

# **GUIDELINES ON PERSONAL DATA SECURITY MEASURES, ETC.**

**(Supplement to Self-Regulating Rules on the  
Protection and Use of Personal Information)**

**February 2005  
Japanese Bankers Association**

**The International Bankers Association received permission from the Japanese Bankers Association to prepare this translation for reference purposes. The Japanese Bankers Association neither reviewed nor approved this translation, and the Japanese original remains the official Japanese Bankers Association document.**

**The International Bankers Association prepared this translation with the intention of having the content accurately represent the Japanese original as much as possible, and it contains all information in Japanese original. However, there may be differences in layout and pagination from the Japanese original.**

## **INTERNATIONAL BANKERS ASSOCIATION**

Ark Mori Building 14F  
1-12-32 Akasaka  
Minato-ku, Tokyo 107-6014  
Japan

Telephone: (03) 5545-7511  
Facsimile: (03) 5545-0502  
E-mail: [info@ibajapan.org](mailto:info@ibajapan.org)

*Japanese Page 1-Japanese Page 2*

CONTENTS

I. PURPOSE, etc. ....	1
(1) Purpose .....	1
(2) Compliance with Guidelines .....	1
(3) Definitions .....	1
II. SECURITY MEASURES .....	2
1. Providing a Basic Policy and Regulations on Handling Personal Data Security, etc.2	
(1) Providing a Basic Policy on Personal Data Security.....	2
(2) Providing regulations on handling of personal data security.....	3
(3) Providing regulations on inspections and/or audits of handling of personal data.	3
(4) Providing regulations on outsourcing .....	4
2. Organizational Security Measures .....	4
(1) Organizational security measures.....	4
(2) Establishing positions of the Chief Personal Data Controller, etc. ....	4
(3) Cross-sectional organizational systems.....	5
(4) Providing security measures in Rules of Employment, etc. <b>Error! Bookmark not defined.</b>	
(5) Applying security measures according to Regulations on Handling Personal Data Security..... <b>Error! Bookmark not defined.</b>	
(6) Providing means of checking conditions of personal data handling .....	<b>Error! Bookmark not defined.</b>
(7) Providing and implementing systems for inspecting and/or auditing handling of personal data .....	<b>Error! Bookmark not defined.</b>
(8) Providing systems for dealing with cases of leaks, etc. <b>Error! Bookmark not defined.</b>	
3. People Security Measures .....	<b>Error! Bookmark not defined.</b>
(1) People security measures.....	<b>Error! Bookmark not defined.</b>
(2) Concluding non-disclosure agreement, etc. on personal data with employees .....	<b>Error! Bookmark not defined.</b>
(3) Defining roles and responsibilities, etc., of employees <b>Error! Bookmark not defined.</b>	
(4) Publicizing security measures among employees, educating and training them in security measures .....	<b>Error! Bookmark not defined.</b>
(5) Checking compliance of employees with personal data management procedures .....	<b>Error! Bookmark not defined.</b>
4. Technical Security Measures .....	<b>Error! Bookmark not defined.</b>
(1) Technical security measures.....	<b>Error! Bookmark not defined.</b>
(2) Identifying and/or authenticating users of personal data <b>Error! Bookmark not defined.</b>	
(3) Setting management classifications and/or controlling access to personal data .....	<b>Error! Bookmark not defined.</b>
(4) Manage authorities to access personal data.....	<b>Error! Bookmark not defined.</b>

- (5) Providing measures to prevent personal data leaks and damage, etc. .... **Error! Bookmark not defined.**
- (6) Recording and/or analyzing accesses to personal data **Error! Bookmark not defined.**
- (7) Recording and/or analyzing operating status of information system handling personal data ..... **Error! Bookmark not defined.**
- (8) Monitoring and/or auditing information system handling personal data .... **Error! Bookmark not defined.**
- 5. Supervision of Outsourcees ..... **Error! Bookmark not defined.**
  - (1) Criteria for selecting outsourcees in personal data protection **Error! Bookmark not defined.**
  - (2) Security content that should be included in outsourcing agreement ..... **Error! Bookmark not defined.**
  - (3) Checking and supervising outsourcees for compliance with security measures ..... **Error! Bookmark not defined.**
- 6. Regulations on Handling Security in Each Management Stage **Error! Bookmark not defined.**
  - (1) Regulations on handling security in stages of obtaining and entering personal information..... **Error! Bookmark not defined.**
  - (2) Regulations on handling security in stages of using and processing personal information..... **Error! Bookmark not defined.**
  - (3) Regulations on handling security in storage and retention stages..... **Error! Bookmark not defined.**
  - (4) Regulations on handling security in transfer and transmission stages ..... **Error! Bookmark not defined.**
  - (5) Regulations on handling security in erasure and discarding stages ..... **Error! Bookmark not defined.**
  - (6) Regulations on handling security in stage of dealing with cases of leaks, etc. .... **Error! Bookmark not defined.**
- III. HANDLING OF SENSITIVE INFORMATION ..... **Error! Bookmark not defined.**
  - 1. Regulations on Handling Security in Each Management Stage **Error! Bookmark not defined.**
    - (1) Regulations on handling security in each management stage **Error! Bookmark not defined.**
    - (2) Regulations on handling security in stages of obtaining and entering personal information..... **Error! Bookmark not defined.**
    - (3) Regulations on handling security in stages of using and processing personal information..... **Error! Bookmark not defined.**
    - (4) Regulations on handling security in storage and retention stages..... **Error! Bookmark not defined.**
    - (5) Regulations on handling security in transfer and transmission stages ..... **Error! Bookmark not defined.**
    - (6) Regulations on handling security in erasure and discarding stages ..... **Error! Bookmark not defined.**
  - 2. Implementing Audits ..... **Error! Bookmark not defined.**

