

**Guidelines for Personal Information Protection  
Management System Implementation  
based on  
JIS Q 15001: 2006**

**Points Related to Each Requirement**

## Contents

1. Scope .....	20
2. Terms and definitions .....	21
3. Requirements of personal information protection management systems .....	22
3.1 General requirements .....	22
3.2 Personal information protection policy .....	23
3.3 Plan .....	24
3.3.1 Specification of personal information .....	24
3.3.2 Laws, guidelines and other codes stipulated by the state .....	25
3.3.3 Recognition, analysis and measures of risk, etc.....	26
3.3.4 Resources, roles, responsibility and authority .....	27
3.3.5 Internal regulations .....	28
3.3.6 Planning documents .....	29
3.3.7 Preparation for state of emergency .....	30
3.4 Implementation and operation .....	31
3.4.1 Operation procedures .....	31
3.4.2 Principles on acquisition, use and provision .....	32
3.4.2.1 Specification of purpose of use .....	32
3.4.2.2 Appropriate acquisition .....	33
3.4.2.3 Restriction of acquisition, use and provision of specific subtle personal information .....	34
3.4.2.4 Measures for acquiring with document directly from the person .....	35
3.4.2.5 Measures for acquiring personal information by methods other than 3.4.2.4 .....	36
3.4.2.6 Measures concerning use .....	38
3.4.2.7 Measures when accessing to the person .....	39
3.4.2.8 Measures concerning provision .....	41
3.4.3 Appropriate control .....	43
3.4.3.1 Securement of accuracy .....	43
3.4.3.2 Security control measures .....	44
3.4.3.3 Supervision of employees .....	47

3.4.3.4 Supervision of trustees .....	49
3.4.4 Rights of the person concerning personal information .....	51
3.4.4.1 Rights concerning personal information .....	51
3.4.4.2 Procedures to meet requests for disclosure and others .....	52
3.4.4.3 Making the matters concerning personal information subject to disclosure widely known, etc. ...	53
3.4.4.4 Notification of purpose of use of personal information subject to disclosure .....	54
3.4.4.5 Disclosure of personal information subject to disclosure .....	55
3.4.4.6 Correction, addition or deletion of personal information subject to disclosure .....	56
3.4.4.7 Veto of use or provision of personal information subject to disclosure .....	57
3.4.5 Education .....	58
3.5 Personal information protection management system documents .....	59
3.5.1 Range of documents .....	59
3.5.2 Document control .....	60
3.5.3 Record control .....	61
3.6 Response to complaints and consultations .....	62
3.7 Inspection .....	63
3.7.1 Confirmation of operations .....	63
3.7.2 Audits .....	64
3.8 Corrective actions and preventive actions .....	65
3.9 Review by the representative of the business entity .....	66

**Note 2:** The following abbreviations are used in this documentation.

- a. The Personal Information Protection Law = The Act on the Protection of Personal Information (Act No. 57 of 2003)
- b. The Guidelines for the Fields of Economy, Trade and Industry = The Guidelines on Laws for the Protection of Personal Information in the Fields of Economy, Trade and Industry (October 2004, Ministry of Economy, Trade and Industry)
- c. The 1999 edition = JISQ15001:1999
- d. The 2006 edition = JISQ15001:2006
- e. The manager = the personal information protection manager
- f. The auditor = the personal information protection auditor

**Note 3:** Permission of the copyright holder cannot be obtained for revisions or publications on the specifications text website. Therefore, Requirements in English are translated by JIPDEC and should be served only as a reference.

The permission of the copyright holder cannot be obtained for revisions or publications on the specification text website. The requirements in English are translated by JIPDEC and should be served only as a reference.

## 1. Scope

This Japanese Industrial Standard stipulates the requirements for personal information protection management systems which is able to business entities of any kind and size for using personal information for their business.

The business entities might use the Standard in the process of implementing the followings;

- a) To establish, implement, maintain, and improve their own personal information protection management system,
- b) To confirm voluntarily that their own personal information protection management system adapts to the Standard and announcing the conformation voluntarily,
- c) To request external organizations or the person to confirm which the personal information protection management system adapts to the Standard, and
- d) To request external organizations to certificate/register the personal information protection management system,

### (1) Purpose of this requirement

The purpose is to define the scope of this Japanese Industrial Standard. The important matter herein is that personal information "used for their businesses" is what is targeted. As stipulated in the commentary pertaining to the Standard, the personal information used for their businesses are not limited to targeting commercial business. Because the personal information of employees is the personal information used for their businesses, in practice all business entities are targeted by these specifications. Regarding business entities which handle information without distinguishing it as personal information, the personal information included within this can be considered as not using personal information for their businesses. However, considering the expectations of the general consumers and partners/clients of these business entities, regardless of whether the business entities themselves identify such information as being personal information, it is of course ideal even pertaining to these types of business entities to define the said information as being equivalent to personal information which use personal information for their businesses and implement the appropriate risk awareness and analysis as well as risk countermeasures.

### (2) Correspondence with the Personal Information Protection Law

- ① Item 3 of Article 2 of the Personal Information Protection Law (Definition of "business entity handling personal information")
- ② Article 2 of the Government Ordinance (Those who are relatively unlikely to damage their rights and benefits of individuals in consideration of the amount and usage of personal information being handled) \*  
In the standard, however, Article 2 of the Government Ordinance is to be waived.

### (3) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that scope in terms of personnel include all employees.	① Scope in terms of personnel shall include all employees.
2	It shall be stipulated that personal information used for their business be targeted.	② Personal information used for their business shall be targeted.

## 2. Terms and definitions

The following definitions are applied for the purpose of the Standard.

### 2.1 personal information

information about an individual that is able to identify the specific individual by name, date of birth, or other description having the information (including the information as will verify other information easily, and thereby allow the identification of the specific individual)

### 2.2 person

a specific individual identified by the personal information

### 2.3 business entity

any corporation, other group or individual engaged in any business form

### 2.4 personal information protection managers

a person appointed by the representative in the business entity who has the responsibility and authority for implementing and operating the personal information protection management system

### 2.5 personal information protection auditor

a person appointed by the representative in the business entity who is in a fair and objective position and has the responsibility and authority for implementing and reporting audits

### 2.6 consent of the person

An assent of the person after the information about the handling of personal information is given, to consent to the handling of his or her personal information. If the person is a child or a person who has a disability in reasonable thinking, the consent of the legal representative, etc. is also required.

### 2.7

#### personal information protection management system

a management system which includes policies, organizations, plans, implementation, audits, and reviews for protecting the rights and interests of individual concerning personal information that a business entity uses for its business, considering the usefulness of personal information

### 2.8 nonconformance

not fulfilling the requirements for the Standard

### (1) Purpose of this requirement

The purpose is to provide regulation pertaining to the terms and definitions used within the Japanese Industrial Standard. Needless to say, the fact that terminology of the 2006 revision is different from that of the 1999 edition does not necessitate the task of altering terminology to match the new terminology in the 2006 edition. The important matter is that the substance conforms to the requirements of the Standard. Thus, it is perfectly acceptable for the terminology used within business entity to be different from the terminology used in the specifications.

It is necessary to note that the definition of personal information is different from that of the Personal Information Protection Law. In the Personal Information Protection Law, personal information is, as a general rule, information pertaining to a living person, and can include information pertaining to deceased persons as exceptions. Contrastingly, in this Standard, personal information is, as a general rule, information pertaining to both deceased and living persons, but does not include information pertaining to historical persons.

### (2) Correspondence with the Personal Information Protection Law

① Items 1-6 of Article 2 of the Personal Information Protection Law (Definition)

②Article 1 of the Government Ordinance (Systematically organized material or databases through which specific personal information can be readily searched.)

③Article 2 of the Government Ordinance (Those who are relatively unlikely to damage their rights and benefits of individuals in consideration of the amount and usage of personal information being handled)

\* In this standard, however, Article 2 of the Government Ordinance is to be waived.

**(3) Points to consider**

	Document Preparation	Operations
1	“Personal information” shall be defined in accordance with 2.1 of the Standard.	
2	“Person” shall be defined in accordance with 2.2 of the Standard.	
3	“Business entities” shall be defined in accordance with 2.3 of the Standard.	
4	“Personal information protection manager” shall be defined in accordance with 2.4 of the Standard.	
5	“Personal information protection auditor” shall be defined in accordance with 2.5 of the Standard.	
6	“Consent of the person” shall be defined in accordance with 2.6 of the Standard.	
7	“Personal information protection management systems” shall be defined in accordance with 2.7 of the Standard.	
8	“Nonconformance” shall be defined in accordance with 2.8 of the Specifications.	
9	Any term not included in the Specifications shall not be defined in a way that is inconsistent with the contents of the Standard.	

### **3. Requirement of personal information protection management systems**

#### **3.1 General requirements**

**The business entity shall establish, implement, maintain, and improve a personal information protection management system. The requirements are stipulated in clause 3.**

#### **(1) Points to consider**

None

### 3.2 Personal information protection policy

The representative of the business entity shall not only establish a personal information protection policy including the following items, but also implement and maintain the policy, after defining the concept of personal information protection;

- a) The appropriate acquisition, use, and disclosure of personal information considering the content and the business size (including not handling personal information over the scope necessary to achieve the specific purpose of use (hereafter referred to as “use other than for intended purposes”) and taking measures for it,
- b) The observation by laws, guidelines and other codes stipulated by the state regarding the handling of personal information,
- c) To prevent leakage, loss or damage of personal information and correction of it,
- d) Response to complaints and consultations
- e) The continuous improvement of a personal information protection management system, and
- f) The name of the representative.

The representative of the business entity shall embody this policy in document form (including the record made by an electronic method, a magnetic method or any other method not being able to recognize to human senses, hereafter this applies in the Standard), take measures that it is available to general people as well as inform the employees of it.

#### (1) Purpose of this requirement

This requirement calls for documenting of implementation by business entities related to the protection of personal information and the internal and external announcement of such. The reason Personal Information Protection activities are conducted ("Concept of Personal Information Protection"), the type of actions that are performed for the protection of personal information (a) to (e), and (f) must be filled out. ➡ Step 1 and Step 4 in No. 4 of Section 1

#### (2) Correspondence with the Personal Information Protection Law, etc.

- ① “Basic Policy on the Protection of Personal Information” (Cabinet decision of April 2, 2004)  
6(1) 1. Clarification of measures carried out by the business entity affecting external parties

#### (3) Points to consider

	Document Preparation	Operations
1	Concept of personal information protection shall be clarified.	
2	Description regarding (a) shall be provided.	
3	Description regarding (b) shall be provided.	
4	Description regarding (c) shall be provided.	
5	Description regarding (d) shall be provided.	
6	Description regarding (e) shall be provided.	
7	Description of (f) shall be provided.	

8	The date of enactment and the date of the latest revision shall be indicated.	① The date of enactment and the date of the latest revision shall be indicated in the personal information protection policy that is published (on the web etc.) or distributed.
9	The document shall stipulate that measures be taken so that information on the personal information protection policy is available to the employees and the general public.	① Measures shall be taken so that information on the personal information protection policy is available to the employees and the general public. ② When published on the website, there shall be the link on the top page. ③ Contact information for inquiries about personal information protection shall be indicated in the published personal information protection policy. ④ The published personal information protection policy shall be identical to that described in the stipulating document.

### 3.3 Plan

#### 3.3.1 Specification of personal information

The business entity shall establish and maintain the procedure to specify all the personal information that the business entity uses for its business.

##### (1) Purpose of this requirement

This requirement calls for the establishment and maintenance of the procedures that enable complete recognition of all instances of personal information used for their business. ☞ Step 5 in No. 4 of Section 1

##### (2) Correspondence with the Personal Information Protection Law

- a. Item 3 of Article 2 of the Personal Information Protection Law (Definition of “business operator handling personal information”)
  - b. Article 2 of the Government Ordinance (Those who are relatively unlikely to damage their rights and interests of individuals in consideration of the amount and usage of personal information being handled)
- \*In this Standard, however, Article 2 of the Government Ordinance is to be waived.

