and data.

## **3. Structure**

These Guidelines consist of system user standards, system manager standards, software developer and vendor standards, computer network service standards, and system service standards. Their structures and contents are described below.

### **(1) System user standards (18 points)**

These standards summarize the measures to be taken by users of a system (hereinafter called "system users").

- ① Software management (2 points)  
This section summarizes the

measures to be taken when system users install software.

- ② Operation management  
(12 points)

This section summarizes the measures to be taken when system users use their systems.

- ③ Post-detection actions (3 points)  
This section summarizes the actions to be taken when system users find a virus.

- ④ Audit (1 point)  
This section summarizes the items to be audited to ensure that virus prevention measures are taken properly.

### **(2) System management standards (31 points)**

These standards summarize the measures to be taken by those who install, maintain, and manage systems (hereinafter called "system managers").

- ① Computer management (8 points)  
This section summarizes the measures to be taken when system managers install or update hardware and software.

- 2) Network management (5 points)  
This section summarizes the



measures to be taken when system managers install or update a network.

- ③ Operation management (9 points)  
This section summarizes the measures to be taken when system managers maintain and manage systems.

- ④ Post-detection actions (6 points)  
This section summarizes the actions to be taken when system managers find a virus or are notified of the detection of a virus by system users.

- ⑤ Education and enlightenment (2 points)  
This section summarizes the anti-virus education and enlightenment to be conducted for system managers and system users.

- ⑥ Audit (1 point)  
This section summarizes the items to be audited to ensure that virus prevention measures are taken properly.

**(3) Software developer and vendor standards (21 points)**

These standards summarize the measures to be taken by those who develop software or develop, manu-

facture, and ship software products (hereinafter called "software developers and vendors").

- ① Development management (9 points)  
This section summarizes the measures concerning the development of software and software products and the introduction, updating, and management of development environments.

- ② Product management (3 points)  
This section summarizes the measures to be taken in the manufacture and shipment of software products.

- ③ Post-detection actions (7 points)  
This section summarizes the actions to be taken when software developers and vendors find a virus or are notified of the detection of a virus by users of products.

- ④ Education and enlightenment (1 point)  
This section summarizes the anti-virus education and enlightenment to be conducted for software developers and vendors.

- ⑤ Audit (1 point)  
This section summarizes the items to be audited to ensure

that virus prevention measures are taken properly.

**(4) Computer network service standards (15 points)**

These summarize the measures to be taken by operators who provide information through personal computer communication and other networks (hereinafter called "network operators").

- ① System management (2 points)  
This section summarizes the measures to be taken in the installation and updating of systems used for network operations.
- ② Operation management (4 points)  
This section summarizes the measures to be taken in the maintenance and management of systems used for network operations.
- ③ Post-detection actions (6 points)  
This section summarizes the actions to be taken when network operators find a virus or are notified of the detection of a virus by users of networks.
- ④ Education and enlightenment (2 points)  
This section summarizes the anti-virus education and enlightenment to be conducted for network

operators and network users.

**⑤ Audit (1 point)**

This section summarizes the items to be audited to ensure that virus prevention measures are taken properly.

**(5) System service standards (19 points)**

These standards summarize the measures to be taken by those who provide such services as system management, maintenance and rental (hereinafter called "system service operators").

- ① System management (5 points)  
This section summarizes the measures to be taken in the installation and updating of systems used for system services.
- ② Operation management (6 points)  
This section summarizes the measures to be taken in the maintenance and management of systems used for system services.
- ③ Post-detection actions (6 points)  
This section summarizes the actions to be taken when system service operators find a virus or are notified of the detection of a virus by users of networks.

④ Education and enlightenment  
(1 point)

This section summarizes the anti-virus education and enlightenment to be conducted for system service operators.

⑤ Audit (1 point)

This section summarizes the items to be audited to ensure that virus prevention measures are taken properly.

## **4. System User Standards**

### **a. Software management**

(1) Obtain software whose sellers or distributors are clearly identified and whose update information is clear.

(2) Store original programs safely, such as by write-protecting the disks and making a backup copy of them.

### **b. Operation management**

(1) Conduct a virus inspection before using files obtained from outside or file media shared with other users.

(2) When using a system, initialize it first in order to minimize the damage from possible virus in-

fection.

(3) Pay attention to changes in system operation in order to detect virus infection quickly.

(4) Conduct virus inspections at regular intervals, using the latest vaccine, etc., in order to detect virus infection early.

(5) In order to prevent damage from virus infection that could result from unauthorized access, set passwords that cannot be guessed easily and keep them secret.

(6) In order to prevent damage from virus infection that could result from unauthorized access, change the passwords from time to time.

(7) In order to prevent damage from virus infection that could result from unauthorized access, do not share system user IDs.

(8) In order to prevent damage from virus infection that could result from unauthorized access, check the access history.

(9) In order to prevent damage from virus infection that could result from unauthorized access, strictly control files that store confidential information.

- (10) Do not leave a system in a state in which it is waiting for input and can thus be used without authorization.

take any necessary steps.

## **5. System Manager Standards**

- (11) Do not use any software of unknown origin, in order to prevent infection by a virus.
- (12) To prepare for responses to possible infection by a virus, make backup copies of files regularly and keep them for a certain time.

### **a. Computer management**

- (1) In order to enforce virus prevention measures smoothly, make the computer management policy clear.
- (2) In order to prevent infection by a virus, conduct a virus inspection whenever installing a device.

### **c. Post-detection actions**

- (1) If a system is infected by a virus, stop using the infected system, report it to the system manager, and follow his/her instructions.
- (2) In order to prevent the spread of damage from virus infection, follow the system manager's instructions for system recovery.
- (3) In order to prevent the spread of damage from virus infection, destroy floppy disks, etc. that contain infected programs.
- (3) In order to prevent infection by a virus, conduct a virus inspection whenever installing software onto a computer.
- (4) In order to prepare for responses to damage from infection by a virus, preserve details of all the software installed on a system.
- (5) Store original programs safely, such as by write-protecting disks and making a backup copy of them.

### **d. Audit**

- (1) In order to improve the effectiveness of virus prevention measures, obtain system audit reports on virus prevention measures and
- (6) In order to prevent damage from virus infection that could result from unauthorized access, minimize the number of system users and their authority to access the system.

(7) In order to prevent damage that could result from infection by a virus, stop system users from writing to the directories where shared programs are stored.

(8) In order to prevent damage that could result from infection by a virus, delete programs that are not necessary for system operation.

### **b. Network management**

(1) In order to enforce virus prevention measures smoothly, make the computer management policy clear.

(2) In order to help identify the scope of damage from possible infection by a virus, record in advance and manage the installation conditions of devices connected to a network.

(3) In order to prepare for responses to damage from infection by a virus, establish an emergency reporting system and make it understood clearly and widely.

(4) In order to prevent damage from virus infection that could result from unauthorized access, ensure the security of network management information.

(5) In order to prevent damage from virus infection that could result from unauthorized access, ensure the security of the devices connected to an outside network.

### **c. Operation management**

(1) Make clear how to manage important information concerning the system.

(2) In order to protect important system information from unauthorized access, use the security function of the system.

(3) Avoid setting easy passwords, so that the passwords will not be guessed easily.

(4) In order to prepare against damage from infection by a virus, back up the system in use regularly and keep it for a specific time.

(5) In order to prevent damage that could result from infection by a virus, limit the services that can be used anonymously.

(6) In order to detect any unauthorized access, analyze the access history regularly.

(7) For early detection of possible infection by a virus, monitor the operation of the system.

(8) For early detection of possible infection by a virus, conduct virus inspections at regular intervals, using the latest vaccine, etc.

(9) If any system trouble is found, identify the cause promptly.

#### **d. Post-detection actions**

(1) In order to prevent any spread of damage from virus infection, stop using the infected system.

(2) In order to prevent any spread of damage from virus infection, promptly convey the necessary information to system users.

(3) In order to understand the damage from infection by the virus, endeavor to identify the kind of virus and the scope of infection.

(4) Work on the recovery of the infected development system by establishing safe recovery procedures.

(5) In order to prevent any recurrence of damage from virus infection, analyze the cause and implement preventive measures.

(6) In order to prevent the spread and recurrence of damage from infection by the virus, report the necessary information to the person specified separately by the Minister of International Trade and Industry.

#### **e. Education and enlightenment**

(1) In order to improve the level of virus prevention measures, collect and thoroughly disseminate virus-related information.

(2) Educate and enlighten system users on security measures and virus prevention measures.

#### **f. Audit**

(1) In order to improve the effectiveness of virus prevention measures, obtain system audit reports on virus prevention measures and take any necessary steps.

### **6. Software Developer and Vendor Standards**

#### **a. Development management**

(1) Make clear how to manage development tools in order to prevent a virus from infecting a development system through develop-

ment tools.

(2) Manage passwords strictly in order to prevent their leakage.

(3) Manage the development system strictly in order to prevent damage from infection by a virus that could result from unauthorized use of the system.

(4) In order to prevent damage from infection by a virus that could result from unauthorized access to the system, apply tight security to access to a development system via networks etc.

(5) In order to prevent damage from infection by a virus that could result from unauthorized access to the system, minimize the developers' authority to access the system.

(6) Clearly identify the developers and testers of a program being developed as well as the persons in charge, and manage the program strictly.