*Japanese Page 3*

## **I. PURPOSE, ETC.**

### **(1) Purpose**

The purpose of these Guidelines is to set down matters on security measures for the personal data handled by banks in accordance with IV, “Security Measures” in Self-Regulating Rules on the Protection and Use of Personal Information (hereafter called “Self-Regulating Rules”), and to set down matters on security measures, etc., for “sensitive information” as set down in II, 5., “Sensitive Information” in the Self-Regulating Rules.

### **(2) Compliance with Guidelines**

In these Guidelines, items indicated as FSA Guidelines 0-0 are measures required by the Practical Guidelines on Security Measures, etc., in Guidelines on Personal Data Protection in the Financial Industry (hereafter called the “FSA Guidelines”).

The items specified by these Guidelines other than these are examples of the specific steps and line of thinking that banks need to take to comply with the FSA Guidelines and to devise necessary and appropriate measures. They are not commentaries on the FSA Guidelines.

Among these, items listed as **Mandatory Items** or items specified as “must do” items (including methods deemed to have equivalent or greater effect) are items that banks must comply with, in the same way as they comply with the main text of the Self-Regulating Rules.

Furthermore, items listed as **Example Items** or as items specified as “examples of ... are as follows” (for example, XYZ, etc.) are specific examples of items that banks must comply with, depending on the practical realities.

### **(3) Definitions**

The definitions of terms used in these Guidelines are based on the provisions in I.2, “Definitions” in the Self-Regulating Rules and also on the following:

A. “Regulations, etc.”

“Regulations, etc.” refers to a bank’s rules documented in internal regulations, work procedures, and manuals, etc.

B. “Recording media,” “paper media,” “recording media, etc.”

- a. “Recording media” refers to the magnetic disks, floppy disks, optical disks, magnetic tape, and DAT, etc., of computers (including server PCs, etc.) used to record and retain data.
- b. “Paper media” refers to paper in forms, etc., used to record information.
- c. “Recording media, etc.” refers to recording media and/or paper media.

*Japanese Page 4*

C “Store,” “retain”

- a. “Store” refers to placing recording media, etc., with a high frequency of use in a room so that it can be used as needed.
- b. “Retain” refers to placing recording media, etc., whose frequency of use has declined in a place other than a work space room such as a storeroom until the required cutoff point is satisfied.

D. “Leaks, etc.,” “leaks and/or damage, etc.,” “cases of leaks, etc.”

“Leaks, etc.” and “leaks and/or damage, etc.” refer to “leaks (flow outside),” “loss through deterioration” (the content is lost), and “damage (the content is changed unintentionally, or the content is retained but is in an unusable state).” “Cases of leaks, etc.” refers to cases of “leaks,” “loss through deterioration,” or “damage.”

*Japanese Page 5*

## II. SECURITY MEASURES

### ***1. Providing a Basic Policy and Regulations on Handling Personal Data Security, etc.***

#### **(1) Providing a Basic Policy on Personal Data Security**

Banks must draw up a Basic Policy on Personal Data Security setting down the items below, and make it public. As well, they must review the Basic Policy as required. (FSA

Guidelines 1-1):

- A. Name of the business handling personal data
- B. Information desk for questions and complaints on security measures
- C. Declaration on security of personal data
- D. Declaration of ongoing improvement of the Basic Policy
- E. Declaration of compliance with relevant laws and ordinances, etc.