##### (3) Points to consider

	Document Preparation	Operations
1	Procedures for identifying and approving every piece of personal information shall be clearly established.	a. Personal information shall be identified in accordance with predetermined procedures. b. Records of identifying personal information shall be maintained. c. Personal information shall be identified without omission.
2	Procedures for updating and periodical review of records of personal information specification shall be provided.	a. Updating and periodical review of records of personal information specification shall be carried out in accordance with predetermined procedures.

### 3.3.2 Laws, guidelines and other codes stipulated by the state

**The business entity shall establish and maintain the procedures to specify and refer to laws, guidelines and other codes stipulated by the state regarding the handling of personal information.**

#### (1) Purpose of this requirement

When specific stipulations regarding the handling of personal information exist in any guidelines and regulations established by the state, and in any laws and ordinances related to the business activities of business entities, such stipulations will be given precedence. Thus, it is necessary to be aware of the status of enactment, reform, and abolishment of guidelines and regulations stipulated by the state, and any other laws and ordinances related to the business activities of business entities, and to establish and enforce processes for constantly maintaining and referring on the latest editions and versions of such stipulations. ➡ Step 6 in No. 4 of Section 1

#### (2) Points to consider

	Document Preparation	Operations
1	Procedures for specifying, referring, and maintaining laws, guidelines and other codes shall be stipulated by the state related to the handling of personal information.	<p>a. Procedures for specifying and referring laws, guidelines and other codes shall be stipulated by the state.</p> <p>b. Procedures for specifying and referring laws, guidelines and other codes shall be stipulated by the state shall be updated as necessary.</p> <p>c. Procedures for specifying and referring laws, guidelines and other codes shall be stipulated by the state shall be appropriate.</p> <p>d. Procedures for specifying and referring laws, guidelines and other codes shall be stipulated by the state shall be available for reference as necessary.</p>

### 3.3.3 Recognition, analysis and measures of risk, etc

The business entity shall establish and maintain the procedures to take the necessary measures so as not to use other than for intended purposes concerning personal information specified in accordance with 3.3.1.

The business entity shall establish and maintain the procedure to recognize, analyze risk in each aspect of the handling of the personal information specified in accordance with 3.3.1. (the possibility of leakage, loss or damage of personal information, violation of relevant laws, guidelines and other codes stipulated by the state, anticipated economical disadvantages and loss of social confidence, influence on the person, etc.) and take the necessary measures.

#### (1) Purpose of this requirement

This requirement calls for the control of all imaginable risks for items targeted for protection pursuant to 3.3.1. In order to clarify thoroughly all risks, it is necessary to examine each phase individually, from entrance into one's company to exit (the "personal information life cycle"). Though this is laborious, through conduction of the actual process itself, the status of the handling of personal information within one's company is clarified and business management should become easier. ☞ Step 7 in No. 4 of Section 1

#### (2) Points to consider

	Document Preparation	Operations
1	Procedures for specifying and referring to laws, guidelines and other codes shall be established and maintained in order not to use other than for intended purposes.	a. Procedures for preventing the use of personal information for using other than for intended purposes shall be implemented.
2	Procedures shall be clearly established to identify risks to particular personal information according to the life cycle thereof, analyzing risk, taking appropriate measures to deal with these risks, and clearly identifying any remaining risks.	a. Procedures for recognizing, analyzing risk and taking the necessary measures shall be stipulated by state. b. Procedures for recognizing, analyzing risk, taking the necessary measures and identifying remaining risks shall be indispensable for each piece of personal information according to the lifecycle thereof. (Grouping to be allowed for pieces having the same life cycle.) c. Measures that are to be taken shall be reflected in the regulations.
3	Procedures shall be clearly established for periodical review and occasional review according to needs.	a. Risks shall be reviewed in accordance with predetermined procedures.

### 3.3.4 Resources, roles, responsibility and authority

The representative of the business entity shall prepare for indispensable resources to establish, implement, maintain, and improve the personal information protection management system.

The representative of the business entity shall stipulate a role, responsibility and authority, embody them in document form and inform the employees of it to implement the personal information protection management system effectively.

The representative of the business entity shall appoint a personal information protection manager who is able to understand and implement the content of the Standard in the business entity, give the responsibility and authority to the manager regarding the implementation and operation of the personal information protection management system independent of any other responsibilities and make him or her implement its operations.

The personal information protection manager shall report an operation status of the personal information protection management system to the representative of the entity as the base of review and improvement of the personal information protection management system.

#### (1) Purpose of this requirement

This requirement calls for the upgrading of the system in order to enforce personal information protection management systems. ☞ Step 8 in No. 4 of Section 1

The implementation of personal information protection management systems is a part of the conducting of affairs for business entities, and is an ongoing activity. Thus, when auditors make up a portion of the system, because it continuously falls under the supervision of a representative, this is considered a violation of Article 335 of the Companies Law. (The substance of this stipulation also applies to audit committee members in corporations which utilize committees and accounting officials for close companies. These posts are regulated by the same type of restrictions as in the case of auditors in Article 400, Clause 4 and Article 333, Clause 3, No. 1 of the Companies Law, respectively. Furthermore, because accounting officials are included as officers pursuant to Article 324 of the Companies Law, they are counted as employees.) However, this does not preclude auditors completely from contributing to the implementation of this management system. Considering that this management system includes in its content adherence to the Private Information Protection Law, just as there is an obligation of auditors for attendance and declaration of opinion at Board of Directors meetings, if meetings pertaining to the protection of personal information are held, such as inner-company committee meetings, audit report meetings, and revision meetings conducted by representatives, attendance and opinion declaration from auditors is actually preferable from the viewpoint of operational auditing (legality audits).

#### (2) Points to consider

	Document Preparation	Operations
1	The functions and authority of each staff member shall be clearly determined and documented.	<p>a. Role, responsibility and authority of each staff member shall be clearly determined.</p> <p>b. Every member of staff shall be informed of the role and authority of all other members.</p> <p>c. Auditors, inspection commissioners, or accounting advisers, as defined by the Companies Law, shall not take part in the system.</p>

2	It shall be stipulated that the personal information protection manager shall be selected from within the organization by the representative.	a. The personal information protection manager shall be selected from within the organization by the representative.
3	It shall be stipulated that the personal information protection manager shall report the operating status of the personal information protection management systems to the representative of the business entity in order to provide the basis to review and improve the personal information protection management systems.	b. The personal information protection manager shall not be the same person as the personal information protection manager. a. The personal information protection manager shall report the operating status of the personal information protection management systems to the representative of the business entity in order to provide the basis to review and improve the personal information protection management systems.

### 3.3.5 Internal regulations

The business entity shall embody internal regulations including the following items in document form and maintain them;

- a) Regulations regarding the procedures to specify personal information,
- b) Regulations regarding the specification, reference and maintenance of laws, guidelines and other codes stipulated by the state,
- c) Regulations regarding the procedures to recognize, analyze risks related to personal information and take measures for them,
- d) Regulations regarding the authority and responsibility to protect personal information in each section and level of the business entity,
- e) Regulations regarding the preparation for states of emergency and response to them (in case of leakage, loss and damage of personal information),
- f) Regulations regarding the acquisition, use and provision of the personal information,
- g) Regulations regarding the appropriate management of personal information,
- h) Regulations regarding the response to a request for disclosure and others from the person,
- i) Regulations regarding the education,
- j) Regulations regarding the control of personal information protection management system documents,
- k) Regulations regarding the response to complaints and consultations,
- l) Regulations regarding the inspection,
- m) Regulations regarding the corrective action and preventative action,
- n) Regulations regarding the review implemented by the representative, and
- o) Regulations regarding the penal provisions about the violation of internal rules.

The business entity shall revise internal regulations so that the personal information protection management system can be applied certainly according to the content of the business,

#### (1) Purpose of this requirement

This requirement calls for the documenting of established procedures in the form of internal regulations. ☞ Step 9 in No. 4 of Section 1

#### (2) Points to consider

	Document Preparation	Operations
1	Specific regulations corresponding to (a) to (o) shall be provided in the form of procedure manuals.	<p>①Such regulations shall be established by following prescribed procedures such as board resolutions.</p> <p>②Regulations including (a) to (o) shall be available to the employees so that they can refer to them.</p>

### 3.3.6 Planning document

**The business entity shall make, document, and maintain a plan related to the education, audit, etc. required for ensuring the implementation of the personal information protection management system.**

#### (1) Purpose of this Requirement

This requirement calls for the formulation of planning document necessary for implementation of the personal information protection management systems. Regarding an creation of planning document, the approval of a representative of the business entities is required. The planning document must be described precisely as far as is enforceable. Annual plans and individual plans may be created as necessary.

Furthermore, PrivacyMark screening calls for instruction and auditing conducted at least once per year. (Refer to Article 10 of the "Guidelines for the establishment and operation of the PrivacyMark System")

#### (2) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that an audit plan shall be created upon the approval of a representative of the business entities.	a. An instruction plan shall be created upon the approval of a representative of the business entities. b. The content of a created instruction plan shall be appropriate.
2	It shall be stipulated that an inspection plan shall be created with the approval of a representative of the business entities.	a. An inspection plan shall be created with the approval of a representative of the business entities. b. The content of a created inspection plan shall be appropriate.

### 3.3.7 Preparation for state of emergency

The business entity shall establish and maintain the procedures to specify the states of emergency and the procedures for how to respond to them.

The business entity shall establish and maintain the procedure to minimize the influence on consideration of the possibility for economical disadvantages and loss of social confidence, effect on the person, etc. anticipated in case of leakage, loss or damage of personal information.

Also in preparation for the case of leakage, loss or damage of personal information takes place, the business entity shall establish and maintain the procedure for response including the following items;

- a) To place the person in such a condition that he/she is informed promptly of the content of the personal information when leakage, loss or damage of personal information occurred, or to place the person in a readily accessible condition for him/her about the content,
- b) To announce the facts publicly, causes and measures as much as possible with no delay in the viewpoint of prevention of secondary damages, avoidance of occurrence of corresponding cases, etc., and
- c) To report promptly the causes and the measures to the relevant organizations.

#### (1) Purpose of this Requirement

This requirement calls for the advance establishment of procedures for minimizing damages in the event that personal information is leaked, lost, or has damaged. Even in the case of states of emergency, it is not always required that all of the measures from (a) through (c) be enforced. It is necessary, of course, to execute measures which are obligatory pursuant to laws, ordinances, guidelines and other regulations stipulated by the state. In cases where such does not apply, however, considering the risks of economical disadvantages and loss of societal credibility, effects on the person, it is necessary to stipulate in advance what measures should be taken in which cases. ☞ Step 9(e) in No. 4 of Section 1

#### (2) Points to consider

	Document Preparation	Operations
1	The Procedure for specifying states of emergency and procedure for how to respond to them shall be stipulated.	a. The emergencies shall be identified and coped with in accordance with predetermined procedures.
2	The procedure for minimizing the effects in consideration of the possibility for economical disadvantages and loss of social credibility, effects on the person, etc. supposed in case of leakage, loss or damage of personal information shall be stipulated.	a. The procedure for minimizing the effects in consideration of the possibility for economical disadvantages and loss of social credibility, effects on the person, etc. supposed in case of leakage, loss or damage of personal information shall be implemented.
3	In case of states of emergency: (a) Placing the person in such a condition that the person is readily informed of the content of the personal information occurred, or placing the person in a promptly accessible condition for the person with regard to the content shall be stipulated.	a. Placing the person in such a condition that the person is readily informed of the content of the personal information occurred, or placing the person in a promptly accessible condition for the person with regard to the content.

4	In case of states of emergency: (b) Publicly informing facts, causes and measures as much as possible with no delay from the perspective of prevention of secondary damages, avoidance of occurrence of similar cases shall be stipulated.	a. Publicly informing facts, causes and measures as much as possible with no delay from the perspective of prevention of secondary damages, avoidance of occurrence of similar cases.
5	In case of states of emergency: (c) Promptly reporting causes and measures to the related organizations shall be stipulated.	a. Promptly reporting causes and measures to the related organizations. b. The point of contact in the event of an emergency shall be made clear for the employees.

### 3.4 Implementation and operation

#### 3.4.1 Operation procedures

**The business entity shall clarify the procedure of operation to assure the implementation of the personal information protection management system.**

#### **(I) Points to consider**

There are no specific examinations corresponding to this requirement. Whether procedures are clarified or not will be examined for each individual requirement.

### 3.4.2 Principles on acquisition, use and provision

#### 3.4.2.1 Specification of purpose of use

**The business entity, when acquiring personal information, shall identify the purpose of use as much as possible within the scope necessary for the achievement of the purpose.**

##### (1) Purpose of this requirement

The acquisition of personal information must, upon identifying the usage purpose as specifically as possible, be limited to the range necessary for achieving the purpose.

##### (2) Correspondence with the Personal Information Protection Law

a. Item 1 of Article 15 of the Personal Information Protection Law (Specification of the Purpose of Utilization)

##### (3) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that, upon the acquisition of personal information, the purpose of utilization thereof be specified to the greatest possible extent, and the scope necessary for the achievement of the purpose not be exceeded.	a. The purpose of utilization shall be specified as concretely as possible.
2	Procedures for specifying the purpose of utilization shall be stipulated.	a. The purpose of utilization shall be specified in accordance with predetermined procedures. b. The employees who handle personal information shall clearly appreciate the purpose of utilization thereof.

### 3.4.2.2 Appropriate acquisition

**The business entity shall acquire personal information legally and fairly.**

#### (1) Purpose of this requirement

The acquisition of personal information must be conducted by legal and equitable methods. Article 17 of the Personal Information Protection Law states, "personal information must not be acquired by deceit or other dishonest methods." The requirement herein has the same meaning, but the reason the wording differs from the law is to clarify the point that acquisition using methods which although not dishonest are not equitable (using a dominant bargaining position, etc.) is not allowed.

#### (2) Correspondence with the Personal Information Protection Law

a. Article 17 of the Personal Information Protection Law (Appropriate acquisition)

#### (3) Points to consider

	Document Preparation	Operations
1	It shall be stipulated as a principle that acquisition of personal information be carried out in a legal and fair way.	a. Acquisition of personal information shall be carried out in a legal and fair way.

### 3.4.2.3 Restriction of acquisition, use and provision of specific subtle personal information

The business entity shall not acquire, use or provide the personal information including the following content except when the person consents to the acquisition explicitly, use or provision of personal information, or any of a) to d) of provisory clauses in 3.4.2.6 can be applied.

- a) Matters regarding ideology, belief, or religion,
- b) Races, ethic groups, lineages, permanent domiciles (excluding information on prefecture to which he/she belongs), physical or mental handicaps, criminal records, or other items that could be factors in special discrimination,
- c) Matters regarding trade union membership, collective bargaining, or other group affiliations or activities,
- d) Matters regarding participation in group actions, the exercise of petition rights, or the exercise of other political rights, and
- d) Matters regarding health and medical treatments, or sex life.

#### (1) Purpose of this requirement

This requirement calls for the special consideration for the handling of particularly sensitive personal information as specified in (a) through (e). Thus, the acquisition, usage and supply of these types of personal information is, as a general rule, prohibited, and only allowed as exceptions.

Furthermore, pertaining to information regarding the health of employees, it is necessary to note that the following requirements are stipulated in 3.4 of "Regarding points of concern in the handling of health information from amongst personal information pertaining to employee management" (Director of the Labour Standards Bureau of the Ministry of Health, Labour and Welfare, October 26, 2004), and referred to as, "pertaining to the matters stipulated below, stipulating them as rules in the workplace, notifying workers of these rules, and making related entities adhere to these relevant rules is desired..."

- Matters related to the purpose of health information usage
- Matters related to the safety control system regarding health information
- Matters related to the persons who handle health information, the authority therein, and the scope of health information to be handled
- Matters related to methods of disclosure, revision, addition, and deletion (including abolishment) of health information
- Matters related to the handling of complaints regarding the handling of health information

#### (2) Points to consider

	Document Preparation	Operations
1	It shall be stipulated as a principle that the business entities not acquire, use, or provide specific delicate pieces of personal information (a) to (e).	a. Specific delicate pieces of personal information (a) to (e) shall not be acquired, used, or provided except in the cases in the proviso in 3.4.2.3 of the Standard.
2	Exceptional acquisition, use, or provision of delicate pieces of personal information shall be limited exclusively to the cases in the proviso stipulated in 3.4.2.3 of the Standard.	a. Acquisition of specific delicate pieces of personal information (a) to (e) shall be limited exclusively to cases to which the proviso applies.
3	Procedures for approving exceptional acquisition, use, and provision of delicate pieces of personal information according to the proviso shall be stipulated.	a. Approval by the manager shall be obtained in accordance with predetermined procedures.

4	In cases of acquiring, use, or providing specific delicate pieces of personal information with the consent of a person, procedures for obtaining consent from the person shall have been concretely stipulated.	a. Acquisition, use or provision of specific delicate pieces of personal information with the consent of a person shall be conducted after obtaining explicit consent from the person in accordance with the procedures that have been concretely stipulated.
---	---	---

### 3.4.2.4 Measures for acquiring with document directly from the person

The business entity, when acquiring the personal information described in the document (including a record made by an electronic method, a magnetic method or any other method not recognizable to human senses, hereafter this is applied in the Standard) directly from the person, shall describe clearly at least the matter shown below or the matter equivalent to or better than that in content in writing beforehand and acquire the consent of the person except when it is urgently required to protect the life, body or property, any of a) to d) of provisory clauses in 3.4.2.5 can be applied and any of a) to d) of provisory clauses in 3.4.2.6 can be applied;

- a) Name o designation of the business entity,
- b) Name or title, section and the contact of personal information protection manager (or the agent),
- c) Purpose of the use,
- d) Matters when personal information is planned to be provided to a third party,
  - Purpose for providing to a third party
  - Items of personal information to be provided
  - Means or methods for the provision
  - Recipient of provision of the information, or type and attribute of organization of recipient of the provision
  - When there is an agreement regarding the handling of personal information, the said effect
- e) When the entrustment of personal information is planned, the said effect,
- f) When 3.4.4.4 to 3.4.4.7 can be applied, the effect of response to the request and the person to contact for the inquiry,
- g) Voluntariness of the person's provision of personal information and when the person did not provide the personal information, consequences that occurs to the person, and
- h) When personal information is acquired by the means which the person cannot recognize easily, the said effect.

#### (1) Purpose of this requirement

The consent of the person about whom the information is gathered is required as a general rule for the acquisition of personal information. As evidenced by the explanation about documents in the specifications text, acquisition in the form of writing includes data entered via websites. The act by the person in question of beginning to fill out a form that has been proffered to that person by no means constitutes the conferring of consent. The fact that the person in question has consented to the matters clearly indicated in the form of writing must be clearly shown. ☞ Refer to the explanation of 3.4.2.5

"Clearly specify" requires that the location in which the matters of consent are written be clearly indicated. For example, if a membership agreement or a contractual condition is designated as the notification document and the location in which the matters of consent are written is not clear due to small print or lengthy content, even if the content fulfills the matters in (a) through (h), this cannot be viewed as being in fulfillment of the direction to "clearly specify". In such a case, it is necessary to emphasize the portion regarding the handling of personal information using a suitable method, and implement measures that allow the person in question to easily recognize this information.

Furthermore, entering information in writing which the individual in question provides orally does not constitute acquisition with document directly from the person.

**(2) Correspondence with the Personal Information Protection Law**

- ①Item 2 of Article 18 of the Personal Information Protection Law (Acquiring with document directly from the person)
- ②Item 1 of Article 18 of the Personal Information Protection Law (Notification or publication of the purpose of utilization at the time of acquisition)
- ③Item 4 of Article 18 of the Personal Information Protection Law (Exceptions to notification or publication of the purpose of utilization)

**(3) Points to consider**

	Document Preparation	Operations
1	Procedures for approving direct acquisition of new types of personal information with document directly from the person shall be stipulated.	a. Approval by the manager shall have been obtained in accordance with predetermined procedures when acquiring new types of personal information with document directly from the person.
2	It shall be stipulated that procedures be established for each acquisition method and that person be informed of items required in (a) to (h) and consent be obtained.	a. In cases where personal information is directly acquired with document directly from the person, he/she shall be notified in writing accordingly and written consent be obtained.
		b. The notification given to the person upon direct acquisition with document from the person shall fulfill the contents of (a) to (h).
3	It shall be stipulated that acquisition with document directly from the person without the consent of the person be limited exclusively to the cases in the proviso.	a. Direct acquisition with document from the person without consent of the person shall be limited exclusively to the cases in the proviso.
4	Procedures for approving the application of the proviso shall be provided.	a. Approval by the manager shall have been obtained in accordance with predetermined procedures when applying the proviso.

### 3.4.2.5 Measures for acquiring personal information by methods other than 3.4.2.4

The business entity shall, when personal information is acquired by methods other than 3.4.2.4 except when the purpose of use is publicly announced beforehand, inform the person of the purpose of use promptly, or publicly announce it, except when any of the following can be applied;

- a) Cases in which informing the person of the purpose of use or publicly announcing it may harm the life, body, property or other rights and interests of the person or a third party,
- b) Cases in which informing the person of the purpose of use or publicly announcing it may harm the rights or legitimate interests of the business entity,
- c) Cases in which it is necessary to cooperate with a state institution or a local public body when executing the operations inscribed by laws and in which informing the person of the purpose of use or publicly announcing it may hinder the execution of the operations, and
- d) Cases in which it is regarded that the purpose of use is clear in view of the circumstances of the acquisition.

#### (1) Purpose of this requirement

Though the obtaining of consent from the person about whom the information is gathered is a general requirement for the acquisition of personal information, requiring that the person in question provide consent in every case is not realistic. For example, requiring the consent of a person with regard to information acquired by a commissioned business entity is impossible. Likewise, in the case of direct acquisition, requiring the clear specification all the matters for (a) through (h) in 3.4.2.4 and the obtaining of consent therein is, considering the case of oral acquisition or acquisition via surveillance video, impossible. Thus, 3.4.2.4 and 3.4.2.5 are to be regulated pursuant to the realities of acquisition.

It is necessary to establish applicable criteria for allowing provisos (a) through (d), referring to the commentary attached to the specifications body and the Guidelines for the Fields of Economy, Trade and Industry.

What should be noted in regard to this requirement is that, because one does not merely want to notify or announce to the person in question, operation which determines everything as falling under (d) is unacceptable. The stipulations in (a) through (d) are applicable as provisos in the case of acquisition directly in the form of writing. However, cases of reasoning such as, "because the person is to write information on a form labeled 'questionnaire,' considering the acquisition situation, the usage purpose is clear, it falls under (d), and thus clear specification and consent is not required," or, "because the person will include a resume in response to a job offer notice, it is clear that the information will be used for the purpose of hiring, it falls under (d), and thus clear specification and consent is not required," reflect utter misunderstandings of the applicable criteria. If such interpretation were allowed, the requirements of 3.4.2.4 would, for the most part, become dead letter. There are many questionable cases such as receiving direct mail advertising after answering a questionnaire, and the acquisition situation and usage purpose do not always match. Proviso (d) must be recognized as merely an extremely rare exception, and the applicable criteria for the application of (d) must be strictly defined.

In the case of a commissioned entity, cases of misinterpretation such as, "if the original acquirer (for example, the assignor) has already clearly specified to or notified the person about whom the information has been gathered, then because the usage purpose is already clear to the person in question, the case of commissioning falls under (d)," are frequent, so caution is necessary. Even in the case of accepting commissions, there is an obligation to notify or officially announce the purpose of use to the person in question.

According to the Guidelines for the Fields of Economy, Trade and Industry, writing the following, for example, constitutes the commissioned entity announcing the purpose of use.

"We handle commissioned personal information in order to conduct, as information processing business such as payroll accounting services, address printing services, and bill printing and dispatching services."

Because the assignor of the commission source is a business secret, notification or official

announcement of source is not required.

Furthermore, though it goes without saying, it is a misconception to assume that personal information acquired contrary to the principles of 3.4.2.2 "Appropriate acquisition" can be considered clean by merely applying the measures of 3.4.2.5.

**(2) Correspondence with the Personal Information Protection Law**

①Item 1 of Article 18 of the Personal Information Protection Law (Notification or publication of the purpose of utilization at the time of acquisition)

②Item 4 of Article 18 of the Personal Information Protection Law (Exception to notification or publication of the purpose of utilization)

**(3) Points to consider**

	Document Preparation	Operations
1	Procedures for approving acquisition of new types of personal information through methods other than direct acquisition with document from the person shall be stipulated.	① Approval by the manager shall have been obtained in accordance with predetermined procedures when acquiring new types of personal information through methods other than acquisition with document directly from the person.
2	In cases where personal information is being acquired through methods other than those stipulated in 3.4.2.4, procedures shall be stipulated for: notifying the purpose of use in advance, announcing the person of the purpose of use immediately after acquisition.	① Except in cases where the purpose of use has been notified in advance in accordance with predetermined procedures, announcement about the purpose of use shall be given to the person. ② There shall be no omissions in the notification and announcement.
3	It shall be stipulated that notification or announcement of the person shall be carried out without fail except in the cases prescribed in provisos (a) to (d).	① Notification or announcement of the individual concerned shall be carried out without fail except in the cases prescribed in the provisos.
4	Procedures for approving the application of provisos (a) to (d) shall be provided.	② Approval by the manager shall have been obtained in accordance with predetermined procedures when applying the provisos.

### 3.4.2.6 Measures concerning use

The business entity shall use the personal information within the scope necessary for the achievement of the specific purpose of use.

The business entity, when using personal information beyond the scope necessary for the achievement of the specific purpose of use, shall inform the person of at least the matters shown in a) to f) of 3.4.2.4 or the matters equivalent to or better than these in content beforehand and acquire the consent of the person except when any of the following can be applied;

- a) Cases in which the provision of personal information is based on the laws,
- b) Cases in which the provision of personal information is necessary for the protection of the life, body, or property of an individual and in which it is difficult to acquire the consent of the person,
- c) Cases in which the provision of personal information is specially necessary to improve public hygiene or promote the sound growth of children and in which it is difficult to acquire the content of the person, and
- d) Cases in which the provision of personal information is necessary for cooperating with a state institution, a local public body, or an individual or entity entrusted by one when executing the operations described by laws and in which acquiring the consent of the person may hinder the execution of the operations.

#### (1) Purpose of this requirement

Personal information must be used within the scope of the identified usage purpose range. It is necessary to note that changes in purpose of use pursuant to Article 15, Clause 2 of the Personal Information Protection Law constitute usage outside the scope of purpose according to these specifications.

Furthermore, integration of customer databases is conceivable in situations such as corporate mergers, and the purposes of use for each party of the merger stated upon acquisition do not always match. Because using information for portions of the purposes which are not shared by both parties constitutes usage outside the scope of purpose, the usage must either be limited to within the scope which is shared by both parties or usage which is extended to the portions which are not shared by both parties only after obtaining consent for these portions from the individual(s) in question.

It is necessary to establish applicable criteria for allowing provisos (b) through (d), referring to the commentary attached to the body and the Guidelines for the Fields of Economy, Trade, and Industry.

#### (2) Correspondence with the Personal Information Protection Law

- ① Article 15 of the Personal Information Protection Law (Specification of the purpose of utilization)
- ② Item 3 of Article 16 of the Personal Information Protection Law (Utilization other than for intended purposes which does not require consent)

#### (3) Points to consider

	Document Preparation	Operations
1	It shall be clearly stipulated as a principle that personal information be utilized within the scope necessary for the achievement of the specific purpose of use.	a. Personal information shall not be used other than for intended purposes.
2	Procedures for approving changes in the purpose of utilization shall be stipulated.	a. Approval by the manager shall have been obtained in accordance with predetermined procedures when the purpose of use is changed.

3	Procedures for announcing the person of the items given in 3.4.2.4 (a) to (f) or items at least equivalent to those upon making changes in the purpose of use, and for obtaining consent thereto shall be stipulated.	<p>a. Notification shall be given to the individual concerned and consent shall be obtained in accordance with predetermined procedures.</p> <p>b. The contents of such notification shall fulfill the requirements of (a) to (f).</p>
4	It shall be stipulated that use other than for intended purposes which does not require the consent of the person be limited exclusively to the cases in the proviso.	a. Use other than for intended purposes which does not require the consent of the person shall be limited exclusively to the cases in the proviso.
5	Procedures for approving the application of provisos (b) to (d) shall be stipulated.	a. Approval by the manager shall have been obtained in accordance with predetermined procedures when applying provisos (b) to (d).
6	It shall be stipulated that when it is not possible to judge whether or not a case falls under use other than for intended purposes, the manager shall be requested to judge.	a. When it is not possible to judge whether or not a case falls under use other than for intended purposes, the manager shall be requested to judge.

### 3.4.2.7 Measures when accessing to the person

The business entity, when accessing to the person, for using personal information, shall inform the person of the matters shown in a) to f) of 3.4.2.4 or the matters equivalent to or better than these in content and the acquisition method, and acquire the consent of the person except when any of the following can be applied;

- a) When the matters shown in a) to f) of 3.4.2.4 or the matters equivalent to or better than those in content are specified clearly or informed, and the consent of the person is acquired,
- b) When all or part of the handling of personal information is entrusted, in case the personal information is handled within the scope of the achievement of the purpose of use,
- c) When personal information is provided with the succession of the business because of mergers and other reasons, the business entity that already provides personal information clearly specified the matters shown in a) to f) of 3.4.2.4 or the matters equivalent to or better than those in content or informed the person of it, and acquired the consent of the person, in case the personal information is handled within the scope of the purpose of use before succession,
- d) When personal information is used jointly between specific individuals or entities, and the joint user already specified the matter clearly shown in a) to f) of 3.4.2.4 or the matters equivalent to or better than those in content or informed the person of it, and acquired the consent of the person, in case the joint user informs the user of the matters given below or the matters equivalent to or better than those in content beforehand, or places the person in a readily accessible condition for the person,
  - To use jointly
  - Items of the personal information jointly used
  - Scope of the joint users
  - Purpose of use of the joint users
  - Name or designation of those who have responsibility for control of the personal Information jointly used
  - Acquisition methods
- e) When the business entity accesses to the person by using the acquired personal information with no clear statement of the purpose of use, etc. to the person, informing the person of them, or publicly announcing them as d) of provisory clause of 3.4.2.5 can be applied, and
- f) When any of a) to d) of provisory clauses of 3.4.2.6 can be applied.

#### (1) Purpose of this requirement

Pertaining to the usage of personal information, many complaints are made about telephone calls or direct mails from unknown business entities. Nevertheless, if personal information is used appropriately, it is an important tool which can provide effective services. Both the Personal Information Protection Law and JISQ15001 strike a balance between the protection and effective utilization of personal information, and this requirement is an arena wherein that character manifests itself straightforwardly.

Consumers want to know just how and from where their personal information has been acquired. In response to this, business enterprises must, in addition to matters given in (a) through (f) of 3.4.2.4 or the matters equivalent to or better than these in content and the acquisition method, and obtain the consent of that person. The obligation to give notification about the acquisition method as well is the

major point of this requirement. The acquisition method must be specified, including details on both the source of personal information (acquisition sources such as: graduating student rosters, Basic Resident Registers, telephone books, and registry books) and how it was acquired (the acquisition process, such as: "purchased in a bookstore" or "received as a supply").

Needless to say, using personal information which does not fulfill 3.4.2.2 "Appropriate acquisition" to access the person(s) in question is not allowed. It is a misconception to assume that private information acquired through improper means can be considered clean merely through notification of the acquisition method. The same applies for 3.4.2.8.

Furthermore, even in the case of receiving a commission pursuant to proviso (b), if the assignor did not acquire information via appropriate means, the entity accepting the commission has, in effect, promoted improper acquisition and usage. This is in violation of the purport of this specification. Therefore, the entity which is entrusted must confirm that the assignor is not in violation of any laws, ordinances, and guidelines stipulated by the national government. If the commissioned party accepts a commission with knowledge that the acquisition is inappropriate, this constitutes a lack of fulfillment of 3.4.2.2 "Appropriate acquisition."

## (2) Correspondence with the Personal Information Protection Law

① Item 4 of Article 23 of the Personal Information Protection Law (Cases which do not fall under provision to a third party)

② Item 3 of Article 16 of the Personal Information Protection Law (Use other than for intended purposes which does not require consent)

## (3) Points to consider

	Document Preparation	Operations
1	Procedures for approving access to the person shall be provided.	a. Approval by the manager shall be obtained in accordance with predetermined procedures.
2	Procedures for matters given in (a) through (f) of 3.4.2.4 or the matters equivalent to or better than these in content and the acquisition method, and obtain the consent of that person shall be stipulated.	a. Consent of person shall be obtained in accordance with predetermined procedures. b. Content for matters given in (a) through (f) of 3.4.2.4 or the matters equivalent to or better than these in content and the acquisition method, and obtain the consent of that person is fulfilled.
3	It shall be stipulated that consent of a person always be required except in the cases prescribed in the provisos.	a. Consent of a person shall always be required except in the cases prescribed in the provisos.
4	Procedures for approving the application of provisos (b) to (f) shall be provided.	a. Approval by the manager shall be obtained in accordance with predetermined procedures.
5	It shall be stipulated that, in the case of proviso (b), the assignor check that personal information is appropriately handled in line with the Personal Information Protection Law and guidelines.	a. The assignor shall check with the assignor as to the status of personal information being handled in accordance with predetermined procedures.
6	In cases where proviso (d) is applied, procedures for notifying the person of the items stipulated in (d) in advance or putting them in a readily accessible form for the person in advance shall be stipulated.	a. The items stipulated in (d) shall be notified to the person or put in a readily accessible form for the person in advance in accordance with predetermined procedures.

### 3.4.2.8 Measures concerning provision

The business entity, when providing the third party with personal information, shall inform the person of the matters shown in a) to f) of 3.4.2.4 or the matters equivalent to or better than those in content and acquire the consent of the person except when any of the following can be applied;

- a) When the business entity already informed the matters clearly shown in a) to f) of 3.4.2.4 or the matters equivalent to or better than these in content to the person or inform the person of it and acquire the consent of the person in accordance with the requirements in 3.4.2.4 or 3.4.2.7,
- b) When it is difficult to acquire the consent of the person to provide people at large with much personal information widely, in case the business entities informs the person of the matters shown in the following or the matters equivalent to or better than those in content beforehand, or alternatively takes the equivalent measures,
  - Provision to the third party is the purpose of use
  - Items of personal information which is provided to the third party
  - Measures or method of provision to the third party
  - Provision of personal information which leads to the identification of the person to the third party is stopped according to the request of the person
  - Acquisition methods
- c) In the case where the information regarding directors and stockholders of the corporation and other groups included in the information regarding the corporation and other groups, or the information based on laws or disclosed or publicly announced voluntarily by the person or the corporation and other groups is provided, when the business entity informs the person of the matter given in b) or the matter equivalent to or better than that in content beforehand, or puts the matter in a readily accessible condition to the person,
- d) When the business entity entrusts all or part of the handling of personal information within the scope necessary for the achievement of the specific purpose of use,
- e) In the case where personal information is provided with the succession of business because of mergers and other reasons, when the personal information is handled within the scope of the purpose of use before succession, and
- f) When personal information is used jointly between specific persons or entities, in case the business entity informs the person of the matters given in the following or the matters equivalent to or better than that in content beforehand, or places the matters in a readily accessible condition to the person.
  - To use jointly
  - Items of the personal information jointly used
  - Scope of the joint users
  - Purpose of use of the joint users
  - Name or designation of those who have responsibility for control of the personal Information jointly used
  - Acquisition methods

**g) When any of a) to d) of provisory clauses of 3.4.2.6 can be applied**

**(1) Purpose of this requirement**

When providing a third party with personal information, obtaining the consent of the person has been gathered is a general rule.

Needless to say, it is a misconception to assume that personal information acquired through improper means can be considered clean merely through notification about the acquisition method.

Though the existence of a requirement for obtaining consent in the case of supply outside of the scope of purpose is clearly specified in "Measures concerning use and supply outside the scope of the gathering purpose" of 4.4.3.2 in the 1999 edition, it is not stipulated in the 2006 edition. The reason it is not stipulated in the 2006 edition is that supply outside of the scope of the purpose constitutes use other than for intended purposes, and so consent of the person for whom information has been gathered is necessary as a matter of course pursuant to 3.4.2.6 of the body.

Though proviso (b) is similar to the opt-out clause in the case of supply to a third party stipulated in Article 23, Clause 2 of the Personal Information Protection Law, it is not the same. Unlike the Law, it calls for, "the implementation of measures equivalent to notification." This is the requirement of implementation with all possible measures which can be accepted as being equivalent to notification. The requirement for, "announcement or easy access by the person in question," of the Personal Information Protection Law is insufficient herein. Also, proviso (b) should not be applied without careful consideration, and the establishment of applicable criteria is required.

Proviso (d) includes cases for which no plans for commission existed at the time of acquisition. Therefore no notification regarding commission was made at the time of acquisition, and due to company splitting or an expansion of business activities, ex-post facto commission became necessary.

When personal information which was acquired via a third party constitutes personal information targeted for disclosure, it is necessary to note that the requirements from 3.4.4.1 through 3.4.4.7 are applicable.

**(2) Correspondence with the Personal Information Protection Law**

- ① Article 23 of the Personal Information Protection Law (Restriction of provision to a third party)
- ② Item 3 of Article 16 of the Personal Information Protection Law (Use other than for intended purposes which does not require consent)

**(3) Points to consider**

	Document Preparation	Operations
1	Procedures for approving the provision to a third party shall be stipulated.	① Approval by the manager shall be obtained in accordance with predetermined procedures.
2	In cases where personal information is provided to a third party, procedures for notifying the person in advance of the acquisition method and of the items given in 3.4.2.4 (a) to (d) or items at least equivalent to those, and for obtaining his or her consent thereto shall be stipulated.	① Notification shall be given to the person and his or her consent shall be obtained in accordance with predetermined procedures. ② Content about which the person has been notified shall at least include the acquisition method and the items given in 3.4.2.4 (a) to (d).

		③ In cases where personal information is provided that exceeds the scope necessary for the achievement of the specified purpose of utilization, consent shall have been obtained in accordance with the procedure for use other than for intended purposes based on the provisions in 3.4.2.6.
3	It shall be stipulated that consent of the person always be required except in the cases prescribed in the provisos.	a. Consent of the person shall always be required except in the cases prescribed in the provisos.
4	Procedures for approving the application of the provisos (b) to (g) shall be provided.	a. Approval by the manager shall be obtained in accordance with predetermined procedures. b. Application criteria for the application of proviso (b) shall be stipulated.
5	In the case wherein proviso (b) is applied, procedures for taking necessary steps shall be provided.	a. Sub-items given in proviso (b) shall be notified to the person in advance, or alternatively, an equivalent measure shall be taken, in accordance with predetermined procedures.
6	In the case wherein proviso (c) is applied, procedures for taking necessary steps shall be provided.	a. The items given in (b) or items having contents equivalent thereto shall be notified to the person or put in a readily accessible form for the person in advance in accordance with predetermined procedures.
7	In cases where proviso (f) is applied, procedures shall be stipulated for notifying the person of the items in advance, or for putting them in a readily accessible form for the person in advance.	a. The items shall be notified to the person or put in a readily accessible form for the person in advance in accordance with predetermined procedures.

### 3.4.3 Appropriate control

#### 3.4.3.1 Securement of accuracy

**The business entity shall control personal information correctly in the state of up-to-date within the scope necessary for the achievement of the purpose of use.**

##### (1) Purpose of this requirement

This requirement calls for the obligation for personal information shall be controlled correctly and kept up-to-date within the scope necessary for the achievement of the purpose of use. ➡ Step 9(g) in No. 4 of Section 1

##### (2) Correspondence with the Personal Information Protection Law

① Article 19 of the Personal Information Protection Law (Securement of accuracy)

##### (3) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that checks for incorrect input be conducted.	a. Checks for incorrect input shall be conducted in accordance with predetermined procedures.
2	Procedures for determining the retention period of personal information shall be stipulated.	a. Retention periods shall be determined in accordance with predetermined procedures.
3	Procedures for backing up personal information shall be stipulated.	a. Backup shall be conducted in accordance with predetermined procedures.

### 3.4.3.2 Security control measures

**The business entity shall take the necessary and appropriate measures to prevent leakage, loss or damage, and for other control of security of personal information, according to the risk of the personal information to be handled.**

#### (1) Purpose of this requirement

This requirement prescribes the obligation for business entities to implement reasonable security control measures corresponding to the risk of the personal information handled. This is, of course, linked with 3.3.3 "Recognition, analysis and measures of risk etc." The countermeasures to be implemented pursuant to 3.3.3 should be reflected in security control measures. Uniform countermeasures for all business entities are not required. ☞ Step 7 and Step 9(g) in No. 4 of Section 1

Furthermore, though it is needless to say, acts such as the construction of facilities which are in violation of laws and ordinances such as the Fire Defense Law are not allowed, even in an attempt to increase security levels.

#### (2) Correspondence with the Personal Information Protection Law

①Article 20 of the Personal Information Protection Law (Security control measures)

#### (3) Points to consider

The security control measures described in the "Guidelines for Personal Information Protection Law Concerning Fields of Economy and Industry (October 2004)" will serve as a useful reference. However, since business entities ought to establish and execute measures as rules that should have been determined in accordance with the provisions in "Recognition, analysis and measures of risk etc." (3.3.3), it is natural that levels of security control measures vary depending on the scale and content of business. Something which is too much for one business entity might be too little for another. Business entities are required to take necessary and sufficient measures according to their scale and business content.

Security control measures	Check items
1. Physical security control measures	
1.1 Entrance/exit control	①There is a mechanism to control entrances to and exits from the buildings, rooms, machine rooms, and places where personal information is handled. ② Entrances to and exits from the buildings, rooms, machine rooms, and places where personal information is handled are restricted. ③Records of entrances to and exits from the buildings, rooms, machine rooms, and places where personal information is handled are taken and maintained. ④Records of entrances to and exits from the buildings, rooms, machine rooms, and places where personal information is handled are periodically checked.
1.2 Antitheft control	①Documents, media, portable computers, etc, on which personal information is contained shall not be left on the desk when the person in charge is not at the desk. ②Each computer containing personal information is logged off or a screensaver with a password is launched whenever the person in charge leaves her/his computer.

	<p>③Media (recording media and papers) on which personal information is recorded are kept under lock and key, and the presence of all of the media which are supposed to be present is confirmed.</p> <p>④The keys to the media storage places (recording media and papers) on which personal information is recorded are managed by specific persons.</p> <p>⑤ Any media (recording media and papers) on which personal information is recorded are made unusable when they are disposed of.</p> <p>⑥Antitheft measures are applied to portable computers, etc, on which personal information is recorded.</p> <p>⑦Rules are established and followed with regard to the use of external storage media such as floppy disks, magneto-optical disks, compact disks, and USB flash memory.</p> <p>⑧Operation manuals for information systems with which personal information is handled are not left on desks.</p>
1.3 Physical protection of equipment	①Equipment with which personal information is handled is physically protected from security risks (including theft, disposal, and breakage) as well as environmental risks (including water leaks, fire, power failures, and earthquakes).
2. Technical security control measures	
2.1 Specification and authentication with respect to access to personal information	<p>①Authentication using specification data (username, password, etc.) is performed in order to control access to personal information.</p> <p>②Default settings are not left in place in information systems on which personal information is stored.</p> <p>③Rules are established and followed to issue, update, and dispose of specification data.</p> <p>④Specification data is not stored in plain text.</p> <p>⑤ Measures are taken including setting of password expiration dates, restrictions of the reuse of the same or similar passwords, setting of a minimum number of characters for a password and suspension of specification data when login failure exceeds a certain limit.</p> <p>⑥The use of terminals and addresses for employees having access rights to personal information are restricted through such authentication measures as MAC address authentication, IP address authentication, electronic certificates and secret-sharing plans.</p>
2.2 Control of access to personal information	<p>①The number of employees who are allowed to access personal information is kept to a bare minimum.</p> <p>②Specification data for accessing personal information is not shared with more than one person.</p> <p>③Access rights granted to employees are kept to a bare minimum.</p> <p>④The number of simultaneous users of an information system on which personal information is stored is limited.</p> <p>⑤ Utilization time of the information systems on which personal information is stored is limited.</p> <p>⑥The information systems on which personal information is stored is protected against unauthorized access.</p>

	<p>⑦ Unauthorized use of applications where there is a possibility of access to personal information is prevented.</p> <p>⑧ Effectiveness of the access control functions introduced to information systems for handling personal information has been verified.</p>
2.3 Control of access rights to personal information	<p>① Control of rights to give permission to persons to access personal information is performed appropriately on a regular basis.</p> <p>② Access to information systems for handling personal information is controlled by being kept to a bare minimum.</p>
2.4 Records of access to personal information	<p>① Records of access to personal information and of the success or failure of operation thereof are acquired and maintained.</p> <p>② Acquired records are appropriately protected against leaks, loss, and damage.</p>
2.5 Protection against malware for systems handling personal information	<p>① Antivirus software is installed and kept up-to-date.</p> <p>② Security-fix programs (or security patches) for the operating systems and applications are applied.</p> <p>③ Effectiveness and stability of the protection measures against malware have been confirmed.</p> <p>④ File-sharing software, such as Winny and Share, is not installed in terminals where access to personal information is possible.</p>
2.6 Measures at the time of transfer and communication of personal information	<p>① Records of giving and receiving personal information are maintained.</p> <p>② Measures are provided in case a recording medium containing personal information is lost or stolen during transfer.</p> <p>③ Personal information being transmitted through a network which is vulnerable to sniffing (e.g. the internet and wireless LAN) is encrypted or password-locked; when, for example, the person or an employee enters or accesses personal information, or transmits data such as an attached file in an e-mail.</p>
2.7 Measures when checking the operation of information systems for handling personal information	<p>① Personal information is not used as test data when checking the operation of information systems.</p> <p>② When changes are made in information systems, it has been confirmed that the level of security of the information systems and the operational environment will not be decreased thereby.</p>
2.8 Monitoring of information systems for handling personal information	<p>① Usage of the information systems for handling personal information is periodically checked.</p> <p>② Status of access to personal information (including operation details) is periodically checked.</p>

### 3.4.3.3 Supervision of employees

**The business entity, when making its employees handle personal information, shall supervise the employees with necessary and appropriate way to ensure the control of security of the personal information.**

#### **(1) Purpose of this requirement**

This requirement calls for the appropriate supervision to the employees who engage in handling personal information.

The conclusion of a nondisclosure agreement is required at the time of a consignment contract or an employment contract with an employee. In the case of company employees, as long as a nondisclosure statement is included and prescribed in the company rules (the content of the employment contract), this constitutes the conclusion of a nondisclosure agreement. In most cases, the target for nondisclosure in the company rules is not limited to personal information only, and generally extends to all confidential information learned through the business. Therein, as long as it is recognized that personal information is included in the target for nondisclosure, there is no particular need to clearly specify "personal information."

It is common for dispatched employees (including individuals who work at the client's location as per commission) to conclude a confidentiality agreement with the business enterprise which serves as the parent organization for that individual, and for that concerned business entity to conclude a confidentiality agreement with the business entity which receives the dispatched employee. Furthermore, p.34 of the "Guidelines for Management of Trade Secrets (revised edition)" released in October 2005 by the Ministry of Economy, Trade and Industry, states the following:

"...Though the conclusion of a direct confidentiality agreement between a dispatched employee and a company supplied with a dispatched employee ("recipient company" hereinafter) is not an immediate violation of the law, the essence of the Temporary Worker Service System discourages the conclusion of a confidentiality agreement directly between the dispatched employee and the recipient company, and instead promotes the conclusion of a confidentiality agreement between the dispatched employee and the supplier as the employer of the dispatched employee, with the supplier bearing liability to the recipient company pertaining to the confidentiality of the dispatched employee..."

Though this point recognizes the right of command to the dispatched employee pursuant to the contract of supply of temporary labor, because the dispatched employee doesn't conclude an employment contract with the recipient company, the recipient company does not have the right to enforce disciplinary actions. Therefore, while a written pledge that does not constitute an employment relationship is allowed, written pledges which stipulate disciplinary actions (annulment of a contract, etc.) are not allowed because such pledges construct a state of double employment with the supplier and the recipient company as well as contradicting Article 44 ("Prohibitions pertaining to worker supply services") of the Employment Security Law.

Therefore, as long as a confidentiality agreement is concluded between the two business entities involved, there is no need for a recipient business entity to conclude a confidentiality agreement with each dispatched employee. In such cases, demanding the conclusion of a confidentiality agreement which includes disciplinary actions is in fact a violation of the law as well as an overreaction to the Personal Information Protection Law.

Also, in terms of the supervision of employees, it is necessary to be aware that items which fall under "Important matters related to the handling of personal information as pertains to employment management," which are prescribed in 39(1) of the "Guidelines regarding measures for employment management which should be taken by business entities to ensure the appropriate handling of personal information" (No. 259 in the 2004 Announcement of the Ministry of Health, Labor and Welfare) are stipulated as requiring advance notification to the labor union, etc. with a conference occurring as necessary. According to the Guidelines for the Fields of Economy, Trade and Industry, the items

pertaining to the implementation of the monitoring of employees constitute important matters in the aforementioned guidelines.

**(2) Correspondence with the Personal Information Protection Law**

① Article 21 of the Personal Information Protection Law (Supervision of employees)

**(3) Points to consider**

	Document Preparation	Operations
1	It shall be stipulated in accordance with the specifications that necessary and appropriate supervision to the employees be carried out.	a. Necessary and appropriate supervision to the employees be carried out.
2	It shall be stipulated that a non-disclosure agreement with respect to personal information be signed with an employee at the start of the employment contract or the entrustment contract.	a. A non-disclosure agreement with respect to personal information be signed with an employee at the start of the employment contract or the entrustment contract.
3	It shall be stipulated that, in cases where an employment contract or an entrustment contract is entered into, the non-disclosure provision be valid for a certain period even after the termination of the contract.	a. When an employment contract or an entrustment contract is entered into, the non-disclosure provision shall be stipulated therein to be valid for a certain period even after the termination of the contract.
4	Provisions shall be established and maintained for measures to deal with cases of breaches of the Personal Information Protection management system.	a. In cases where the Personal Information Protection Management Systems are violated, measures shall be implemented in accordance with the provisions.

### 3.4.3.4 Supervision of trustees

The business entity, when entrusting all or part of the handling of personal information, shall select the trustee who fills the sufficient protection level of personal information. For the reason, the business entity shall establish the basis for selecting the trustee.

The business entity, when entrusting all or part of the handling of personal information, shall supervise the trustee with necessary and appropriate way to the trustee to ensure the control of security of the personal information.

The business entity shall stipulate the matters given below by an agreement, and shall guarantee the sufficient protection level of personal information;

- a) Clarification of responsibility of the trust and the trustee,
- b) Items regarding security control of personal information,
- c) Items regarding re-entrusting,
- d) Content and frequency of the report about the handling status of personal information to the trust,
- e) Items which the trust can confirm that the content of agreement is observed,
- f) Measures in case the content of agreement is not observed, and
- g) Items regarding report and communication when an incident or an accident occurs.

The business entity shall at least maintain documents such as the agreement concerned over the holding period of personal information.

#### **(1) Purpose of this requirement**

This requirement stipulates the matters which should be enforced in the case of assigning the task of handling personal information. However, in the case that accidents such as leaks occur in the trustee, the mere taking of these measures does not in any way constitute exemption of liability for the assignor. The entity which bears liability to the person for whom personal information has been gathered is the assignor.

Regarding contracts such as agreements with cleaning companies, equipment maintenance companies and security companies, as long as the agreements do not contain content pertaining to the handling of personal information, the agreements fall outside the target of the requirements of 3.4.3.4 "Supervision of trustees." However, because agreements with such business entities are broadly included in content targeted under 3.4.3.2 "Security control measures," it is desirable to include within the contract the scope of entrance and access which such entities are allowed, as some of these contracted entities could possibly come into contact with personal information.

In the case where a trustee handles commissioned information without being aware of whether or not such information contains personal information, though a contract is required, the exact wording "Personal Information" is not required to be contained in the contract.

#### **(2) Correspondence with the Personal Information Protection Law**

①Article 22 of the Personal Information Protection Law (Supervision of trustees)

**(3) Points to consider**

	Document Preparation	Operations
1	Procedures for establishing and reviewing criteria for selecting trustees shall be stipulated.	①Criteria for selecting trustees shall be established in accordance with predetermined procedures.
		②Criteria for selecting trustees shall be concrete and feasible.
		③Criteria for selecting trustees shall be reviewed as necessary.
2	It shall be stipulated that trustees be evaluated based on the criteria for selection (including periodical reevaluations).	①Trustees shall be evaluated based on the criteria for selecting (including periodical reevaluations).
		② All relevant trustees shall be recognized.
3	Procedures for entering into a contract that includes the contents of (a) to (g) shall be provided.	① Consultation with the manager shall have been conducted in advance to confirm that the entrustment contract is within the scope of the specified purpose of use in accordance with predetermined procedures.
		② A contract that includes the contents of (a) to (g) shall be entered into in accordance with predetermined procedures.
		③The contents of the contract shall be implemented.
4	Procedures for retaining the relevant documents including the said contract for the holding period of personal information shall be provided.	①The relevant documents including the said contract shall be retained for the holding period of personal information in accordance with predetermined procedures.

### 3.4.4 Rights of the person concerning personal information

#### 3.4.4.1 Rights concerning personal information

Concerning the personal information in which the business entity owns the authority that the business entity can respond to all of the requests for the disclosure, correction of content, addition or deletion, stopping use, erasing, and stopping provision to the third party which are requested by the person (hereafter referred to as “personal information subject to disclosure” in 3.4.4), which is the personal information that is composed of a set of information systematically constituted as it can easily retrieve using a computer or a set of information systematically constituted as it can easily retrieve the specific personal information by arranging and classifying according to the established regulation and attaching contents, indices, symbols, etc., when the acknowledgement of the purpose of use, disclosure, correction of content, addition or deletion, stopping use, erasing and stopping provision to the third party (hereafter referred to as “disclosure and others”) are requested by the person, the business entity shall respond to these with no delay in accordance with the requirements in 3.4.4.4 to 3.4.4.7. However, the personal information when any of the following can be applied is not the personal information subject to disclosure;

- a) Cases in which it may harm the life, body, property of the person or the third party that the existence of the personal information becomes clear,
- b) Cases in which it may promote or provoke illegal or unfair acts that the existence of the personal information becomes clear,
- c) Cases in which it may harm the safety of the state, damage the confidential relationship with foreign countries or international organizations, or suffer disadvantages when negotiations with foreign countries or international organizations that the existence of the personal information becomes clear, and
- d) Cases in which it may hinder the prevention of crimes, the public safety and maintenance of order of suppression or criminal investigations, and others that the existence of the personal information becomes clear.

#### **(1) Purpose of this requirement**

If a person about whom personal information is gathered requests the disclosure of the said personal information from the business entity that handles the information, it is a general rule to comply with the request. However, if the entity handling the said personal information is merely assigned to handle this information, even if a request is issued from the person in question, the said entity usually does not have the authority to answer such a request. The entity which possesses the authority to respond to the entirety of requests for disclosure, etc., becomes the target.

It is necessary to establish applicable criteria for allowing provisos (a) through (d), referring to the commentary attached to the body and the Guidelines for the Fields of Economy, Trade, and Industry.

#### **(2) Correspondence with the Personal Information Protection Law**

- ①Item 5 of Article 2 of the Personal Information Protection Law (Definition of “retained personal data”)
- ②Article 3 of the Government Ordinance (Cases which do not fall under retained personal data)
- ③Article 4 of the Government Ordinance (Retention period for personal data) \*In these specifications, however, Article 4 of the Government Ordinance is to be waived.

**(3) Points to consider**

	Document Preparation	Operations
1	It shall be stipulated that the business entity respond to requests for disclosure etc. of personal information subject to disclosure in accordance with the Standard.	①The business entity shall respond to requests for disclosure etc. ②There shall be no omissions in personal information subject to disclosure.
2	It shall be stipulated that items excepted from the category of personal information subject to disclosure be limited to the cases in the proviso.	① Items except from the category of personal information subject to disclosure shall be limited to the cases in the proviso.
3	Procedures for approving the application of provisos shall be provided.	① Approval by the manager shall be obtained in accordance with predetermined procedures.

### 3.4.4.2 Procedures to meet requests for disclosure and others

The business entity shall stipulate the following items as the procedure in order to meet requests for disclosure and others;

- a) The other party for meeting requests for disclosure and others,
- b) Document form to submit when making a request for disclosure and others, and other methods to make a request for disclosure and others,
- c) Method to confirm that those who make a request for disclosure and others are the person or the agent, and
- d) Collection method of charges in the case of 3.4.4.4 or 3.4.4.5 (only when charges are determined).

The business entity, when establishing the procedure for meeting requests for disclosure and others from the person, shall regard that a burden with too heavy is not given to the person.

The business entity, when meeting requests from the person in accordance with 3.4.4.4 or 3.4.4.5 shall determine the amount of charges within the scope regarded reasonable in consideration of actual costs to collect charges.

#### (1) Purpose of this requirement

Regarding personal information subject to disclosure, this requirement calls for the prescription of procedures for responding to requests from the person in question for disclosure, etc. Furthermore, even if there is not even one case of a request for disclosure, etc. from the person in question, instead of merely being satisfied that no cases exist, it is necessary to suspect that insufficient functioning of the prescribed procedure is impeding requests made by such a person from reaching those in the position of responsibility.

#### (2) Correspondence with the Personal Information Protection Law

- ① Article 29 of the Personal Information Protection Law (Procedures to meet requests for disclosure etc.)
- ② Article 7 of the Government Ordinance (Items that can be provided in procedures for accepting requests for disclosure etc.)
- ③ Article 8 of the Government Ordinance (Agent who can request disclosure etc.)

#### (3) Points to consider

	Document Preparation	Operations
1	Procedures for meeting requests shall be stipulated for items (a) to (d) of the specifications respectively.	<ul style="list-style-type: none"> <li>a. Item (a) shall be properly stipulated.</li> <li>b. Item (b) shall be properly stipulated.</li> <li>c. Item (c) shall be properly stipulated.</li> <li>d. In cases where charges are collected, item (d) shall be properly stipulated.</li> </ul>
2	It shall be stipulated that the business entity take care, upon establishing procedures for meeting requests for disclosure etc., that such procedures will not impose an excessive burden on the person.	a. The business entity shall take care, upon establishing procedures for meeting requests for disclosure etc, that such procedures will not impose an excessive burden on the person.

**3.4.4.3 Making the matters concerning personal information subject to disclosure widely known, etc**

The business entity, when the acquired personal information can be applied to the personal information subject to disclosure, shall place the following items regarding the personal information subject to disclosure in a readily accessible condition to the person (including when the response is made with no delay at the request of the person);

- a) Name or designation of the business entity,
- b) Name or title, section and the contact of personal information protection manager (or the agent),
- c) Purpose of use of all of the personal information subject to disclosure (except when a) to c) of 3.4.2.5 can be applied),
- d) The other party to whom for a complaint on the handling of the personal information subject to disclosure is filed,
- e) When the business entity is the target business entity of an entity authorized under Clause 1 of Article 37 of Act on the protection of personal information (Law No.57, 2003) (hereafter referred to as “authorized personal information protection organization”), designation of the authorized personal information protection organization and the other party for applying for solution of the complaints, and
- f) Procedures stipulated in 3.4.4.2.

**(1) Purpose of this requirement**

Regarding personal information subject to disclosure, the business entity shall put the items (a) through (f) to the category of information knowable to the person. Even if, pursuant to 3.4.2.4 and 3.4.2.6 through 3.4.2.8, the business entity clearly specifies to the person about cases of personal information being targeted for disclosure, or notifies them thereof, it is necessary to situate items (a) through (f) into the information knowable to the person in order to conform to this requirement.

**(2) Correspondence with the Personal Information Protection Law**

- ①Item 1 of Article 24 of the Personal Information Protection Law (Public announcement of matters concerning retained personal data, etc.)
- ②Article 37 of the Personal Information Protection Law (Authorization of personal information protection organizations)
- ③Article 5 of the Government Ordinance (Matters necessary for ensuring the proper handling of retained personal data)

**(3) Points to consider**

	Document Preparation	Operations
1	Specific procedures for putting items (a) to (f) in an accessible form for the person shall be stipulated.	<p>a. With respect to personal information subject to disclosure, items (a) to (f) shall be put in an accessible form for the person.</p> <p>b. With respect to personal information subject to disclosure, the content of the items put in a readily accessible form for person shall fulfill the requirements of (a) to (f) in the specifications.</p>

### 3.4.4.4 Notification of purpose of use of personal information subject to disclosure

The business entity, when the notification of the purpose of use is requested from the person about personal information subject to disclosure which leads to the identification of the person, shall respond to this with no delay. However, when any of a) to c) of provisory clauses of 3.4.2.5 can be applied, or when the purpose of use of personal information subject to disclosure which leads to the identification of the person is clear in accordance with c) of 3.4.4.3, though it is not necessary to inform the person of the purpose of use, at that time, the business entity shall inform the person of that effect with no delay as well as explain the reason.

#### (1) Purpose of this requirement

This prescribes the required response to a request in the event that a request for notification pertaining to the purpose of using personal information subject to disclosure identifies the person in question.

#### (2) Correspondence with the Personal Information Protection Law

- ① Items 2 and 3 of Article 24 of the Personal Information Protection Law (Notice of the purpose of use)
- ② Article 28 of the Personal Information Protection Law (Explanation of reasons)

#### (3) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that the business entity shall respond without undue delay when the notification of the purpose of use is required from the person in regard to such personal information subject to disclosure as may lead to the identification of the person.	<ul style="list-style-type: none"> <li>a. The business entity shall respond to requests from the person in accordance with predetermined procedures.</li> <li>b. It shall be carried out without undue delay.</li> </ul>
2	Procedures for approving the content of the reply to the person (including cases where the request is to be denied) shall be stipulated.	a. Approval by the manager shall be obtained regarding the content of the reply to the person (including cases where the request is to be denied) in accordance with predetermined procedures.
3	It shall be stipulated that the purpose of utilization shall always be notified except for the cases stipulated in the proviso stipulated in the Standard.	a. The purpose of use shall always be notified except for the cases stipulated in the proviso stipulated in the Standard.
4	Procedures for approving the non-notification of the purpose of use according to the proviso shall be provided.	a. Approval by the manager shall be obtained when the purpose of utilization is not notified according to the proviso.

### 3.4.4.5 Disclosure of personal information subject to disclosure

The business entity, when the disclosure of personal information subject to disclosure which leads to the identification of the person is requested from the person (including when personal information subject to disclosure which leads to the identification of the person does not exist, the notification of the effect), except when the special procedure is stipulated by laws, shall disclose the personal information subject to disclosure with no delay on the document (when there is a method which those who make a request for agreed disclosure, the method). However, when any of a) to c) given below can be applied by disclosing, though it is not necessary to disclose all or part of it, at that time, the business entity shall inform the person of the effect with no delay as well as explain the reason;

- a) Cases in which disclosure may harm the life, body, property and other rights and interests of the person or the third party,
- b) Cases in which disclosure may seriously disturb the appropriate execution of the operations of the business entity, and
- c) Cases in which disclosure violates the laws.

#### (1) Purpose of this requirement

This prescribes the response method upon receiving a request from a person (about whom information has been gathered) relating to the personal information subject to disclosure that identifies the person in question.

It is necessary to establish applicable criteria for allowing proviso (b), referring to the commentary attached to the specifications body and the Guidelines for the Fields of Economy, Trade and Industry.

#### (2) Correspondence with the Personal Information Protection Law

- ① Article 25 of the Personal Information Protection Law (Disclosure)
- ② Article 28 of the Personal Information Protection Law (Explanation of reasons)
- ③ Article 6 of the Government Ordinance (Method of responding to requests to disclose retained personal data)

#### (3) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that the business entity respond without undue delay when the notification of the purpose of use is required from the person in regard to such personal information subject to disclosure as may lead to the identification of the person, except in cases wherein special procedures are prescribed by any other laws and regulations.	<ul style="list-style-type: none"> <li>a. The business entity shall respond to a request from a person in accordance with predetermined procedures.</li> <li>b. It shall be carried out without undue delay.</li> </ul>
2	Procedures for approving the content of the reply to the person (including cases where the request is to be denied) shall be provided.	a. Approval by the manager shall be obtained regarding the content of the reply to the person (including cases where the request is to be denied) in accordance with predetermined procedures.
3	It shall be stipulated that the business entity always meet requests for disclosure except for the cases stipulated in the proviso stipulated in the Standard.	a. The business entity shall always meet requests for disclosure except for the cases stipulated in the proviso stipulated in the Standard.

4	Procedures shall be provided for approving the decision not to disclose personal information subject to disclosure to a person according to the proviso.	a. Approval by the manager shall be obtained when personal information subject to disclosure is not disclosed to a person according to the proviso.
---	--	---

### 3.4.4.6 Correction, addition or deletion of personal information subject to disclosure

The business entity, when the correction, addition or deletion of personal information subject to disclosure is requested from the person on the ground that the content of personal information subject to disclosure which leads to the identification of the person is unfounded, except in case the special procedure is stipulated by laws, shall execute the necessary investigation with no delay within the scope necessary for the achievement of the purpose of use, and based on the results, make a correction, etc. of the personal information subject to disclosure. Also, the business entity, when a correction, etc. were made, shall inform the person of the effect and the content with no delay, and when determined that a correction, etc. were not made, shall inform the person of the effect and explain the reason with no delay.

#### (1) Purpose of this requirement

This prescribes the response method upon receiving a request from the person in regard to such personal information subject to disclosure as may lead to the identification of the person. The deletion (elimination) of the personal information targeted for disclosure itself is targeted under 3.4.4.7.

It is necessary to establish applicable criteria in cases where alterations are not executed, referring to the commentary attached to the specifications body and the Guidelines for the Fields of Economy, Trade and Industry.

#### (2) Correspondence with the Personal Information Protection Law

① Article 26 of the Personal Information Protection Law (Corrections, etc.)

#### (3) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that the business entity respond without undue delay when the correction is required in regard to personal information subject to disclosure as may lead to the identification of the person within the scope necessary for the achievement of purpose of use, except in cases wherein special procedures are prescribed by any other laws and regulations. On the basis of the results, correct, add, or delete the personal information subject to disclosure shall be implemented.	①The business entity shall respond to requests from person in accordance with predetermined procedures. ②It shall be carried out without undue delay.
2	Procedures for approving the content of the reply to the person (including cases where the request is to be denied) shall be provided.	a. Approval by the manager shall be obtained regarding the content of the reply to the person (including cases wherein the request is to be denied) in accordance with predetermined procedures.
3	Procedures for approving the decision not to correct, add, or delete the personal information subject to disclosure shall be provided.	a. Approval by the manager shall be obtained when personal information subject to disclosure is not corrected, added, or deleted.

### 3.4.4.7 Veto of use or provision of personal information subject to disclosure

The business entity, when stopping the use, erasing or stopping the provision to the third party of personal information subject to disclosure which leads to the identification of the person (hereafter referred as “stopping the use, etc.”) is requested from the person, shall respond to them. Also, the business entity, after taking measures, shall inform the person of the effect with no delay. However, when any of a) to c) of provisory clauses of 3.4.4.5 can be applied, though it is not necessary to execute the stopping of the use, etc. at that time, the business entity shall inform the person of the effect with no delay as well as explain the reason.

#### (1) Purpose of this requirement

This prescribes the response method upon receiving a request from a person about whom the person in regard to stopping the use, etc. of personal information subject to disclosure as may lead to the identification of the person. Under the Personal Information Protection Law, as long as the business entity has not violated the law by use other than for intended purposes (violation of Article 16), dishonest acquisition (violation of Article 17), or provide to a third party without consent from the person in question (violation of Article 23), the said business entity is not obligated to respond to requests for stopping the use even when made by the person in question. However, it is necessary to note that in this Standard, regardless of the presence or absence of prior or posteriori consent from the person in question, if a request has been received from the person in question, the business entity must comply with the request unconditionally.

Regarding the case of applying proviso (b) of 3.4.4.5, it is necessary to establish applicable criteria for allowing the said application, referring to the commentary attached to the Standard body and the Guidelines for the Fields of Economy, Trade and Industry.

#### (2) Correspondence with the Personal Information Protection Law

- ① Article 27 of the Personal Information Protection Law (Stopping the use, etc.)
- ② Article 28 of the Personal Information Protection Law (Explanation of reasons)

#### (3) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that, when the business entity is requested by a person for stopping the use, etc. of personal information subject to disclosure as may lead to the identification of the person concerned, the business entity accept the request and, after taking necessary measures, notify the person to that effect without undue delay.	<ul style="list-style-type: none"> <li>① The business entity shall respond to requests from the person in accordance with predetermined procedures.</li> <li>② It shall be carried out without undue delay.</li> </ul>
2	Procedures for approving the contents of the reply to the person (including cases where the request is to be denied) shall be stipulated.	① Approval by the manager shall be obtained regarding the content of the reply to the person (including cases where the request is to be denied) in accordance with predetermined procedures.

3	It shall be limited that the business entity shall always meet requests for stopping the use, etc. except for the cases stipulated in the proviso provided in the Standard.	①The business entity shall always meet requests for stopping the use, etc. except for the cases stipulated in the proviso provided in the Standard.
4	Procedures for approving the decision not for stopping the use, etc. of personal information subject to disclosure according to the proviso shall be stipulated.	① Approval by the manager shall be obtained when stopping the use, etc. of personal information subject to disclosure is not carried out according to the proviso.

### 3.4.5 Education

The business entity shall periodically give employees appropriate education. The business entity shall establish and maintain the procedure to make employees understand the following items in each relevant function and level;

- a) Importance and advantage of the conformity to the personal information protection management system,
- b) Role and responsibility to conform to the personal information protection management system, and
- c) Results to be anticipated when the personal information protection management system is violated.

The business entity shall establish, implement and maintain the procedure for determining the responsibility and authority regarding the education plan and the implementation, the report of the result and the review, the review of the plan, and the retention of the records by these.

#### (1) Purpose of this requirement

The purpose is to enforce thorough skill acquisition in employees necessary for enabling the implementation of a Personal Information Protection Management Systems. For this purpose, measures that assess the comprehension level of trainees and enforce follow up education for trainees with insufficient comprehension are necessary.

Education must be enforced for all employees. Even in departments that do not directly handle personal information, they have possibilities to come into contact with personal information (for example, information pertaining to employees, information printed on business cards, etc.)

Furthermore, PrivacyMark screening calls for education to be conducted at least once per year (refer to Article 10 of the "Guidelines for the establishment and operation of the PrivacyMark System").

#### (2) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that the business entity periodically provide all employees with proper education concerning personal information protection.	① Education shall be implemented in accordance with an education plan. ② The business entity shall provide all employees with proper education concerning personal information protection.
2	At least the contents of (a) to (c) shall be included in the stipulation or the education plan.	① Education material shall include the contents of (a) to (c).
3	Procedures for checking the participants' level of understanding shall be stipulated.	① The participants' level of understanding shall be checked.
4	Procedures for determining responsibilities and authority with respect to the planning and implementation of the education, report on the results, review of the results and the plan, and the retention of the records thereof shall be stipulated.	① Responsibilities and authority shall be determined with respect to the planning and implementation of the education, report on the results, review of the results and the plan, and the retention of the records thereof. Education shall be implemented based on level of responsibilities and authority.

### 3.5 Personal information protection management system documents

#### 3.5.1 Range of documents

The business entity shall describe in writing the following elements which become the basic of personal information protection management system;

- a) Personal information protection policy,
- b) Internal regulations,
- c) Plans, and
- d) Record required by the Standard and record which the business entity judges that it is necessary for implementing the personal information protection management system.

#### (1) Purpose of this requirement

This prescribes the necessity of describing in writing (a) through (d) from within the elements composing personal information protection management systems as the minimum requirement.

#### (2) Points to consider

	Document Preparation	Operations
1	The scope of personal information protection management systems documents shall be clear, and at least (a) to (d) shall be included.	a. Basis of elements for personal information protection management systems including (a) to (d) shall be described in writing.

### 3.5.2 Document control

The business entity shall establish, implement and maintain the procedure for controlling all documents (except for record) required by the Standard. The procedure of the document control shall include the following items.

- a) Issuance and revision of the document
- b) Clarification of correlation between the content of revision and the version number of the document
- c) To enable easy reference to necessary documents as necessary

#### (1) Purpose of this requirement

In order to provide for the thorough implementation of the established procedures, it is necessary to document those procedures. This requirement calls for the prescription of management procedures for the completed documents. However, document control itself is not the purpose of the personal information management system. The document is a step necessary for infallible operation of the Personal Information Protection Management Systems, and are sufficient as long as they are written and managed in a way that are easily understood by the employees.

#### (2) Points to consider

	Document Preparation	Operations
1	With regard to management of the documents, excluding records, specific procedures including at least (a) to (c) shall be stipulated.	①The documents shall be managed in accordance with predetermined procedures.

### 3.5.3 Record control

**The business entity shall make and maintain the record necessary for validating conformity to the personal information protection management system and the requirements of the Standard.**

**The business entity shall establish, implement and maintain the procedure for the record control.**

#### **(1) Purpose of this requirement**

This requirement calls for the creation and maintenance of records in order to validate conformity with this Standard. The records do not need to be stored in the form of paper, and can be created by any method which is easily operational. Furthermore, because the records themselves may constitute or include personal information in some cases, it is necessary to make sure that they keep specification of personal information. Also, creation of records which unnecessarily increase the amount of personal information should be avoided. In the commentary attached to the Standard, items which include records called for by this Standard are listed. These should be referred to. However, creating records only for the items listed therein may not be sufficient, as records should be created as needed.

#### **(2) Points to consider**

	Document Preparation	Operations
1	Procedures for managing records shall be clearly stipulated.	a. The records shall be managed in accordance with predetermined procedures.

### 3.6 Response to complaints and consultations

The business entity shall establish and maintain the procedure to implement the proper and prompt actions when receiving complaints and consultations from the person about the handling of personal information and the personal information protection management system.

The business entity shall establish the system necessary for achieving the mentioned purpose above.

#### (1) Purpose of this requirement

Upon receiving complaints and consultations from the person regarding the handling of personal information and the personal information management system, execution of appropriate and prompt actions are required. Complaints can be the first step to uncovering nonconformities. Furthermore, even if there has not been one case of a complaint or consultation, instead of merely being satisfied that no cases exist, it is necessary to suspect that insufficient functioning of the prescribed procedure is impeding requests made by the person in question from reaching those in the position of responsibility.

#### (2) Correspondence with the Personal Information Protection Law

- ① Article 31 of the Personal Information Protection Law (Consultation service by business entity handling personal information)
- ② Article 37 of the Personal Information Protection Law ((Authorization of personal information protection organizations)

#### (3) Points to consider

	Document Preparation	Operations
1	Procedures shall be stipulated for appropriately and promptly responding to a complaints and consultations from the person with regard to the handling of personal information and the personal information protection management systems.	① The contact point for complaints shall be clear for the individual concerned. ② Complaints and inquiries shall be accepted and responded to in accordance with predetermined procedures. ③ Responses shall be made promptly. ④ Procedures for receiving complaints and inquiries shall be functioning.
2	Procedures for approving the details of the response to the person shall be stipulated.	① Approval by the manager regarding the details of the response shall be obtained in accordance with predetermined procedures.
3	Procedures for reporting on the details of complaints and consultations on the results of the response thereto to the representative shall be stipulated.	② Such details and results shall be reported to the representative in accordance with predetermined procedures.

## 3.7 Inspection

### 3.7.1 Confirmation of operations

**The business entity shall establish and maintain the procedure to confirm periodically that the personal information protection management system is operated properly in each section and level of the business entity.**

#### (1) Purpose of this requirement

This requirement envisions the quick discovery of nonconformance and removal of causes for incidents by means of daily confirmation of operation. However, if the introduction of a process to check daily operation ultimately hinders the operation of tasks, the essential purpose of these specifications is not being served. Thus, this requirement is understood as not envisioning an unwieldy system. Implementing a pass-through survey to make sure that operation is proceeding correctly as per the rules is acceptable in fulfillment of this requirement. Also, this should include checks to see if residual risks assessed via 3.3.3 "Recognition, analysis and measures of risk, etc." are exposed. Determination of whether records of the checks are to be kept is up to the business entity. However a minimal level of record-keeping is necessary. For example,

- a) Keeping a record of company premises inspection at the time of final exit from the premises (checking the locks, etc.) and checking the records periodically
- b) Keeping a record of the first person to arrive on the premises and the last person to leave the premises, and checking the records periodically
- c) Keeping an access log for any information systems which store personal information, and checking the log periodically

The above should be carried out on a general basis. Essentially, these measures overlap as security control measures, so prescribing them as such is sufficient.

#### (2) Points to consider

	Document Preparation	Operations
1	Procedures shall be stipulated for the periodical confirmation in each section and level of the business entity with appropriate operation of the personal information protection management systems.	a. Appropriate operation of the personal information protection management systems shall be periodically confirmed in each section and level of the business entity.

### 3.7.2 Audis

The business entity shall periodically audit the conformity status of the personal information protection management system to the Standard and the operation status of the personal information protection management system.

The representative of the business entity shall appoint a personal information protection auditor within the business entity whose position is fair and objective, give the auditor the responsibility and authority to execute and report audits independent of any other responsibilities.

The personal information protection auditor shall direct the audit, and make an audit report to the representative of the business entity. In the selection of auditor and implementation of audit, the objectivity and fairness of audit shall be assured.

The business entity shall establish, implement and maintain the procedure for determining the responsibility and authority regarding the audit plan and the implementation, the report of a result and maintain of record by these.

#### (1) Purpose of this requirement

This requirement calls for periodic audits of the conformity status of the personal information protection management systems to this Standard and the operation status of the personal information protection management systems.

Upon conducting an audit of the conformity status of the personal information protection management systems to this Standard, an audit of the operation state of the personal information protection management systems is required. This is because if a system is put into operation that does not conform to this Standard, then it is of no value.

A personal information protection auditor must be selected from within the business entity, but an auditor can be selected from outside of the business entity. No specific official certification is needed to be a personal information protection auditor or auditor.

The audits must be implemented for all sections. Even in sections that do not directly handle personal information, it may be possible for them to come into contact with personal information (for example, information pertaining to employees, information printed on business cards, etc.)

Furthermore, PrivacyMark screening calls for audits to be conducted at least once per year. (Refer to Article 10 of the "Guidelines for the establishment and operation of the PrivacyMark System")

#### (2) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that conformance to Japanese Industrial Standards (JIS) and the operating status thereof shall be audited.	① Audit shall be implemented in accordance with an audit plan. ② Audit regarding conformance to JIS shall be implemented. ③ Audit regarding operating status shall be implemented. ④ Audit of all sections shall be implemented.
2	It shall be stipulated that the representative of the business entity appoint a person within the entity as the personal information protection auditor.	① Personal information protection auditor shall be appointed from within the business entity by the representative.
3	It shall be stipulated that the personal information protection auditor direct the audit and create an audit report to report to the representative of the business entity.	① Personal information protection auditor shall direct the audit and create an audit report to report to the representative of the business entity.

4	It shall be stipulated that no auditor shall audit the section to which he or she belongs.	a No auditor shall audit the section to which he or she belongs.
5	Procedures for determining responsibilities and authority with the audit plan and the implementation, the report on the result and the retention of record thereof shall be stipulated.	a. In accordance with predetermined procedures: the audit plan and the implementation, the report on the result and the retention of record thereof shall be retained.

### 3.8 Corrective actions and preventive actions

The business entity shall establish, implement and maintain the procedure for determining the responsibility and authority to assure the implementation of corrective actions against nonconformance and preventive actions. The procedure shall include the following items;

- a) Confirm the content of the nonconformance,
- b) Specify the cause of the nonconformance and propose corrective actions and preventive actions,
- c) Determine the period, and implement the proposed actions,
- d) Record the result of the corrective actions and preventive actions that were implemented, and
- e) Review the effectiveness of the corrective actions and preventive actions that were implemented.

#### (1) Purpose of this requirement

This prescribes measures to enforce corrective and preventive actions in the case that nonconformance is discovered. Examples of some areas where nonconformance could be discovered are 1(d) "Screening by an outside agency," 3.3.3 "Recognition, analysis and measures of risk, etc." 3.3.7 "Preparation for state of emergency," 3.6 "Complaints," 3.7.1 "Confirmation of operation" and 3.7.2 "Audits". All discovered nonconformance shall be assigned corrective and preventive actions via this requirement.

Corrective actions are the process of identifying the cause of nonconformance which has been discovered and implementing countermeasures to prevent the reoccurrence of such. Preventive actions are the preemptive deterrence of occurring nonconformities. The meanings of these two concepts are different. However, because it is only the originating situation which is different, and the action taken is the same in both cases, they have been organized into one requirement.

#### (2) Points to consider

	Document Preparation	Operations
1	There shall be a clear relationship between corrective and preventive actions to be implemented based on this requirement in connection with detected nonconformance.	a. Corrective and preventive actions shall be implemented in connection with detected nonconformance.
2	Procedures for the sure implementation of corrective and preventive actions, including the items given in (a) to (e), shall be stipulated.	a. Corrective and preventive actions including the items given in (a) to (e) shall be implemented in accordance with predetermined procedures.

### 3.9 Review by the representative of the business entity

The business entity shall review the personal information protection management system periodically to maintain the proper protection of personal information.

In the review by the representative of the business entity, the following items shall be considered;

- a) Report regarding audits and the operation status of the personal information protection management system,
- b) Opinions from the outside including complaints,
- c) Follow-up for the result until the previous reviews,
- d) Revision status of laws, guidelines and other codes stipulated by the state regarding the handling of personal information,
- e) Change of various environments including change of a social situation, change of a national consensus, and advance in technology,
- f) Change of domain identity for the business entity, and
- g) Proposal for improvement given from both inside and outside the business entity.

#### (1) Purpose of this requirement

In order to improve the personal information management system, this requirement calls for a review of the system based on items (a) through (g). The review should be done without postulating the current condition. Depending on the result of review, impact on future business plans, such as a revision of the allocation of economic resources, is conceivable. This requirement can be understood to call for management decisions. Thus, it is necessary to note that the requirement of 3.9 "Review by the representative of the business entity" exists on a different dimension to improvements based on the audits of 3.7.2.

#### (2) Points to consider

	Document Preparation	Operations
1	It shall be stipulated that the personal information protection management systems be reviewed at specifically determined intervals or timings.	a. Personal information protection management systems shall be reviewed by the representative in accordance with the provisions.
2	Factors to consider upon review, including the items given in (a) to (g), shall be stipulated.	a. Factors to consider upon review shall include the items given in (a) to (g).