(7) To prepare for responses to possible damage from infection by a virus, make and keep a backup copy of the program being developed.

(8) In order to prevent unauthorized use, be sure to remove debugging functions from a program when development has finished.

(9) For early detection of possible infection by a virus, conduct virus inspections at regular intervals, using the latest vaccine, etc.

### **b. Product management**

(1) In order to prevent a product from being infected by a virus in the manufacturing process, copy it using a specialized system or device.

(2) In order to prevent infection by a virus, place the original of each product under strict management.

(3) In order to prevent a product from being infected by a virus in the distribution stage, take such measures as write-protecting disks and sealing packaging.

### **c. Post-detection actions**

(1) If any product infected by a virus is found, stop distribution, notify the users of the product, and recall the product.

(2) In order to prevent the spread of infection by the virus, stop using the infected development system.

(3) In order to prevent the spread of infection by the virus, promptly convey the necessary information to all the software developers and vendors concerned.

(4) In order to understand the damage from infection by the virus, endeavor to identify the kind of virus and the scope of infection.

(5) Work on the recovery of the infected development system by establishing safe recovery procedures.

(6) In order to prevent any recurrence of damage from virus infection, analyze the cause and implement preventive measures.

(7) In order to prevent the spread and recurrence of damage from infection by the virus, report the necessary information to the person specified separately by the Minister of International Trade and Industry.

#### **d. Education and enlightenment**

(1) In order to improve the level of

virus prevention measures, collect and thoroughly disseminate virus-related information.

#### **e. Audit**

(1) In order to improve the effectiveness of virus prevention measures, obtain system audit reports on virus prevention measures and take any necessary steps.

### **7. Computer Network Service Standards**

#### **a. System management**

(1) In order to help identify the scope of damage from possible infection by a virus, record in advance and manage the system setting used for the network service.

(2) In order to prepare for responses to damage from infection by a virus, establish an emergency reporting system and make it understood clearly and widely.

#### **b. Operation management**

(1) In order to prevent damage from infection by a virus that could result from unauthorized access, minimize the network users' access authority as much as necessary.



- (2) In order to prevent any damage that could result from infection by a virus, conduct a virus inspection, using the latest vaccine etc., before releasing a file for public use.
- (3) In order to prevent damage from infection by a virus that could result from unauthorized access, strictly manage network management information such as passwords.
- (4) In order to prepare for responses to damage from infection by a virus, always record the history of use and keep the record for a specified period.
- (4) Establish safe recovery procedures and inform the network users.
- (5) In order to prevent any recurrence of damage from virus infection, analyze the cause and implement preventive measures.
- (6) In order to prevent the spread and recurrence of damage from infection by the virus, report the necessary information to the person specified separately by the Minister of International Trade and Industry.

#### **c. Post-detection actions**

- (1) In order to prevent the spread of infection by the virus, stop distribution of infected files.
- (2) In order to prevent the spread of infection by the virus, promptly inform the network users and the network service operators.
- (3) In order to understand the damage from infection by the virus, endeavor to identify the kind of virus and the scope of infection.

#### **d. Education and enlightenment**

- (1) In order to improve the level of virus prevention measures, collect and thoroughly disseminate virus-related information.
- (2) Educate and enlighten network users on security measures and virus prevention measures.

#### **e. Audit**

- (1) In order to improve the effectiveness of virus prevention measures, obtain system audit reports on virus prevention measures and take any necessary steps.

## **8. System Service Standards**

### **a. System management**

- (1) Use software whose sellers or distributors are clearly identified and whose update information is clear.
- (2) In order to prevent unauthorized use, strictly manage any software that contains a maintenance function and strictly manage its information.
- (3) Store original programs safely such as by write-protecting disks and making a backup copy.
- (4) Prepare the disks to be used for the service from original programs by using initialized disks.
- (5) In order to prepare for responses to damage from infection by a virus, preserve the information on the structure of all the disks used for the service.
- (2) In order to prevent infection by a virus, inspect the systems to be used for the service for viruses in advance by using the latest vaccine etc.
- (3) In order to prepare for responses to damage from possible infection by a virus, keep the history of virus inspection and other system trouble for a specified period.
- (4) In order to prevent infection by a virus, do not use any system for the service after it has been used for another service.
- (5) In order to prevent damage from possible infection by a virus, disconnect any devices that are not necessary for the service.
- (6) Write-protect the disks used for the service in order to prevent them being infected by a virus.

### **b. Operation management**

- (1) In order to prepare for responses to damage from possible infection by a virus, clearly explain how to manage the systems used for the service.

### **c. Post-detection actions**

- (1) In order to prevent the spread of infection by the virus, stop using the infected system for the service.
- (2) In order to prevent the spread of infection by the virus, promptly convey the necessary information

to the users receiving the service.

- (3) In order to understand the damage from infection by the virus, endeavor to identify the kind of the virus and the scope of infection.

- (4) Work on the recovery of the infected system used for the service by establishing safe recovery procedures.

- (5) In order to prevent any recurrence of infection, analyze the cause and implement preventive measures.

- (6) In order to prevent the spread and recurrence of damage from infection by the virus, report the necessary information to the person specified separately by the Minister of International Trade and Industry.

#### **d. Education and enlightenment**

- (1) In order to improve the level of virus prevention measures, collect and thoroughly disseminate virus-related information.

#### **e. Audit**

- (1) In order to improve the effectiveness of virus prevention measures, obtain system audit reports on virus prevention measures and take any necessary steps.

### **9. Notes**

- (1) Use these standards according to actual existing conditions such as the kinds of computer, system setup, and software.

- (2) Standards for software developers and vendors, computer network services, and system services are established from the viewpoints of the respective operators. Accordingly, use the standards for system managers when installing systems to be used for respective business operations.

- (3) For safety measures for systems themselves, use the "Information System Safety Measures Standards."

- (4) To implement a system audit, use the "System Audit Standards."

- (5) Although these standards are primarily intended to be used by businesses and other organizations, they can also be used by individual users.

### III. THE STANDARDS FOR INFORMATION SYSTEMS SAFETY MEASURES (Tentative translation)

#### 1. Purpose

The purpose of the Standards is to ensure the confidentiality, integrity and availability of information systems by enumerating the measures that shall be executed by the users, in order to prevent the destructive consequences of an abnormality such as natural disasters, faults of units, deliberate or erroneous mistakes, and in the event of the occurrence of such an abnormality, to minimize its impact and to expedite the restoration of the affected system.

#### 2. Definition of Terms

The following are the definitions of principal terms used in the Standard:

##### (1) Terms relevant to information systems

- ① Computer: A unit or set of units having functions of computation, storage, control, and input and output.

- ② Host computer: A computer that provides two or more users with computation or database services and can execute network control functions as a server.

- ③ Terminal unit: A unit connected to a computer with a communication line or the like for data input and output. (Workstations, personal computers, automatic telling machines (ATMs), cash dispensers (CDs), various ticket/note dispensers, etc. are included.)

- ④ Communication unit: A communication line, switch, multiplexers, network unit, main distributing frame (MDF), intermediate distributing frame (IDF), etc.

- ⑤ Information system: A data processing system composed, part or whole, of a host computer, terminal units, communication units, and programs.

- ⑥ Information system and the like: An information system and associated facilities.
- ⑦ Data: Input and output information within an information system.
- ⑧ Program: A combination of instructions described in a programming language.
- ⑨ Document: A record of system design, program creation, operation of an information system and the like.
- ⑩ Data and the like: Data, programs and documents.
- ⑪ Record medium: A unit, disk, magnetic tape, film, card, paper (including seal-verified slips) and the like that carry recorded data.
- ⑫ File: Data and the like recorded in a storage device or record medium by electronic or optical means.

## **(2) Terms relevant to facilities**

- ① Power supply facility: A whole or part of facilities comprising a power receiving facility, con-

stant voltage and frequency power supply unit, distribution board, wiring and the like required for operating an information system.

- ② Air-conditioning facility: An air-conditioning unit, cooling tower and their supplementary units for a computer room and the like.
- ③ Monitoring facility: A facility that monitors the operating conditions of an information system, power supply facility, air-conditioning facility and the like, and execute required actions (generation of an fault alarm, recording of the event, and execution of necessary operations).
- ④ Associated facilities: Power supply facility, air-conditioning facility and monitoring facility.
- ⑤ Disaster-preventing facilities: Fire-alarming facility, fire-extinguishing facility, water leakage-detection facility, ultra-high-sensitivity fume sensor, fire-resistant safe, etc.
- ⑥ Crime-preventing facilities: Entrance/withdrawal control

facility, intrusion monitoring facility, storage facility, etc.

### **(3) Terms relevant to buildings and rooms**

- ① Building: A building accommodating information systems and the like.
- ② Computer room: A room exclusively destined for the installation of a host computer.
- ③ Office: A room, store or distributing center and the like in which terminal units, servers, workstations, personal computers and the like are installed.
- ④ Storage room of data and the like: A room where record media containing data, program and the like as well as documents are stored.
- ⑤ Terminal units space: A place where terminal units for general users are installed for specific services.

### **3. Composition of the Standards**

The Standards are composed of In-

stallation Standards, Technical Standards and Operating Standards, of which contents are as follows:

#### **(1) Installation Standards (100 items)**

Measures in the installation environment of facilities and equipment for physically protecting of information systems, their associated facilities, disaster-preventing facilities and crime-preventing facilities from natural disasters such as fire and earthquake, faults of components, and intruders.

#### **(2) Technical Standards (26 items)**

Technical measures with hardware and software for smoothly and safely enhancing the functions required for information systems.

#### **(3) Operating standards (66 items)**

Measures in view of operation for the pertinent application of the measures prescribed in the Installation Standards and Technical Standards and for ensuring the safety and reliability of information systems and the like.

## 4. Application Classifications

for the relevant building or the room.

### (1) Installation Standards

The Installation Standards are classified into a total of six items including building, computer room, office, storage room of data and the like, terminal units space, and associated facilities, and specify the application classification of each item of measures with due consideration of the extent of importance of the information system that is operated.

When comprehensive measures are required for the items of associated facilities in combination with the building or room involved, the application classifications are speci-

### (2) Technical Standards and Operating Standards

The Technical Standards and Operating Standards specify the application classifications of each item of measures by taking into consideration of the extent of importance of each information system in view of the impact of faults and applicability of measures depending on the mode of its usage and the extent of the identification feasibility of specific users.

(3) The concept of application classifications in Technical Standards and Operating Standards is analyzed in the following table:

User classification	Non-specific user	Specific in-house user	User within a specific department
Users of an information system	<ul style="list-style-type: none"><li>• Non-specific general individuals</li></ul>	<ul style="list-style-type: none"><li>• Personnel belonging to a company having an information system</li></ul>	<ul style="list-style-type: none"><li>• Personnel belonging to a specific department of a company or other companies having information systems</li></ul>
Example of information system	<ul style="list-style-type: none"><li>• Online system of a bank</li><li>• Computer communication system</li><li>• Online transaction system (value-added network)</li></ul>	<ul style="list-style-type: none"><li>• Sales and inventory management system</li><li>• Residents information system</li></ul>	<ul style="list-style-type: none"><li>• Personnel Information System</li><li>• Accounting system</li><li>• Aviation control system</li><li>• Dam water control system</li><li>• CAD, CAM and CIM</li><li>• Intercompany fund transfer system</li></ul>



User classification	Non-specific user	Specific in-house user	User within a specific department
Range of terminal units and clients	<ul style="list-style-type: none"> <li>Terminal units and clients of the host station and servers of other companies connected with the information system are included. (Internal system and physical control is impracticable.)</li> </ul>	<ul style="list-style-type: none"> <li>Terminal units within a company (Internal control is feasible.)</li> </ul>	<ul style="list-style-type: none"> <li>Terminal units within a department (Control within the department is feasible.)</li> </ul>
Administrator of terminal units and clients	<ul style="list-style-type: none"> <li>Other departments of a company (Internal system and physical control is feasible.)</li> <li>Other companies (Internal system control is feasible. Physical control is impracticable.)</li> </ul>	<ul style="list-style-type: none"> <li>Other departments of a company (Internal system and physical control is feasible.)</li> </ul>	<ul style="list-style-type: none"> <li>Within a department (Physical and system control within a department is feasible.)</li> </ul>
Administrator of host station and servers	<ul style="list-style-type: none"> <li>System administration departments</li> <li>Departments having an information system</li> </ul>	<ul style="list-style-type: none"> <li>System administration departments</li> <li>Departments having an information system</li> </ul>	<ul style="list-style-type: none"> <li>Specific department having an information system</li> </ul>

(4) When using the Standards, the following matters shall be considered:

① Information systems are classified into the following three groups according to the extent of importance:

A Information systems that have influence on human lives, properties of others, and privacy of those concerned.

B Information systems having a great influence on a company.

C Information systems having little influence on a company.

② The standards evaluate the cost, effect, extent of difficulty of each item of measures for the groups A, B, and C under above item ①, and distinguish the application classifications with the following marks of

application ranges against the room or user classifications:

☆: Measures required exclusively for the group A under item 1.

○: Measures required for the

groups A and B under item 1.

◎: Measures required for all of the groups A, B, and C under item 1.

-: Excluded from the application

## 5. Installation Standards

Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office and the like	4 Storage room for data	5 Terminal units space	6 Associated facilities
A. Installing environment							
1. Site and layout	(1) Buildings and rooms shall be located in such places where no risk of fire damage is conceivable.	☆	◎	☆	◎	☆	-
	(2) Buildings and rooms shall be located in such places where no risk of flood damage is conceivable.	☆	○	☆	○	☆	-
	(3) Buildings shall be located in such places where no risk of thunder damage is conceivable.	☆	-	-	-	-	-
	(4) Buildings and rooms shall be located in such places where no risk of damages due to electric or magnetic field is conceivable.	☆	◎	☆	◎	☆	-
	(5) Buildings and rooms shall be located in such places where no risk of damages due to air pollution is conceivable.	☆	☆	☆	☆	-	-
	(6) Each room shall be destined for the exclusive use for data processing.	-	○	-	○	☆	-
	(7) When an information system is installed in an office, due consideration shall be given to its location.	-	-	○	-	-	-
	(8) The locations of information system and record media shall not be indicated inside and outside of the building and the room.	◎	◎	☆	◎	-	-

(Continued)

Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office	4 Storage room for data and the like	5 Terminal units space	6 Associated facilities
	(9) A space required for evacuation shall be provided in the room and building where an information system is installed.	◎	◎	◎	◎	-	-
2. Opening areas	(1) Windows facing outside and common area shall be provided with disaster-preventing measures.	☆	◎	☆	◎	-	-
	(2) Windows which can readily be accessed from outside shall be provided with crime-preventing measures.	○	◎	☆	◎	-	-
	(3) Rooms shall be provided with necessary measures for preventing the influence of external light.	-	◎	◎	◎	-	-
	(4) The entrance/exit shall be constructed where non-specific persons use the system.	☆	◎	☆	◎	-	-
	(5) The number of entrances/exits shall be limited to the least possible and an entrance/withdrawal facility shall be installed.	☆	◎	☆	◎	-	-
	(6) An emergency exit shall be provided at appropriate locations of the buildings and rooms.	◎	◎	☆	◎	-	-
3. Structure	(1) Buildings shall possess the fire-resistant properties stipulated by the Building Standards Law.	◎	-	-	-	-	-
	(2) The room destined for the exclusive use for an information system shall constitute an independent fire-preventing compartment.	-	○	☆	○	-	-
	(3) Buildings and rooms shall be given necessary measures for preventing damages due to flood.	◎	◎	☆	◎	☆	-
4. Interior structures and furnishings	(1) The interior of a building and room shall be made of non-flammable materials.	☆	◎	○	◎	☆	-
	(2) The ceiling and wall of a room shall possess acoustic insulation properties.	-	◎	○	-	-	-
	(3) Lighting fitting shall be given dazzle-proof measures.	-	◎	◎	-	-	-

(Continued)

Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office and the like	4 Storage room for data	5 Terminal units space	6 Associated facilities
	(4) Major part of free-access floor of a room shall be made of non-flammable materials.	-	◎	○	◎	-	-
	(5) The surface materials of the floor of a room shall be given measures for preventing electrostatic troubles.	-	◎	◎	◎	☆	-
	(6) The curtains, blinds, carpet and the like of a building shall be made of flame-retardant materials.	☆	◎	◎	◎	☆	-
5. Building facilities	(1) Buildings shall be equipped with lightning arrester facilities.	◎	-	-	-	-	-
	(2) Buildings and rooms shall be equipped with an automatic fire-alarm facility.	◎	◎	◎	◎	◎	-
	(3) Buildings and rooms shall be equipped with an emergency broadcasting facility.	◎	◎	◎	◎	-	-
	(4) Buildings and rooms shall be equipped with fire-extinguishing facilities.	◎	◎	◎	◎	☆	-
	(5) Buildings and rooms shall be equipped with a fume-exhausting facility.	☆	◎	○	◎	-	-
	(6) Buildings and rooms shall be equipped with emergency lighting facilities.	☆	◎	◎	◎	-	-
	(7) Buildings and rooms shall be equipped with guide lighting fitting or guide markings.	☆	◎	◎	◎	-	-
	(8) Buildings and rooms shall be equipped with evacuating fitting.	◎	◎	◎	-	-	-
	(9) The inside of a room shall be equipped with no aqueous facilities except those required for operating the information system.	-	◎	☆	◎	-	-
	(10) The inside of a room and behind the ceiling shall be free from water piping.	-	◎	☆	◎	-	-
	(11) Buildings and rooms shall be given measures for preventing damages due to small animals and the like.	○	◎	○	◎	◎	-
	(12) The room in which an information system is installed shall be equipped with receptacles for maintenance work.	-	◎	◎	-	◎	-

(Continued)

Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office	4 Storage room for data and the like	5 Terminal units space	6 Associated facilities
6. Fixtures and utensils	(1) Fixtures and utensils shall be those made of non-flammable materials.	-	◎	○	◎	☆	-
	(2) Each room shall be provided with water-proof cover sheets for equipment associated with the operation of an information system.	-	◎	◎	◎	☆	-
	(3) Clothing, footwear, fixtures, and utensils shall be given preventive measures for the generation of static electricity.	-	◎	☆	◎	-	-
7. Information system	(1) A certain space required for maintenance of information system shall be provided.	-	◎	◎	-	◎	-
	(2) To prevent the leakage of information by the radiowave emission from a computer, terminal and communications units, necessary measures shall be taken.	☆	☆	☆	-	☆	-
	(3) When a water-cooled computer is installed, preventive measures for water leakage shall be taken and a water-leak detector shall be installed at any spot where water leakage might occur.	-	◎	-	-	-	◎
	(4) When a communications unit is installed, disaster- and crime-preventing measures shall be taken.	-	◎	◎	-	◎	-
	(5) When a communications unit is installed, lighting protection measures shall be taken.	◎	-	-	-	◎	-
	(6) The inlet opening for the lead-in communications lines from outside shall be multiplexed and destined for the exclusive use.	☆	-	-	-	-	-
	(7) Communications lines shall be installed in an exclusive wiring space.	-	◎	☆	-	-	-
	(8) Record media shall be given theft-preventing measures.	☆	◎	◎	◎	◎	-
B: Power supply facilities							
1. Installation	(1) Power supply facilities shall be given preventive measures for service interruptions.	-	-	-	-	-	○

(Continued)

Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office	4 Storage room for data and the like	5 Terminal units space	6 Associated facilities
	(2) Power supply facilities for information systems shall be given necessary measures for the fluctuation of voltage and frequency.	-	-	-	-	-	○
	(3) The capacity of power supply facilities for information systems shall have a necessary allowance in view of the load characteristics of each unit.	-	-	-	-	-	◎
	(4) The transformer for an information system shall be exclusively assigned for it.	-	-	-	-	-	○
	(5) The power supply facilities of information systems shall be given necessary measures for suppressing the feedback of alternating transmission current through a line filter to a specified value.	-	-	-	-	-	◎
	(6) When a single-phase unit is connected to the three-phase power source for an information system, measures for preventing faults due to imbalance of units shall be taken.	-	-	-	-	-	◎
	(7) To prevent noise induction in the wiring of an information system, electromagnetic shielding shall be provided.	-	-	-	-	-	◎
	(8) A space for power supply wiring exclusively for an information system shall be provided.	-	-	-	-	-	☆
	(9) Each of distribution boards shall be exclusively assigned to a specified information system and installed in the same room.	-	-	-	-	-	◎
	(10) Each information system shall be independently grounded.	-	-	-	-	-	◎
	(11) An auxiliary power supply facility shall be installed for monitoring, disaster- and crime-preventing facilities.	-	-	-	-	-	◎
2. Disaster- and Crime-preventing measures	(1) Power supply facilities shall be given disaster- and crime-preventing measures.	-	-	-	-	-	◎
	(2) Power supply facilities shall be given lightning protection measures.	-	-	-	-	-	◎

(Continued)

Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office	4 Storage room for data and the like	5 Terminal units space	6 Associated facilities
	(3) The power cables from power supply facilities room to an information system room shall be given measures for fire-, crime-, and noise-prevention. (4) The area where power cable are fed through a fire-preventing wall and the adjacent areas shall be given measures for preventing fire propagation and fume emission. (5) The live parts of distribution boards shall be given preventive measures for electric shocks. (6) The main circuit of a distribution board shall be equipped with a ground fault-detecting and alarming device or an automatic circuit breaker.	-	-	-	-	-	◎
		-	-	-	-	-	◎
		-	-	-	-	-	◎
		-	-	-	-	-	◎
C: Air-conditioning facility							
1. Installation	(1) An air-conditioning facility shall be given measures for maintaining satisfactory room environment with due consideration of ensuring normal operation of an information system and the health of personnel responsible for the operation. (2) The air-conditioning facility for a computer room shall be exclusively assigned to it. (3) The air-conditioning facility for a computer room shall have an allowance in its capacity. (4) The air-conditioning facility for a computer room shall be equipped with an automatic control unit that accurately operates against load fluctuations. (5) The air-conditioning facility for a computer room shall be given anti-freezing measures. (6) The air-conditioning facility for a computer room shall be given measures for controlling water quality.	-	-	-	-	-	◎
		-	-	-	-	-	○
		-	-	-	-	-	○
		-	-	-	-	-	○
		-	-	-	-	-	○
		-	-	-	-	-	○

(Continued)

Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office	4 Storage room for data and the like	5 Terminal units space	6 Associated facilities
2. Disaster- and Crime-preventing measures	(1) Air-conditioning facilities shall be given disaster- and crime-preventing measure.	-	-	-	-	-	○
	(2) Air-conditioning facilities shall be given measures for water leakage, water-leak detector shall be installed at any spot where water leakage might occur.	-	-	-	-	-	○
	(3) The structures of intake and exhaust openings shall be such that rain water does not be induced inside.	-	-	-	-	-	○
	(4) The piping and ducts and the like of air-conditioning facilities shall be made of materials with excellent fire-resistance.	-	-	-	-	-	○
	(5) The area where ducts of air-conditioning facilities are fed through a room shall be given measures for fire prevention and fume protection.	-	-	-	-	-	○
	(6) The thermal insulation material for air-conditioning facilities shall be non-flammable.	-	-	-	-	-	○
D: Monitoring facility	(1) The buildings and rooms in which information systems are installed shall be equipped with a monitoring facility that conducts remote monitoring of persons entering and exiting the buildings and rooms.	-	-	-	-	-	○
	(2) The buildings and rooms in which information systems are installed shall be equipped with a monitoring facility that conducts remote monitoring of the operation of disaster- and crime-preventing facilities.	-	-	-	-	-	○
	(3) A facility that conducts remote monitoring of the operating status of power supply and air-conditioning facilities shall be installed.	-	-	-	-	-	○
	(4) A facility that monitors the service status and eventual faults of communications lines shall be installed.	-	-	-	-	-	○

(Continued)



Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office and the like	4 Storage room for data	5 Terminal units space	6 Associated facilities
E: Preventive measures for earthquake damages							
a. Installation environment							
1. Site and layout	(1) Buildings shall be located where damages of earthquake due to active dislocations is not feared. (2) Rooms shall be located where little damages of earthquake is conceived. (3) When backup buildings and rooms are constructed as a provision for disasters, they shall be located remote from the main buildings and rooms.	☆	-	-	-	-	-
		-	◎	☆	◎	☆	-
		☆	☆	☆	☆	-	-
2. Structure	(1) Building shall be the earthquake proof properties stipulated by the Building Standards Law.	◎	-	-	-	-	-
3. Opening areas	(1) The door of entrance/exit of a building and room shall be of fire-proof door with sufficient strength. (2) The windows of buildings and rooms shall be given measures for preventing the breakage scattering and falling of the panes.	◎	◎	☆	◎	☆	-
		☆	◎	◎	◎	◎	-
4. Interior structures and furnishings	(1) The interior structures, furnishings and lighting fittings of a building and room shall be given preventive measures for falling and damages in the event of an earthquake. (2) The free-access floor of a room shall be of earthquake-proof or earthquake-resistant structure.	◎	◎	◎	◎	◎	-
		-	◎	◎	◎	☆	-
5. Facilities	(1) A facility that detects earthquakes and controls the operation of information systems and the like shall be installed.	-	-	-	-	-	☆

(Continued)

Item	Item of measures	Application classification					
		1 Building	2 Computer room	3 Office	4 Storage room for data and the like	5 Terminal units space	6 Associated facilities
	(2) An emergency communications facility as a provision for the event of disasters shall be installed in each room. (3) An auxiliary water supply facility as a provision for disasters shall be installed.	-	◎	☆	☆	◎	-
		☆	-	-	-	-	-
6. Fixtures and utensils	(1) Fixtures and utensils shall be given measures for preventing moving and falling which are appropriate for their locations. (2) The glass components of fixtures and utensils shall be given measures for preventing their breakage, scattering, and falling. (3) Record media, documents and the like shall be given measures for preventing moving and falling which are appropriate for their locations.	-	◎	◎	◎	-	-
		-	○	○	○	-	-
		-	◎	◎	◎	-	-
7. Information systems	(1) Information systems shall be given measures for preventing moving, falling, and vibration which are appropriate for their installed locations. (2) When a backup information system as a provision for disasters is installed, it shall be located remote from the main system.	-	◎	◎	-	○	-
		-	☆	☆	-	-	-
b. Power supply facilities	(1) Power supply systems shall be given measures for preventing moving, falling, and vibration which are appropriate for their installed locations. (2) An in-house power generating facility shall be installed as a provision for service interruptions in the event of disaster occurrence.	-	-	-	-	-	◎
		-	-	-	-	-	☆
c. Air-conditioning facilities	(1) Air-conditioning facilities shall be given measures for preventing moving, falling, and vibration which are appropriate for their installed locations.	-	-	-	-	-	◎
d. Monitoring facility	(1) A monitoring facility shall be given measures for moving, falling, and vibration which are appropriate for their installed locations.	-	-	-	-	-	◎

## 6. Technical Standards

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
A: Application of information technology	(1) The safety functions by means of information technology shall be employed in accordance with the form of centralized or decentralized processing of an information system.	◎	◎	◎
	(2) The products of information technology shall be pertinently utilized by evaluating and confirming the safety functions.	◎	◎	◎
B: Functions of disaster- and fault-preventing measures				
1. Functions of disaster-preventing measures	(1) An information system shall be provided with required functions for replacement operation.	◎	○	☆
	(2) A function that performs restoration of data and programs shall be installed.	◎	○	☆
	(3) A backup function that is activated within the recovery allowance time shall be installed.	◎	○	☆
	(4) A functions that backs up an information system at a remote location shall be installed.	☆	☆	☆
2. Functions of fault-preventing measures	(1) A data error detecting function shall be installed.	◎	◎	○
	(2) A function that detects fault spot in an information system and allows the system to independently resume operation in accordance with its form of centralized or decentralized processing system shall be installed.	◎	◎	○
	(3) A functions that restores operation after an outage due to a fault of an information system in accordance with its form of centralized or decentralized processing system shall be installed.	◎	◎	○

(Continued)

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
3. Maintenance functions	(1) A function that analyzes the nature of a fault and identifies the fault spot shall be installed.	◎	◎	○
	(2) A function that performs maintenance without interrupting an information system shall be installed.	○	○	☆
	(3) A function that performs maintenance operation under remote control shall be installed.	○	○	☆
4. Operation support functions	(1) A function that monitors the operation status of an information system for eventual faults and controls the operation shall be installed.	○	○	☆
	(2) A function that automatically operates shall be installed.	○	○	☆
C: Functions of preventive measures for deliberate or erroneous mistakes				
1. Access control functions	(1) A function that determines the extent of confidentiality of the resources of an information system in accordance with the form of centralized or decentralized processing shall be installed.	◎	◎	○
	(2) A function that conducts the registration and management of users of an information system in accordance with the form of centralized or decentralized processing shall be installed.	◎	◎	◎
	(3) A function that identifies and verifies the validity of users who have access to an information system and its resources in accordance with the form of centralized or decentralized processing shall be installed.	◎	◎	○
	(4) A function that controls the access authority to an information system and its resources in accordance with the form of centralized or decentralized processing shall be installed.	◎	◎	○

(Continued)

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
	(5) A function that monitors access status shall be installed.	◎	◎	☆
2. Functions preventing illegal data processing	(1) A function that detects illegal data revision in accordance with the form of centralized or decentralized processing shall be installed.	◎	◎	☆
	(2) A function that detects illegal data revision and execution in accordance with the form of centralized or decentralized processing shall be installed.	○	○	☆
	(3) A function that bypasses or interrupts operation in accordance with the form of centralized or decentralized processing when it detects illegal data revision and program execution.	○	○	☆
	(4) A function that protects common resources shall be installed.	◎	◎	◎
3. Information leakage preventing functions	(1) A function that prevents information leakage by the radiowave emission from a computer, terminal and communications units shall be installed.	☆	☆	☆
	(2) A function that encodes files and transmitted information shall be installed.	○	○	○
D: Auditing function	(1) An auditing function for an information system shall be installed.	○	○	☆

## 7. Operating Standards

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
<b>A: Planning</b>				
1. Operating plan for information systems	(1) The operating plan for an information system shall be formulated in accordance with the form of centralized or decentralized processing. (2) The managing plan for the modification of the constituent units as well as the revision and modification of software of an information system shall be formulated in accordance with the form of centralized or decentralized processing. (3) An operating plan shall comprise the safety measures for disasters, faults, deliberate and erroneous mistakes on the basis of risk evaluation.	◎  ◎  ◎	◎  ◎  ◎	○  ◎  ◎
2. Managing plan for data and the like	(1) Data and the like shall be classified in accordance with the extent of confidentiality and importance, and a managing plan for retention, utilization, distribution, take-out, take-in, storage, erase, deletion, etc. shall be formulated. (2) For the creation, updating, copying, removal, transfer and the like of data, a managing plan shall be formulated in accordance with the form of centralized or decentralized processing.	◎  ◎	◎  ◎	◎  ◎
3. Organization and administration regulations	(1) The organizations for performing smooth operations of an information system and for being prepared for disasters shall be created. (2) In the operation of information systems and the like, the sharing and definition of responsibilities shall be clarified. (3) An administration regulation concerning the operation shall be established and an administrator shall be appointed in accordance with the form of centralized or decentralized processing in an information system.	◎  ◎  ◎	◎  ◎  ◎	◎  ◎  ○

(Continued)

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
	(4) An administration regulation concerning the use and storage of data as well as record media and an administrator shall be appointed. (5) An administration regulation concerning the entrance/withdrawal in/from buildings and rooms shall be established and an administrator shall be appointed. (6) An administration regulation concerning disaster- and crime-prevention shall be established and an administrator shall be appointed. (7) An administration regulation concerning associated facilities, disaster- and crime-preventing facilities shall be established and an administrator shall be appointed.	◎ ◎ ◎ ◎	◎ ◎ ◎ ◎	○ ☆ ○ ○
4. Disaster action plans	(1) An disaster operation manual stipulating the replacement operation and restoration measures for an information system shall be established. (2) Services shall be conducted by setting a recovery allowance time and the priority order for resumption. (3) A personnel assignment plan shall be established.	○ ○ ◎	○ ○ ◎	○ ○ ☆
B: Operation of information systems				
1. Systems administration	(1) Detailed rules of information systems and data in accordance with the form of centralized or decentralized processing shall be established. (2) In the modification of constituent units and the revision and modification of software, measures for preventing adverse influence on the normal operation of an information system shall be taken in accordance with the form of centralized or decentralized processing.	○ ◎	○ ○	○ ○

(Continued)

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
	(3) The monitoring, control and recording of operation shall be conducted in accordance with the form of centralized or decentralized processing, and the status of daily operation shall be analyzed.	◎	◎	☆
	(4) The results of access monitoring shall be analyzed, and measures for preventing illegal actions shall be taken in accordance with the form of centralized or decentralized processing.	◎	○	☆
	(5) The keys of constituent units of an information systems shall be administered by appointed personnel.	◎	◎	○
	(6) The faults of information systems shall be analyzed, and necessary measures for preventing the recurrence shall be taken.	◎	◎	◎
	(7) The details and results of the maintenance of information systems shall be investigated and analyzed.	◎	◎	◎
	(8) In the maintenance of information systems, necessary measures for protecting data shall be taken in accordance with the form of centralized or decentralized processing.	◎	◎	◎
	(9) Terminal units shall be pertinently administered in accordance with their usage and installed environment.	◎	◎	◎
2. Users management	(1) Users' manual shall be compiled in accordance with the form of centralized or decentralized processing, and the users shall be ensured to observe the contents of the manual.	◎	◎	◎
	(2) The users' access authority for information systems shall be stipulated in accordance with the form of centralized or decentralized processing.	◎	○	☆
	(3) The users' passwords, identification codes and the like for information systems shall be controlled in accordance with the form of centralized or decentralized processing.	◎	○	☆
	(4) The qualifications of the users of information systems shall be determined in accordance with the form of centralized or decentralized processing.	☆	☆	☆

(Continued)



Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
3. Operation	(1) The operation manual of information systems based on the tasks processing schedule shall be constantly maintained.	◎	◎	○
	(2) The operation manual and operation guide for terminal units shall be constantly maintained in accordance with the form of centralized or decentralized processing.	◎	◎	◎
	(3) A manual prescribing the actions and recovery procedure required in the event of fault occurrence shall be constantly maintained.	◎	○	☆
4. Actions for disaster occurrence	(1) When a disaster occurs, the extent of damages in information systems and the like shall be promptly investigated and analyzed in accordance with the disaster action plans.	◎	◎	○
	(2) In proportion to the extent of damages, the service resumption methods shall be determined in accordance with the predetermined disaster operation manual.	◎	◎	○
C: Storage and usage of data and the like and record media				
1. Administration	(1) Detailed rules of storage and usage of data and the like and record media in accordance with the form of centralized or decentralized processing.	◎	◎	◎
2. Storage	(1) Data and the like and record media shall be stored in specified places in accordance with the form of centralized or decentralized processing.	◎	◎	◎
	(2) The keys of recording media shall be administered by appointed personnel.	○	○	○
	(3) The storage status of record media shall be periodically inspected by appointed personnel.	◎	○	○

(Continued)

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
3. Usage	(1) The handling as well as handing over of data and the like and record media shall be conducted by specified methods. (2) An administration record shall be maintained for the creation, addition, updating, copying, deletion and the like.	◎	◎	○
4. Crime-preventing measures	(1) In order to prevent the illegal take-out and illegal use of data and the like and record media, responsible administrators shall inspect the status of their usage. (2) The administration of the coded keys of data and the like shall be conducted by appointed personnel.	◎	◎	◎
5. Measures for preventing disasters and faults	(1) The decentralized storage of record media shall be conducted in accordance with the form of centralized or decentralized processing. (2) The backup of data and the like shall be conducted.	○	○	○
D: Entrance/withdrawal in/from buildings/rooms				
1. Personnel entrance/withdrawal	(1) In accordance with the form of centralized or decentralized processing, detailed rules of authorization shall be established for the entrance/withdrawal in/from buildings and rooms in which information systems and the like are installed. (2) In order to control the entrance/withdrawal in/from buildings and rooms, an examination of the personnel who enter/withdraw in/from buildings and rooms shall be conducted for authorization and an authorized identification card shall be issued to them. (3) Personnel who is/are temporarily authorized for the entrance in buildings and rooms shall be escorted by an authorized attendant as required, and the entrance areas shall be restricted to specified areas only.	◎	◎	◎

(Continued)

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
	(4) Depending on the importance of a building or a room, the entrance and withdrawal shall be recorded. (5) The administration of keys of entrance is conducted by recording the locking and unlocking of entrance as well as the storage and handing over of the keys.	◎ ◎	◎ ◎	○ ○
2. Articles carried in/out	(1) The articles carried in/out from each room for operation of information systems and the like shall be limited to those required only. (2) The contents or details of articles carried in/out shall be inspected and recorded.	◎ ○	◎ ○	◎ ☆
E: Associated facilities, disaster- and crime-preventing facilities				
1. Administration	(1) In the modification or extension of associated facilities, disaster- and crime-preventing facilities, necessary measures for preventing adverse influence on the normal operation of information systems shall be taken. (2) The periodical inspection of associated facilities, disaster- and crime-preventing facilities and subsequent examination and analysis of the results shall be conducted. (3) The faults of associated facilities, disaster- and crime-preventing facilities shall be investigated and analyzed, and necessary measures for preventing the recurrence shall be taken.	◎ ◎ ◎	○ ○ ◎	☆ ☆ ○
2. Operation	(1) The operation and maintenance of associated facilities, disaster- and crime-preventing facilities shall be conducted by appointed personnel. (2) The operation manual prescribing the necessary actions in the event of disaster or faults as well as in normal conditions of associated facilities, disaster- and crime-preventing facilities shall be constantly maintained.	◎ ◎	◎ ○	☆ ☆

(Continued)

Item	Item of measures	Application according to user classification		
		1 Non-specific	2 Within a specific company	3 Within a specific departments
3. Monitoring	(1) In response to the change in operation status of an information system, the operation of power supply and air-conditioning facilities shall be controlled by means of monitoring facility. (2) The monitored data of power supply and air-conditioning facilities shall be recorded and subsequently analyzed. (3) In order to ensure the disaster- and crime-prevention, the patrol shall be exercised in the buildings and rooms.	<input checked="" type="radio"/>   <input checked="" type="radio"/>  <input type="radio"/>	<input checked="" type="radio"/>   <input checked="" type="radio"/>  <input type="radio"/>	<input type="radio"/>   <input type="radio"/>  <input checked="" type="radio"/>
F: Personnel	(1) The administration of personnel stationing and shift shall be pertinently conducted in accordance with the form of centralized or decentralized processing. (2) In order to allow the personnel to be versed in regulations and manuals relevant to safety measures, education and training courses shall be executed. (3) Education and training courses in accordance with the disaster action plan shall be conducted.	<input checked="" type="radio"/>   <input checked="" type="radio"/>  <input checked="" type="radio"/>	<input checked="" type="radio"/>   <input checked="" type="radio"/>  <input checked="" type="radio"/>	<input checked="" type="radio"/>   <input checked="" type="radio"/>  <input checked="" type="radio"/>
G: Commissioning	(1) When the operation and administration work for information systems is commissioned to an external organ, a work commissioning agreement comprising items of safety measures shall be concluded. (2) The implemented status of safety measures at the commissioned party's premises shall be confirmed. (3) When the backup of an information system is commissioned to an external organ, periodical tests of switching, activation, returning and the like shall be conducted.	<input checked="" type="radio"/>   <input checked="" type="radio"/>  <input type="radio"/>	<input checked="" type="radio"/>   <input checked="" type="radio"/>  <input type="radio"/>	<input checked="" type="radio"/>   <input checked="" type="radio"/>  <input type="radio"/>
H: Systems auditing	(1) The report on the systems auditing of safety measures shall be received, and necessary measures shall be taken. (2) The report on the systems auditing concerning disaster action plans shall be received, and necessary measures shall be taken.	<input checked="" type="radio"/>  <input checked="" type="radio"/>	<input type="radio"/>  <input type="radio"/>	<input type="radio"/>  <input type="radio"/>

## 8. Facts To Be Considered

- (1) For successful application of the Standards, optimum combination of items of measures should be examined on the basis of risk assessment, and due consideration shall be given to the balance of restrictions incurred by the implementation of measures and the benefits or serviceability of information systems.
- (2) As to the items of measures for earthquakes, the largest possible magnitude of earthquake disasters shall be assumed and necessary measures shall be taken. Among the earthquake measures, those assumed for a disaster may be appropriated for other large scale disasters such as flood, fire, and explosion.
- (3) Since the Technical Standards mainly describe the functions of the systems, in the implementation of each item of measures, the hardware and software required for the realization of those functions and pertinent operation shall be endeavored.
- (4) For the execution of systems auditing, the "Systems Auditing Standards" shall be applied.
- (5) As to the implementation of measures for computer viruses, the "Computer Viruses Measure Standards" shall be applied.

## IV. System Audit Standards (Tentative translation)

### 1. Purpose

The purpose of the Standards is to improve the reliability, security, and efficiency of information systems and thus contribute to the realization of a healthy information society by enumerating the matters necessary for system audits.

### 2. Definitions of Terms

These are the principal terms used in the Standards:

(1) System audit: A series of activities in which a system auditor, an impartial position independent of the object of audit, performs overall inspection and evaluation of an information system, issues advice and recommendations, and provides any necessary follow-up.

(2) System auditor: A person who engages in system audits with the following knowledge and abilities:

① Basic knowledge of information

systems

② Knowledge of system audits

③ Ability to perform system audits

④ Related knowledge for the performance of system audits

(3) Improvement of reliability: To improve the quality of information systems, prevent failure, minimize the effects of failure, and speed up recovery

(4) Improvement of security: To make an information system more secure from natural disasters, unauthorized access, and destructive actions

(5) Improvement of efficiency: To improve the cost performance of an information system by making the most of its resources

(6) Audited division: A division that is an object of a system audit

(7) Basic plan: An general plan of system audits to be performed

during any given year

- (8) Individual plan: A plan for any of the individual system audit operations based on a basic plan
- (9) Risk analysis: To identify the risks that may arise from or in connection with the use of an information system and analyze the degrees of their effects
- (10) Matter noted: A problem pointed out by a system auditor according to his or her criteria and noted on a system audit report
- (11) Recommendation of improvement: A matter noted that is judged by a system auditor as requiring improvement and noted as such on a system audit report
- (12) Follow-up: The measure or measures taken by a system auditor to ensure the audited division carries out any recommendations of improvement

### **3. Composition of the Standards**

The Standards are composed of General Standards, Implementation Standards, and Reporting Standards, which break down as follows:

#### **(1) General Standards (9 items)**

General Standards outline the principles of an audit plan that provides a basis for a system audit, the qualifications of a system auditor, and so forth.

#### **(2) Implementation Standards (191 items)**

Implementation Standards outline the audit items concerning planning, development, operation, maintenance, and common work of the processes of constructing and operating the information system being audited.

#### **(3) Reporting Standards (8 items)**

Reporting Standards outline the process of compiling the audit results and the measures to be taken based on the results.

### **4. Philosophy behind the Implementation Standards**

(1) The Implementation Standards must be capable of being applied both to centralized processing and to distributed processing.

(2) The Implementation Standards must be capable of being applied without regard to the method of development.

(3) Planning must cover subjects ranging from information strategy to the definition of requirements.

(4) Development must cover subjects ranging from system design to system conversion.

(5) Operation must cover the management of the software, hardware, networks, buildings, and so on related to information system operation.

(6) Maintenance must cover subjects related to software modification, ranging from a maintenance plan to disposal of the old system.

(7) A major system change shall be treated as planning and development.

(8) Common work shall consist of work required in common for planning, development, operation, and maintenance as well as measures against disasters.

(9) Criteria for common work must be considered and applied in the audit of planning, development, operation, and maintenance.

The criteria for common work can be applied independently.

(10) The Implementation Standards must be applied properly in accordance with the actual conditions of an organization.

## **5. General Standards**

### **1. System**

(1) The organization must prepare a system that can ensure the proper implementation of a system audit.

### **2. Audit Plan**

(1) The system auditor shall formulate a basic plan and individual plans for a system audit.

(2) The system audit shall be implemented according to the individual plan and in the order preliminary inspection, full inspection, evaluation, and conclusion.

### **3. Responsibility and Authority of the System Auditor**

(1) The system auditor shall make the grounds for each of his or her judgments clear.

(2) The system auditor may demand data and materials from the audited division.



- (3) The system auditor may demand a report on the implementation of improvement be issued by the head of an organization to an audited division.

#### **4. Professional Ethics**

- (1) The system auditor shall firmly maintain his or her position as an impartial evaluator.
- (2) The system auditor shall be aware of the ethical demands on himself or herself and meet the internal and external trust by performing an accurate and sincere system audit.

#### **5. Confidentiality**

- (1) The system auditor must not, without good reason, divulge any secret he or she may come to know in the course of performing his or her job or use such secret for any undue purpose.

#### **6. Implementation Standards**

##### **I. Planning**

##### **1. Information Strategy**

- (1) Has an information strategy been worked out consistent with man-

agement strategy?

- (2) Has the policy been made clear for the standardization of planning, development, operation, and maintenance of an information system?

- (3) Has the validity of an information strategy been evaluated?

##### **2. Formulation of a General Plan**

- (1) Has the system for formulating a general plan been fully established and approved by the head of the organization?

- (2) Has the general plan been formulated according to general plan formulation rules and approved by the head of the organization?

- (3) Does the general plan make clear the effects, promotion, expenses, etc. of the information system?

- (4) Does the general plan make clear the general image of the information system?

- (5) Does the general plan make the priority of system development clear?

- (6) Does the general plan make clear

the policy for changes in the organization and for alteration, creation, and abolishment of operations that may arise from system development?

- (7) Does the general plan make the security policy clear?
- (8) Does the general plan include periodic review in response to changes in the management environment and the like?

### **3. Formulation of a Development Plan**

- (1) Does the development plan make clear the purpose, the objects of development, costs and benefits, and so on?
- (2) Have the conditions been made clear for the setting of the life cycle of an information system?
- (3) Has the development plan been formulated based on the results of domestic and overseas surveys of information technologies?
- (4) Has the development strategy been worked out in consideration of its consistency with the general plan?
- (5) Has the development plan been

approved by the head of the organization?

### **4. System Analysis and Definitions of Requirements**

- (1) Have the definitions of requirements under the development plan been approved by the persons in charge of the development and user divisions?
- (2) Does a survey of user needs have clearly defined objects, scope and method?
- (3) Has the analysis of the present conditions been done by users who are versed in practical business?
- (4) Has analysis been made of the risks that may arise from or in connection with the installation of the information system?
- (5) Has a survey been made of all the laws and regulations related to information systems?
- (6) Has a review or other study been made of the operations, management system, regulations, and others that will be affected by the installation of the information system?

- (7) Has the division of roles been made clear between the user division and the information system division?
- (8) Have hardware, software, networks, and the like selected in accordance with a development plan and user needs?
- (9) Has a realistic alternative plan for the achievement of the purpose of an information system been prepared and studied?
- (10) Has the method of development been determined in consideration of the scale and period of development and system characteristics?
- (11) Have the bases of calculation of the development and operation expenses been made clear?
- (12) Have the effects of an information system been evaluated quantitatively and qualitatively?
- (13) Have the personnel, money, facilities, time, and others required for the execution of development been secured?
- (1) Have the development procedures been prepared according to the method of development?
- (2) Have the development procedures been determined from the scale of development and so forth?
- (3) Have the development procedures been approved by the person in charge of development?

## 2. System Design

- (1) Have the design sheets been approved by the persons in charge of development and user divisions?
- (2) Has the system been designed in a way to ensure data integrity?
- (3) Has the system configuration been designed in anticipation of peak use?
- (4) Have the I/O documents, I/O screens, and so on been designed in a way that can be used easily?
- (5) Have the databases been designed appropriately for business?
- (6) Have the networks been designed appropriately for business?

## II. Development

### 1. Development Procedures

(7) Has the performance of the information system been designed in a way to meet the requirements defined?

(8) Have measures been taken against an information system failure?

(9) Have technical methods been designed for realization of the performance management required for operation?

(10) Have functions been designed to prevent unauthorized access, protect confidentiality, and so on?

(11) Have the a purpose, scope, method, schedule, and other details been set for a test plan?

(12) Have the education policy, schedule, and other details been set for using the information system?

### **3. Program Design**

(1) Have the program specifications been approved by the person in charge of development?

(2) Have programs been designed according to system design sheets?

(3) Have any system design inconsistencies found during system design been solved through a review of that system design?

### **4. Programming**

(1) Has it been verified that programming is done according to program specifications?

(2) Have the results of program tests been recorded and stored?

(3) Have important programs been tested by a person other than the person who wrote it?

### **5. System Tests**

(1) Have test data been prepared and system tests made according to the test plan?

(2) Have system tests been done by a person who is in a fair and impartial position?

(3) Have system tests been done according to the user manual?

(4) Have the results of system tests been approved by the persons in charge of development, operation, maintenance, and user divisions?

(5) Have the results of system tests

been recorded and stored?

## **6. Conversion**

(1) Have a conversion plan and the operation plan accompanying it been formulated?

(2) Have the personnel, money, facilities, and others required for conversion been secured in accordance with the conversion plan?

(3) Has the method of verifying the completion of conversion been made clear?

(4) Has an implementation plan been formulated for operation following conversion?

## **III. Operation**

### **1. Operation Control**

(1) Have operation control rules been established and observed?

(2) Have operation procedures been made clear and have measures against accidents and failures been made clear?

(3) Have job schedules been set considering the priority of processing?

(4) Have operations been conducted according to the job schedule and instruction sheets?

(5) Have exceptional treatment operations been conducted according to operation control rules?

(6) Have operator changes been done according to operation control rules?

(7) Has an analysis been made of the differences between job schedules and operation records?

(8) Have the information system operation records been grasped for performance management and effective use of resources?

(9) Have operation records been stored for a certain period according to operation control rules?

(10) Have accidents and failures been recorded and reported to the person in charge of information system operation?

(11) Have the causes of accidents and failures been clarified and measures taken to prevent their recurrence?

(12) Have measures been taken to

prevent unauthorized acts and protect confidentiality in managing identification codes and passwords?

- (13) Have users been provided with education and training concerning information system security?

## **2. Input Management**

- (1) Have input management rules been established and observed?

- (2) Have measures been taken to prevent errors and unauthorized acts and to protect confidentiality in input data preparation procedures, handling, and so on?

- (3) Has data been entered according to input management rules?

- (4) Have the measures for data input error prevention, unauthorized act prevention, and confidentiality protection been functioning effectively?

- (5) Has entered data been stored and discarded according to input management rules?

## **3. Data Management**

- (1) Have data management rules been established and observed?

- (2) Are data access control and monitoring functioning effectively?

- (3) Has the state of data use been recorded and analyzed periodically?

- (4) Have the scope and timing of data backup been determined in consideration of the contents of operations, the form of processing, and the method of recovery?

- (5) Has data been delivered and received according to data management rules?

- (6) Have measures been taken to prevent unauthorized acts and protect confidentiality in data exchanges?

- (7) Have measures been taken to prevent unauthorized acts and protect confidentiality in data storage and disposal?

- (8) Have measures been taken to prevent unauthorized acts and protect confidentiality in the copying of data?

- (9) Have measures been taken for data against computer viruses?

- (10) Have intellectual property rights for data been protected?

#### **4. Output Management**

- (1) Have output management rules been established and observed?
- (2) Have measures been taken to prevent unauthorized acts and protect confidentiality in preparing and handling output information procedure?
- (3) Has output information been delivered according to output management rules?
- (4) Has output information been stored and discarded according to output management rules?
- (5) Have output information errors been recorded and analyzed periodically?
- (6) Has the state of output information use been recorded and analyzed periodically?

#### **5. Software Management**

- (1) Have software management rules been established and observed?
- (2) Have control and monitoring of software access been functioning effectively?
- (3) Has the state of software use been

recorded and analyzed periodically?

- (4) Have the scope and the method of software backup been determined in consideration of the contents of operations and the form of processing?
- (5) Has software been delivered and received according to data management rules?
- (6) Have measures been taken to prevent unauthorized acts and protect the confidentiality in software storage and disposal?
- (7) Have measures been taken for the prevention of unauthorized acts and the protection of confidentiality in the copying of software?
- (8) Have measures been taken for software against computer viruses?

- (9) Have intellectual property rights for software been protected?

#### **6. Hardware Management**

- (1) Have hardware management rules been established and observed?
- (2) Has hardware been installed in

an environment in which anticipated risks can be avoided?

(3) Has hardware been maintained periodically?

(4) Have measures been taken against hardware failure?

(5) Has the state of hardware use been recorded and analyzed periodically?

## **7. Network Management**

(1) Have network management rules been established and observed?

(2) Have network access control and monitoring been functioning effectively?

(3) Has the state of network use been recorded and analyzed periodically?

## **8. Configuration Management**

(1) Has the scope of software, hardware, and network to be managed been made clear?

(2) Have the configurations, suppliers, and support conditions of software, hardware, and networks been made clear?

(3) Has the scope to be affected by the installation and modifications of software, hardware, and networks been studied?

(4) Have the installation and modifications of software, hardware, and networks been executed according to plan?

## **9. Management of Buildings and Related Facilities**

(1) Have buildings and related facilities been installed in an environment in which anticipated risks can be avoided?

(2) Have measures been taken to prevent unauthorized acts and protect confidentiality in controlling entry into and exit from buildings and rooms?

(3) Have related facilities been maintained periodically?

(4) Have measures been taken against failure of related facilities?

## **IV. Maintenance**

### **1. Maintenance Procedures**

(1) Have necessary maintenance documents been taken over from



the person in charge of development according to take-over rules?

- (2) Have maintenance procedures been determined in consideration of the scale and period of maintenance, system characteristics, and so on?
- (3) Have the maintenance procedures been approved by the person in charge of maintenance?

## **2. Maintenance Plan**

- (1) Have a survey and analysis been made of the contents of maintenance and the scope affected by dealing with requests for modifications and the like?
- (2) Have maintenance plans been formulated based on the results of a survey and analysis and approved by the persons in charge of maintenance and user divisions?
- (3) Have the purpose, scope, method, schedule, and other details been set for a maintenance test plan?

## **3. Implementation of Maintenance**

- (1) Have system design sheets, pro-

gram specifications, and the like changed according to maintenance plans and approved by the persons in charge of maintenance and user divisions?

- (2) Have program changes been made according to maintenance procedures and with the approval of the person in charge of maintenance?
- (3) Has it been verified that programming is performed according to changed program specifications?

## **4. Confirmation of Maintenance**

- (1) Have changed programs been tested according to maintenance test plans?
- (2) Is the testing done on changed programs similar in level to the testing done in new development?
- (3) Has the testing of changed programs been participated in by users and conducted according to the user manual?
- (4) Have the results of tests of changed programs been approved by the persons in charge of the development, operation, maintenance,

nance, and user divisions?

- (5) Have the results of tests of changed programs been recorded and stored?

## **5. System Conversion**

- (1) Have conversion procedures been prepared in consideration of the conditions of conversion?
- (2) Have the pre-change programs and data been backed up prior to conversion?
- (3) Does the person in charge of conversion verify that the conversion does not affect any other systems?

## **6. Disposal of Old Systems**

- (1) Have old systems been disposed of according to the disposal plan, approved by the persons in charge of operation and user divisions?
- (2) Have the method and the time of disposal of the old system been determined in consideration of preventing unauthorized acts and protecting confidentiality?

# **V. Common Work**

## **1. Document Management**

### **1. Preparation**

- (1) Have document preparation rules been established and observed?
- (2) Have document preparation plans been formulated?
- (3) Have the kinds, purposes, methods of preparation, and other details of documents been made clear?
- (4) Have documents been prepared according to preparation plans?
- (5) Have documents been approved by the persons in charge of the information system division and the related user divisions?

### **2. Management**

- (1) Have document management rules been established and observed?
- (2) Have the contents of documents been updated and an update history recorded in response to system changes?
- (3) Have the contents of updated documents been approved by the persons in charge of the information system division and the related user divisions?

(4) Have measures been taken to prevent unauthorized acts and protect confidentiality in the storage and disposal of documents?

(5) Have measures been taken to prevent unauthorized acts and protect confidentiality in the copying of documents?

## **2. Progress Management**

### **1. Implementation**

(1) Have the method or system of managing progress been determined and approved by the person in charge of the information system division?

(2) Do the persons in charge of planning, development, operation, and maintenance grasp the state of progress?

(3) Have measures been taken to solve problems such as a delay in progress?

### **2. Evaluation**

(1) Have the results been analyzed and evaluated in comparison with plans at the end of the operating process?

(2) Have the results of the evalua-

tion been reflected in planning the next process?

(3) Have the results of the evaluation been reflected in improving the method, system, etc. of progress management?

## **3. Personnel Management**

### **1. Responsibility and Authority**

(1) Have the responsibilities and authorities of personnel been determined according to the characteristics of planning, development, operation, and maintenance?

(2) Have the responsibilities and authorities of personnel been reviewed in response to changes in the information environment?

(3) Have the responsibilities and authorities of personnel been thoroughly made known?

### **2. Implementation of Work**

(1) Have personnel been faithfully observing their authorities?

(2) Have the division of work and the volume of work been studied from the viewpoint of personnel's knowledge, abilities, and so on?

(3) Has the changing of personnel been studied from the viewpoint of unauthorized acts and the protection of confidentiality?

(4) Has the securing of substitute personnel been studied in preparation for unexpected events?

### 3. Education and Training

(1) Have education and training curriculums been prepared and reviewed in line with an information strategy?

(2) Have education and training curriculums been studied from the viewpoint of improving technical capabilities, acquiring business knowledge, securing information system security, and so on?

(3) Have education and training been conducted periodically and effectively in line with curriculums?

(4) Has a career path been established for personnel and reviewed in response to changes in the information environment?

### 4. Health Management

(1) Is the work environment prepared in terms of health management?

(2) Have health checkup and coun-

seling been performed?

## 4. Outsourcing

### 1. Outsourcing Plan

(1) Have the purpose and the scope of outsourcing been made clear?

(2) Has outsourcing been determined based on the evaluation of concrete effects, problems, and so forth?

(3) Have outsourcing plans been formulated and approved by the person in charge of outsourcing?

### 2. Selection of Service Providers

(1) Have the criteria for selecting service providers been made clear?

(2) Have the service conditions offered by several prospective service providers been compared?

### 3. Service Agreements

(1) Have service agreements been concluded according to outsourcing rules?

(2) Have measures been made clear for preventing unauthorized acts, protect confidentiality, and soon?

(3) Has it been made clear to whom intellectual property rights belong to?

(4) Have special provisions and exemptions been made clear?

#### 4. Contents of Services

(1) Do the contents of the services provided correspond exactly to the contents of the agreement?

(2) Has the progress of the work under a service agreement been grasped, and measures taken against delay?

(3) Have the conditions for implementing measures to prevent unauthorized acts, protect confidentiality, and so forth on the side of the service providers been grasped under the service agreement, and measures taken against problems?

(4) Have the results of service been inspected and received according to the service agreement?

(5) Have the results of service been analyzed and evaluated?

#### 5. Measures against Disasters

##### 1. Risk Analysis

(1) Have the risks such as earthquakes and the scope of their effects on the information system been made clear?

(2) Has the loss the organization would suffer from a halt or the like of the information system been analyzed?

(3) Have the time permissible for recovery of operation and the order of priority of recovery been determined?

##### 2. Anti-Disaster Plan

(1) Has an anti-disaster plan been formulated based on the results of risk analysis and approved by the head of the organization?

(2) Can the anti-disaster plan be materialized?

(3) Has training been conducted periodically in line with the anti-disaster plan?

(4) Has the an anti-disaster plan reviewed from time to time?

##### 3. Backup

(1) Have the method and the procedures for backing up an information system, data, and related

facilities been determined in response to a operation recovery target?

- (2) Have the method and the procedures of backup been verified by the person in charge of operation?

#### 4. Alternative Processing and Recovery

- (1) Have alternative processing procedures and the system to be used until recovery been determined and verified by the persons in charge of the operation and user divisions?

- (2) Have recovery procedures and system been determined and verified by the persons in charge of the operation and user divisions?

## 6. Reporting Standards

### 1. Preparation of Reports

- (1) The system auditor must prepare a system audit report.
- (2) The system audit report must state the results of evaluation of the reliability, security, and efficiency of an information system.

- (3) The system audit report must state, as matters noted, the problems based on the results of the audit.

- (4) The system audit report must state, as recommendations of improvement, the important matters that need to be improved.

- (5) The system audit report must state improvements that can be proposed for the matters that need to be improved.

- (6) The system auditor must state on his or her system audit report any other matters he or she considers necessary.

### 2. Reporting

- (1) The system audit report must be submitted to the head of the organization.

### 3. Follow-up

- (1) The system auditor must try to grasp the progress of improvement made based on recommendations of improvement and promote that improvement.

**Back Issues of JIPDEC Informatization Quarterly  
(Formerly Japan Computer Quarterly) are as follows:**

**Published in 1995**

- No. 102: Mobile Communications and All about PHS
- No. 101: The 9th Japan-Germany Forum on Information Technology
- No. 100: Recommendations for G7 Conference and Program for Advanced Industrial Information Infrastructure

**Published in 1994**

- No. 99: EDI Development in Japan
- No. 98: Program for Advanced Information Infrastructure
- No. 97: The Computer System and Patent Information at the Japanese Patent Office
- No. 96: Informatization of Home Life in Japan

**Published in 1993**

- No. 95: Informatization Policy in Japan
- 94: Cutting-Edge New-Media Technologies in Japan
- 93: Fifth Generation Computer Systems (FGCS) Project in Japan
- 92: Hypermedia in Japan

**Published in 1992**

- No. 91: Japanese ISDN: Present and Future
- 90: Regional Informatization in Japan
- 89: Real World Computing & Related Technologies
- 88: Information-related Examinations in Japan

**Published in 1991**

- No. 87: Workstations in Japan
- 86: VAN Services in Japan
- 85: CIM in Japan
- 84: Laptop Computer in Japan - Market & User Strategies -

**Published in 1990**

- No. 83: Distribution Information Systems in Japan
- 82: Computer Security in Japan
- 81: Financial Information Systems in Japan
- 80: EDI in Japan

**Published in 1989**

- No. 79: Neurocomputers and Fuzzy Theory - R & D Trends in Japan -
- 78: Japan's Approach to Privacy Protection
- 77: State of CAL (CAI) in Japan
- 76: Software Industry in Japan - Striving for Increased Productivity -

**Published in 1988**

- No. 75: Personal Computers in Japan - An Unabridged Account -
- 74: Globalization of Telecommunication Services
- 73: The Microcomputer Industry  
- Training Engineers, Creating Applications -
- 72: Informatization - Handling Tomorrow's Problems Today -





## Please send the ORDER FORM directly to:

Promotion Division

JIPDEC

3-5-8 Shibakoen, Minato-ku

Tokyo 105 JAPAN

TEL : +81-3-3432-9384

FAX : +81-3-3432-9389

### ORDER FORM

☐ Please send me JIPDEC Informatization Quarterly as checked below:

☐ Annual Subscription

¥ 13, 000

(including air mail charge)

☐ Back Copies

¥ 3, 500 per copy

(including air mail charge)

No. \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Total: ¥ \_\_\_\_\_

☐ I will make a payment as follows:

☐ Bank funds transfer

Bank Account: Mitsubishi Bank, Toranomon Branch

Account Number: Futsu Yokin 0000739

Account Holder : (Zaidan Hojin)

Japan Information Processing

Development Center (JIPDEC)

☐ Check enclosed

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Name: \_\_\_\_\_

Position: \_\_\_\_\_

Company: \_\_\_\_\_

Address: \_\_\_\_\_

Tel: \_\_\_\_\_

Fax: \_\_\_\_\_





JIPDEC