## **(2) Providing regulations on handling of personal data security**

Banks must provide regulations on the handling of personal data security at each stage in the management of personal data and set down the items specified in 6. in each management stage. They must also review the regulations as required.

In small-scale businesses where the same person handles all management stages, instead of setting down regulations for handling personal data security in each management stage, the business is allowed to set down the items listed below in regulations on handling personal data security throughout all management stages (FSA Guidelines 1-2):

- A. Role and responsibilities of handlers
- B. Restrictions on handlers
- C. Procedures considered necessary for personal data security in each management stage

## **(3) Providing regulations on inspections and/or audits of handling of personal data**

- (i) Banks must provide regulations on inspections and/or audits of the handling of personal data, set down the following items, and review the regulations as required.

In banks where there is only one section handling personal data, audits can be replaced with inspections (FSA Guidelines 1-3):

- A. Purpose of the inspection and/or audit
- B. Section implementing the inspection and/or audit
- C. Roles and responsibilities of the Chief Inspector and/or Inspection Coordinator
- D. Roles and responsibilities of the Chief Audit Officer and/or Audit Coordinator
- E. Procedures relating to inspections and/or audits

*Japanese Page 6*

- (ii) Banks must keep an audit trail to show that work procedures were performed appropriately in accordance with the regulations, etc., set down.

#### **(4) Providing regulations on outsourcing**

Banks must provide regulations on the handling of outsourcing, set down the following items, and regularly review the regulations (FSA Guidelines 1-4):

- A. Criteria for selecting outsourcees
- B. Security-related content that should be included in the outsourcing agreement

## ***2. Organizational Security Measures***

### **(1) Organizational security measures**

Banks must take the following measures as the “organizational security measures” for providing systems to implement personal data security measures (FSA Guidelines 1):

- A. Establish the positions of the Chief Personal Data Controller, etc.
- B. Provide security measures in the Rules of Employment, etc.
- C. Apply security measures in accordance with the Regulations on Handling Personal Data Security.
- D. Provide a means for checking the conditions under which personal data is handled.
- E. Provide and implement systems for inspecting and/or auditing the handling of personal data.
- F. Provide systems for dealing with cases of leaks, etc.

### **(2) Establishing positions of the Chief Personal Data Controller, etc.**

(i) Banks must establish the positions of the following executives to “establish positions of the Chief Personal Data Controller, etc.” as prescribed in (1) A. (FSA Guidelines 2-1):

- A. Chief Personal Data Controller who is the person with overall responsibility for the performance of operations to do with personal data security
- B. Personal Data Manager in each section handling personal data

Note that in businesses where there is only one section handling personal data, the Chief Personal Data Controller is allowed to also serve as the Personal Data Manager. If the organization is a company limited by shares, the Chief Personal Data Controller must be a person who is a director or who has responsibility for executing the operations of an operating officer, etc. (FSA Guidelines 2-1)

(ii) Banks must give control over the following operations to the Chief Personal Data Controller as prescribed in (1) A. (FSA Guidelines 2-1-1):

- A. To approve and/or publicize the regulations on personal data security and selection criteria for outsourcees

*Japanese Page 7*

- B. To appoint a Personal Data Manager and a manager of “information on customer ID checking” as set down in 4. (2) (i).
- C. To collect reports from and/or provide advice and guidance to the Personal Data Manager
- D. To plan the education and training of the Personal Data Manager on security
- E. To do other matters concerning personal data security in Businesses Handling Personal Information as a whole.

(iii) Banks must give control over the following operations to the Personal Data Manager prescribed in (i) B. (FSA Guidelines 2-1-2):

- A. To designate the handler of personal data and/or to manage changes, etc.
- B. To approve applications to use personal data and/or to manage records, etc.
- C. To designate and/or change the installation location of storage media on which personal data is handled
- D. To set and/or manage changes in classifications for managing personal data and/or authorities for managing personal data
- E. To comprehend the conditions under which personal data is handled
- F. To supervise the conditions, etc., under which personal data is handled at the outsourcee
- G. To implement education and training in personal data security
- H. To report to the Chief Personal Data Controller
- I. To do other matters concerning personal data security in the section with jurisdiction

### **(3) Cross-sectional organizational systems**

To assist the Chief Personal Data Controller, banks can provide organizational systems to perform cross-sectional hearings, communications, coordination, and instructions, etc., of the various departments and branches concerned to achieve thoroughness in personal data security.

This can be done by setting up cross-sectional committees, etc., or by any method that clearly specifies the department that handles personal data security in a unified way. “An organization to perform cross-sectional hearings, communications, coordination, and instructions, etc., of the various related departments and branches” can perform the operations listed below: