No.	Article	Requirements to the Business Entity
1.1	General requirements	The applicant business entity shall establish, implement, maintain, and improve its personal information protection management system.
1.2	Option for the individual	The applicant business entity shall make the acquisition, use and disclosure of personal information optional for the individual.
1.3	Privacy policy (personal information protection policy)	Privacy policy (personal information protection policy) of the applicant business entity published on its website shall fulfill the following conditions. (1). It defines the concept of personal information protection of the entity, and the content thereof is appropriate. (2). It indicates matters related to the appropriate acquisition, use, and provision of personal information considering the content and the business size (including matters related to not handling personal information beyond the scope necessary to achieve the intended purpose of use; hereafter referred to as "use other than for intended purposes"), and the content thereof is appropriate. It includes provisions that are in accordance with the nine principles of the APEC Privacy Framework. (3). It indicates the strict abidance by laws, guidelines and other codes stipulated by the state regarding the handling of personal information, and the content thereof is appropriate. (4). It indicates how to prevent leakage, loss, and damage of personal information and correction of the same, and the content thereof is appropriate. (5). It indicates how to respond to complaints and consultations, and the content thereof is appropriate. (6). It indicates matters related to the continual improvement of a personal information protection management system of the entity, and the content thereof is appropriate. (7). It indicates the name of the relevant representative, and the content thereof is appropriate. (8). It indicates the date of enactment, and the date of enactment (including the date of the latest revision) is indicated in the personal information protection policy published on its website. (9). It stipulates that measures shall be taken so that information on the personal information protection policy is available to employees and the general public; and the measures are taken. The measures shall fulfill the following conditions. - When published on its website, there is a link to the personal information protection policy on the top page. - Contact information for inquiries about personal information protection is indicated in the published personal information protection policy. - The published personal information protection policy is identical to that described in the regulations of the entity.
2.1	Identification of personal information	The applicant business entity shall establish and maintain a procedure for identifying all of the personal information that the entity uses for the business. The procedure shall fulfill the following conditions. (1). Procedure for identifying every piece of personal information is provided clearly. (2). Personal information is identified in accordance with the aforementioned procedure, and approval is obtained from a manager in charge. (3). Records, etc. for identifying personal information is maintained. (4). Procedure for updating and periodic review of the records, etc. of personal information identification is provided clearly. (5). Updating and periodic review of the records, etc. of personal information identification are conducted in accordance with the aforementioned procedure.

2.2	Laws, guidelines, and other codes stipulated by the state	The applicant business entity shall establish a procedure and management system for identifying and referring to laws, guidelines, and other codes stipulated by the government of Japan regarding the handling of personal information including responding to judicial or other government subpoenas, warrants and orders. The procedure and management system shall fulfill the following conditions (1). Procedure for identifying, referring to, and maintaining laws, guidelines, and other codes stipulated by the government of Japan related to the handling of personal information is established. (2). Laws, guidelines, and other codes that need to be referenced are identified in accordance with the aforementioned procedure and updated as necessary with approval of a manager in charge. (3). Identified laws, guidelines, and other codes that need to be referenced are appropriate. (4). Identified laws, guidelines, and other codes that need to be referenced are made available for reference as necessary and such references are required to include appropriate procedures to handle inquiries, requests, etc. from abroad.
2.3	Recognition, analysis of risk, and related measures	The applicant business entity shall establish and maintain a procedure for taking necessary measures so as not to use identified personal information other than for the intended purposes. The procedure shall fulfill the following conditions. (1). Procedure for taking necessary measures is established and maintained so that relevant information shall not be used other than for the intended purposes; and the procedure is implemented. (2). Procedures for identifying risks of identified personal information throughout its lifecycle analyzing risks taking appropriate measures to deal with these risks, and recognizing any remaining risks are established clearly; and the procedures are implemented. (3). Risks of each personal information throughout its lifecycle are recognized and analyzed. Appropriate measures are taken to deal with such risks, and any remaining risks are identified clearly. (4). Measures to be taken against identified risks are approved by the representative of the entity. (5). Aforementioned measures are reflected in the regulations of the entity. (6). Procedures for periodic review and occasional review in accordance with needs are established clearly; and the review of risks is conducted in accordance with the procedures.
2.4	Resources, roles, responsibility, and authorities	Representative of the applicant business entity shall prepare indispensable resources for establishing, implementing, maintaining, and improving its personal information protection management system. The resources shall fulfill the following conditions. (1). Role and authority of each staff member are determined clearly and documented. (2). Role, responsibility, and authority of each staff member are determined clearly. (3). A personal information protection manager is appointed from within the entity by the representative. A personal information protection auditor is appointed from within the entity by the representative; and auditors as defined by the Companies Law shall not take part in the system. The personal information protection manager is not the same person as the personal protection auditor. (4). The role and authority of each staff member are informed to every staff member. (5). The personal information protection manager is obliged to report on the operational status of the personal information protection management system to the representative of the entity in order to provide a basis for reviewing and improving the personal information protection management system; and the reporting is conducted.
2.5	Internal regulations	The applicant business entity shall have detailed regulations which cover items (1) to (15) below. These regulations shall be determined in accordance with its formal internal procedures, and they shall be available for reference to all employees. (1). Procedure for identifying personal information (2). Procedure for identification, reference, and maintenance of laws, guidelines, and other codes stipulated by the government of Japan.

		(3). Procedure for recognizing and analyzing risks related to personal information and taking relevant measures (4). Authority and responsibility to protect personal information in each section and at each level of the entity (5). Preparation for states of emergency and responses thereto (when leakage, loss, or damage of personal information occurs) (6). Acquisition, use, and provision of personal information (7). Appropriate management of personal information (8). Response to a request for disclosure and other matters from individual (9). Education of staff members (10). Management of documents of the personal information protection management system (11). Responses to complaints and consultations (12). Internal inspection (13). Corrective action and preventative action (14). Review by the representative (15). Punitive provisions for violation of the internal regulations
2.6	Planning document	The applicant business entity shall make, document, and maintain a plan related to education, audit, etc., required to ensure the implementation of the personal information protection management system. The plan shall fulfill the following conditions. (1). An education plan is required to be created upon approval of the representative, and the same is created in an appropriate manner. (2). An audit plan is required to be created upon approval of the representative, and the same is created in an appropriate manner.
2.7	Emergency responses	The applicant business entity shall establish, implement, and maintain a procedure for identifying states of emergency and responding thereto. Such procedure shall be established to minimize the effects in consideration of the possibility of economic disadvantages and loss of social credibility, effects on the individual, etc., supposed in case of leakage, loss, or damage of personal information. The procedure shall fulfill the following conditions. (1). Procedure for identifying states of emergency and responding thereto is established; and the procedure is implemented. (2). Procedure for minimizing the effects in consideration of the possibility of economic disadvantages and loss of social credibility, effects on the individual, etc., supposed in case of leakage, loss, or damage of personal information, is established; and measures in accordance with the procedure are implemented. (3). Procedure for ensuring that the individual is promptly informed of the content of the personal information leaked, lost, or damaged, or ensuring that the individual is easily accessible to be informed of the content thereof, is established and measures in accordance with the procedure are implemented. (4). Procedure for publicly announcing facts, causes, and counter measures insofar as is possible without delay from the perspective of prevention of secondary damage and avoidance of the occurrence of similar events is established, and measures in accordance with the procedure are implemented. (5). Procedure for promptly reporting on facts, causes, and counter measures to related organizations (organizations that have an interest in receiving such reports) in case of emergency is established.

3.1	Identification of the purpose of use	The applicant business entity, when acquiring personal information, shall identify the purpose of use insofar as is possible, and use personal information within the scope of such purpose. The following conditions related to the identification of the purpose of use shall be fulfilled. (1). Upon acquisition of personal information, the purpose of use thereof is identified to the greatest possible extent, and personal information is used within the scope necessary for the achievement of the purpose, in accordance with the regulation of the entity; and the business of the entity is conducted accordingly. (2). Procedure for identifying the purpose of use is established, and approval is obtained from a manager in charge when identifying the purpose of use. (3). Employees of the entity that handles personal information recognize clearly the purpose of use.
3.2	Appropriate acquisition of personal information	The applicant business entity shall acquire personal information by fair and lawful means. The following conditions related to the acquisition of personal information shall be fulfilled. 1. Acquisition of personal information is carried out in a fair and lawful manner in accordance with the regulation of the entity; and the business of the entity is conducted accordingly. 2. In the case of acquiring personal information from any person other than the individual, including in cases of entrustment, the entity confirms, in accordance with the regulation of the entity, that a provider or trustee handles personal information in an appropriate manner; and the business of the entity is conducted accordingly to confirm that personal information is handled by the provider or trustee in accordance with the procedure.
3.3	Restriction of acquisition, use, and provision of specific sensitive personal information	The applicant business entity shall not acquire, use, or provide personal information that includes the following content. • Matters related to thought, creed, or religion • Matters related to race, ethnic group, family origin, registered domicile (excluding cases of information only about the prefecture in which the registered domicile exists), physical or mental disorders, criminal records, or other matters that could lead to social discrimination • Matters related to the right of workers to organize, bargain, and otherwise act collectively • Matters related to participation in a mass demonstration, exercise of the right of petition, or exercise of other political rights • Matters related to health, medical treatment, or sexual life However, this requirement shall not apply in cases in which the person explicitly consents to such acquisition, use or provision, or in any of the cases stipulated in (4) of "3.6 Measures concerning use". The following conditions related to the restriction for the sensitive personal information shall be fulfilled. (1). The entity does not acquire, use or provide the aforementioned specific sensitive personal information in accordance with its regulation; and the business of the entity is conducted accordingly. (2). Acquisition, use, and provision of the sensitive personal information are limited exclusively to the aforementioned cases in accordance with the regulation of the entity; and the business of the entity is conducted accordingly. (3). In cases of the exceptional acquisition, use, or provision of sensitive personal information, a procedure for approving such exceptional acquisition, etc., is established, and the business related thereto is conducted in accordance with the procedure and with approval of a manager in charge. (4). In cases of acquisition, use, or provision of the sensitive personal information with the consent of the individual, a procedure for obtaining the consent of such person is established; and the business of the entity is conducted accordingly and with consent of that person.
3.4	Measures for acquiring personal information with documentation directly from the individual	The applicant business entity, when acquiring personal information with documentation directly from a person, shall describe clearly the matters described below in writing beforehand and acquire consent of the individual. (1). In cases of direct acquisition of new types of personal information with documentation from an individual, procedure for approval of such direct

		acquisition; and the approval is obtained from a manager in charge in accordance with the procedure. (2). Procedure for each acquisition method in which the individual is informed of the matters in a) to h) below with documentation and consent is obtained; and the business is conducted accordingly. a) Name or nomenclature of the business entity b) Name or title, section, and contact information of the personal information protection manager (or his/her alternate) c) Purpose of use of personal information d) Matters when it is planned to provide personal information to a third party - Purpose for provision to the third party - Items of personal information to be provided - Means or method for provision - Recipient of the information, or type and attributes of organization of the recipient - When there is an agreement regarding the handling of personal information, the effect thereof e) When entrustment of personal information handling is planned, the effect thereof f) In cases of notice of the purpose of use, disclosure, correction, addition, or deletion of personal information subject to disclosure, or the right to refuse use or provision, the effect of response to the request and the person to contact for such inquiries g) Voluntary nature of the individual's provision of personal information and, when the individual does not provide personal information, consequences to such person h) When personal information is acquired by means that the individual cannot easily recognize, the effect thereof (3). Cases in which consent of the individual is not required are limited only to any of (3) a) to (3) d) of "3.5 Measures for acquiring personal information by methods other than direct acquisition with documentation" or any of (4)a) to(4) d) of "3.6 Measures concerning use." (4). Procedure for approval of the cases stipulated in (3) above, and the business is conducted accordingly with approval of a manager in charge.
3.5	Measures for acquiring personal information by methods other than direct acquisition with documentation	The applicant business entity, when acquiring personal information by methods other than direct acquisition with documentation, shall inform the individual of the purpose of use promptly, or publicly announce it unless the purpose of use is publicly announced beforehand. The following conditions related to such acquisition of personal information shall be fulfilled. (1). In cases of acquisition of new types of personal information through methods other than direct acquisition with documentation, procedure for approval of such acquisition is established; and the approval is obtained from a manager in charge in accordance with the procedure. (2). In cases of acquisition of personal information through methods other than direct acquisition with documentation, procedure for publicly announcing the purpose of use beforehand, or procedure for informing the individual of the purpose of use or publicly announcing it immediately after acquisition are established;, and the business is conducted accordingly in these cases. (3). Always notify the individual or make an announcement except in the cases prescribed in a) to d) below; and the business is conducted accordingly. a) Cases in which informing the individual of the purpose of use or publicly announcing it may harm the life, body, property, or other rights or interests of the individual or a third party. b) Cases in which informing the individual of the purpose of use or publicly announcing it may harm the rights or legitimate interests of the entity. c) Cases in which the entity cooperates with a governmental institution or a local public body when executing activities prescribed by law and in which informing the individual of the purpose of use or publicly announcing it may disturb the execution of such activities. d) Cases in which it is regarded that the purpose of use is clear in view of the circumstances of the acquisition. (4). In cases of application of any of a) to d) above, procedure for approving such application is established; and the business is conducted accordingly. (5). Application of the cases d) above is restricted in accordance with the regulation of the entity; and the business is conducted accordingly.

3.6	Measures concerning use	The applicant business entity shall use the personal information within the scope necessary for the achievement of the identified purpose of use. When using personal information beyond the scope necessary for the achievement of the identified purpose of use, the entity shall inform the person of matters equivalent to or more satisfactory than those provided upon direct acquisition of personal information with documentation from the individual in content, and obtain consent of the person. The following conditions related to the measures concerning use shall be fulfilled. (1). Personal information is utilized within the scope necessary for the achievement of the identified purpose of use in accordance with the regulation of the entity; and the business is conducted accordingly. (2). Procedure for approving changes in the purpose of use is established; and the business is conducted accordingly. (3). Procedures for informing the individual of the matters stipulated in (2) a) to (2) f) of "3.4 Measures for acquiring personal information with documentation directly from the individual" or matters equivalent to or more satisfactory than such matters in content upon making changes in the purpose of use and for obtaining consent of such person are established, and the business is conducted accordingly. (4). Use other than for intended purposes that does not require the consent of the individual is limited exclusively to the cases in a) to d) below, and the business is conducted accordingly. a) Cases in which the use of personal information is required by a law. b) Cases in which the use 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 individual. c) Cases in which the use of personal information is especially necessary to improve public hygiene or promote the sound growth of children and in which it is difficult to acquire the consent of the individual. d) Cases in which the use of personal information is necessary for cooperating with a governmental institution or a local public body when executing activities prescribed by law and in which acquiring the consent of the individual may disturb the execution of such activities. (5). In cases of application of any of a) to d) above, procedure for approving such application is established; and the business is conducted accordingly. (6). When it is found difficult to determine whether or not a case falls under the use other than for intended purposes, a manager in charge is requested to determine the same in accordance with the regulation of the entity; and the business is conducted accordingly.
3.7	Measures when accessing the individual	The applicant business entity, when accessing an individual by using his/her personal information, shall inform the individual of matters equivalent to or more satisfactory than those provided upon direct acquisition of personal information with documentation from the individual in content and the acquisition method, and obtain consent of the person. The following conditions related to the measures for accessing the individual shall be fulfilled. (1). Procedure for approving access to the person is established, and the business is conducted accordingly. (2). Procedures for informing the individual of the matters stipulated in (2) a) to (2) f) of "3.4 Measures for acquiring personal information with documentation directly from the individual" or matters equivalent to or more satisfactory than such matters in content and the acquisition method and for obtaining consent of such person are established, and the business is conducted accordingly. (3). Document for informing the individual satisfies the conditions of the matters stipulated in (2) a) to (2) f) of "3.4 Measures for acquiring personal information with documentation directly from the individual" or matters equivalent to or more satisfactory than such matters in content and the acquisition method. (4). Always require the consent of the person except in the cases in a) to e) below, and the business is conducted accordingly. a) When all or part of the handling of personal information is entrusted, and the personal information is handled within the scope necessary for the achievement of the purpose of use b) When personal information is provided with succession of business because of mergers or other reasons, and the business entity that provides personal information had already clearly specified or informed the individual about the matters stipulated in (2) a) to (2) f) of "3.4 Measures for acquiring personal information with documentation directly from the individual" or matters equivalent to or more satisfactory than such matters in content, and acquired the consent of the person, and in case the personal information is handled within the scope of the purpose of use before the business succession. c) When personal information is used jointly by specific entities, and the joint user already clearly specified or informed the individual about the matters stipulated in (2) a) to (2) f) of "3.4 Measures for acquiring personal information with documentation directly from the individual"

		or matters equivalent to or more satisfactory than such matters in content, and acquired the consent of the person, and in case the joint user informed the individual of the matters described below or the matters equivalent to or more satisfactory than such matters in content beforehand, or made information on such matters readily accessible to the person. - The fact that the personal information will be used jointly - Items of the personal information jointly used - Scope of the joint users - Purpose of use of the joint users - Name or nomenclature of a person who has responsibility for controlling the personal information jointly used - Acquisition methods of the personal information jointly used d) When the business entity accesses the individual by using the acquired personal information without describing clearly, not informing, nor publicly announcing the purpose of use, etc. to the individual as (3) d) of "3.5 Measures for acquiring personal information by methods other than direct acquisition with documentation" is applied. e) When any of (4) a) to (4) d) of "3.6 Measures concerning use" is applied. (5). In cases of application of any of a) to e) above, procedure for approving such application is established, and the business is conducted accordingly. (6). In cases in which d) above is applied, procedure therefor is established, and the business is conducted accordingly.
3.8	Measures concerning provision of personal information	The applicant business entity, when providing a third party with personal information, shall inform the individual of the acquisition method and matters equivalent to or more satisfactory than the matters stipulated in (2) a) to (2) d) of "3.4 Measures for acquiring personal information with documentation directly from the individual" in content beforehand, and obtain the consent of the person. The following conditions related to the measures concerning provisional information shall be fulfilled. (1). In cases in which personal information is provided to a third party, procedure for approving such provision is established, and the business is conducted accordingly. (2). In cases in which personal information is provided to a third party, procedures for informing the individual of the acquisition method and matters stipulated in (2) a) to (2) d) of "3.4 Measures for acquiring personal information with documentation directly from the individual" or matters equivalent to or more satisfactory than such matters in content beforehand, and for obtaining the consent of such person are established, and the business is conducted accordingly. (3). In cases in which personal information is provided beyond the scope necessary for the achievement of the identified purpose of use, consent of the person is obtained in accordance with the procedure for use other than for intended purposes stipulated in (3) of "3. 6Measures concerning use." (4). Always require the consent of the person except in the cases in a) to f) below, and the business is conducted accordingly. a) When it is difficult to acquire the consent of the person as the business entity provides a large amount of personal information widely to the public, and in case the business entity informs the individual of the matters described below or matters equivalent to or more satisfactory than such matters in content beforehand, or other equivalent alternative measures are taken. - The fact that provision to the third party is the purpose of use - Items of personal information provided to the third party - Measures or method of provision to the third party - The fact that provision of personal information that could lead to identification of the individual to the third party will be stopped in accordance with a request from the individual - Acquisition methods of the personal information b) In a case in which information regarding executives and stockholders of a corporation or organization included in information regarding the corporation or organization is provided, and the information is provided based on laws or disclosed or publicly announced voluntarily by the person or the corporation or organization; when the business entity informs the individual of the matters described in a) above or matters equivalent to or more satisfactory than that in content beforehand, or makes information on such matters readily accessible to the individual c) When the business entity entrusts all or part of the handling of personal information within the scope necessary for the achievement of the identified purpose of use

		d) In a case in which personal information is provided with succession of business because of mergers or other reasons, and when the personal information is handled within the scope of the purpose of use before the business succession e) When personal information is used jointly by specific entities, and in case the business entity informs the individual of the matters described below or matters equivalent to or more satisfactory than such matters in content beforehand, or makes information on such matters readily accessible to the individual. - The fact that the personal information will be used jointly - Items of the personal information jointly used - Scope of the joint users - Purpose of use of the joint users - Name or nomenclature of a person who has responsibility for controlling the personal information jointly used - Acquisition methods of the personal information f) When any of (4) a) to d) of the proviso of "3.6 (measures concerning use)" can be applied. (5). In cases of application of any of a) to f) above, procedure for approving such application is established, and the business is conducted accordingly. (6). In cases in which a) above is applied, procedures for notifying the individual of each sub-item in advance, or taking alternative equivalent measures are established, and the business is conducted accordingly. (7). In cases in which b) above is applied, procedures for notifying the individual of the matters described in a) or matters equivalent to or more satisfactory than such matters in content beforehand, or making information on such matters readily accessible to the individual are established, and the business is conducted accordingly. (8). In cases in which e) above is applied, procedure therefor is established, and the business is conducted accordingly.

4.1	Securement of accuracy of personal information	The applicant business entity shall maintain personal information correct and in an up-to-date state, within the scope of the purpose of use. The following conditions related to the maintenance of personal information shall be fulfilled. (1). Procedure for enabling reference and confirmation upon input of personal information a) Person in charge of inputting personal information is clearly indicated. b) Procedure for enabling reference to and confirmation of inputted personal information is clearly indicated. c) Referencing and confirmation work are conducted in accordance with the procedure. (2). Procedure for data correction a) Person in charge of correcting personal information data is clearly indicated. b) Procedure for discovering inaccuracy or inconsistency of corrected personal information data is clearly indicated. c) Procedure for enabling reference to and confirmation of corrected personal information data is clearly indicated. d) Data correction work is conducted in accordance with the procedure. (3). Procedure for verifying that personal information is accurate and in an up-to-date state a) Person in charge of verifying that personal information is accurate and in an up-to-date state is clearly indicated. b) Procedures for verifying that personal information is accurate and in an up-to-date state and correcting it as necessary are clearly indicated. c) Verification work is conducted in accordance with the procedure. (4). Update of matters recorded a) Person in charge of maintenance of records of conducted work is clearly indicated. b) Procedure for updating records of conducted work is clearly indicated. c) Procedure for keeping records of conducted work is clearly indicated. d) Update of matters recorded is conducted in accordance with the procedure. (5). Retention period of personal information a) Person in charge of determining retention period is clearly indicated. b) A criterion for determining retention period is clearly indicated. c) Retention period is determined in accordance with the procedure.
4.2	Security control measures for personal information	The applicant business entity, as shown below I and II, shall take necessary and appropriate measures to prevent leakage, loss, and damage of personal information, and other security control measures for personal information, according to the risk of the personal information to be handled. I. Measures that should be taken as physical security control measures (1). Entrance/exit control a) Entrance to and exit from the buildings, rooms, server rooms, and places in which personal information is handled are restricted. b) Records of entrance to and exit from the buildings, rooms, server rooms, and places in which personal information is handled are made and maintained. c) Records of entrance to and exit from the buildings, rooms, server rooms, and places in which personal information is handled are periodically checked. (2). Antitheft control a) Documents, media, portable computers, etc., on which personal information is contained are not left on the desk when the person in charge is not at the desk. b) Each computer with which personal information is handled is logged off or a screensaver with a password is launched whenever the person in charge leaves his/her computer. c) Any media (papers and recording media) on which personal information is recorded are kept under lock and key.

		d) Keys to the storage places for media on which personal information is recorded are in the custody of a person in change. e) Any media (papers and recording media) on which personal information is recorded are made unusable when they are disposed of. f) Antitheft measures are applied to portable computers, etc., on which personal information is recorded. g) Rules are established and followed with regard to the use of portable computers and external storage media such as, USB flash memory, and CD-ROM. h) Operation manuals for information systems with which personal information is handled are not left on desks. (3). Physical protection of equipment and devices, etc. a) Equipment and devices, etc., with which personal information is handled are physically protected from security risks (including theft, disposal, and breakage) as well as environmental risks (including water leaks, fire, power failures, and earthquakes). II. Measures that should be taken as technical security control measures (1). Identification and authentication with respect to access to personal information a) Authentication using identification data (username, password, etc.) is performed in order to control access to personal information. b) Default settings for information systems on which personal information is stored are properly changed as necessary. c) Issuance, updating, and disposal of identification data are taking place in accordance with the rules. d) Identification data is not stored in plain text. e) Setting and use of identification data are taking place in accordance with the rules. f) Use of terminals and addresses, etc., for employees having access rights to personal information is restricted. (2). Control of access to personal information a) The number of employees who have access to personal information is kept to a bare minimum. b) Identification data for accessing personal information is not shared with more than one person. c) Access rights granted to employees are kept to a bare minimum. d) The number of simultaneous users of an information system on which personal information is stored is limited. e) Utilization time of the information systems on which personal information is stored is limited. f) Information systems on which personal information is stored are protected against unauthorized access. g) Unauthorized use of applications which enables accessing to personal information is prevented. h) Effectiveness of the access control functions introduced to the information systems for handling personal information has been verified. (3). Control of access rights to personal information a) Control of rights to give permission to persons to access personal information is performed appropriately on a regular basis. b) Access to information systems for handling personal information is controlled by being kept to a bare minimum. (4). Records of access to personal information a) Records of access to personal information and of the success or failure of such operations are acquired and maintained. b) Acquired records are appropriately protected against leaks, loss, and damage. (5). Protection measures against malware for information systems handling personal information a) Antivirus software is installed in the information system. b) Security-fix programs (or security patches) for the operating systems and applications are applied. c) Effectiveness and stability of the protection measures against malware are confirmed. d) File-sharing software (such as Winny, Share, and Cabos) is not installed in terminals from which access to personal information is possible. (6). Measures at the time of transfer and communication of personal information a) Records of giving and receiving personal information are maintained upon transfer of personal information. b) Measures are established in case a recording medium containing personal information is lost or stolen during transfer. c) Personal information being transmitted through a network that is vulnerable to sniffing (e.g. internet and wireless LAN) is encrypted or password-locked for security purposes. (7). Measures when checking the operations of information systems for handling personal information a) Personal information is not used as test data when checking the operations of the information systems.

		b) When changes are made in the information systems, it is confirmed that the level of security of the information systems and the operational environment are not decreased thereby. (8). Monitoring of information systems for handling personal information a) Usage of the information systems for handling personal information is periodically checked. b) Status of access to personal information (including operation details) is periodically checked.
4.3	Supervision of employees	The applicant business entity, when making its employees handle personal information, shall supervise the employees in an appropriate manner and to the extent necessary to ensure security control measures of the personal information. The following conditions related to the supervision of employees shall be fulfilled. (1). Regulation to conduct necessary and appropriate supervision of the employees is established, and the business is conducted accordingly. (2). Non-disclosure agreement with respect to personal information is signed with each employee at the start of employment contract or entrustment contract in accordance with the regulation of the entity, and the business is conducted accordingly. (3). At the start of employment contract or entrustment contract, etc., the non-disclosure provision is made valid for a certain period even after the termination of the contract in accordance with the regulation of the entity, and the business is conducted accordingly. (4). Regulations regarding measures to deal with cases of breaches of the personal information protection management system are established, and the business is conducted accordingly. (5). In cases of monitoring of employees using a video or online, implementation measures of such monitoring are established, and the business is conducted accordingly. (6). Regulations concerning a person in charge of the monitoring and his/her authority are established, and the business is conducted accordingly. (7). Regulations concerning the monitoring are established and shared throughout the entity beforehand; and audit or confirmation with regard to proper implementation of the monitoring is conducted.

4.4	Supervision of trustees	The applicant business entity, when entrusting handling of personal information, shall establish criteria for selecting trustees and select trustees who satisfy the requirements for the sufficient protection level that is the same as or higher than the protection level of the applicant business entity.(*The term "trustees" here includes processors, agents, contractors or other service providers who are entrusted to handle personal information.) The applicant business entity shall supervise the trustee in an appropriate manner and to the extent necessary to ensure the security control of the entrusted personal information. The following conditions related to the supervision of trustees shall be fulfilled. (1). Procedure for establishing and reviewing criteria for selecting trustees is established, and concrete and feasible criteria for selecting trustees is set in place accordingly. (2). Review of the criteria for selecting trustees is conducted as necessary. (3). Trustees are evaluated based on the criteria for selecting trustees (including periodical reevaluations) in accordance with the regulation of the entity, and the business is conducted accordingly. (4). All relevant trustees are recognized. (5). Procedure for concluding a contract that includes the content of a) to g) below is established, and the business is conducted accordingly. a) Clarification of responsibilities of the trustor and trustee b) Matters regarding security control of personal information c) Matters regarding re-entrusting d) Content and frequency of reports about the handling status of personal information to the trustor e) Matters that enable the trustor to confirm that the content of the agreement is observed f) Measures in case the content of the agreement is not observed g) Matters regarding report and communication to the trustor when an incident or an accident occurs (6). Procedure for retaining the relevant documents including the above said contract for the personal information retention period is established, and the business is conducted accordingly.
5.1	Rights of the individual concerning personal information	Concerning personal information regarding which the applicant business entity has the authority to respond to all requests for the disclosure, correction of content, addition or deletion, stopping use, erasing, and stopping provision to a third party thereof made by the individual, in cases in which such personal information is composed systematically and constituted so as to allow retrieval of specific pieces of information by computers (hereafter referred to as “personal information subject to disclosure”), the business entity shall respond to such requests within one month, in principle, and if it cannot respond to them within one month, it shall inform the individual of the status and reason. The following conditions related to the rights of individual concerning personal information shall be fulfilled. (1). The business entity established regulations to respond to requests for disclosure and other requests regarding personal information subject to disclosure by the individual, and the business is conducted accordingly. (2). There are no omissions in personal information subject to disclosure. (3). Items exempted from the category of personal information subject to disclosure are limited to cases in the exceptional provisions. (4). Procedure for approving the application of the exceptional provisions is established, and the business is conducted accordingly.
5.2	Procedure for satisfying the rights of individual concerning personal information	The applicant business entity shall establish a procedure including the following items to respond to requests for disclosure and other requests regarding personal information. a) Person to contact for the requests for disclosure and other requests regarding personal information are submitted b) Form of documentation to be submitted when making the requests for disclosure and other requests regarding personal information, and other methods for making the requests c) Method for confirming that the individual who makes a request for disclosure and other requests is the individual to whom the personal information belongs to or his/her alternate d) Method for collecting charges in cases of disclosure, correction, addition, or deletion of personal information

		The applicant business entity shall make sure, upon establishing the procedure for responding to requests for disclosure and other requests, that such procedure does not impose an excessive burden on the requesting individual and the requested information must be provided to individuals in an easily comprehensible way.
5.3	Making the matters concerning personal information subject to disclosure widely known	The applicant business entity shall configure the personal information subject to disclosure in a condition that it is readily accessible by the individual, or response is given without delay at the request of the individual. The following conditions regarding the issue shall be fulfilled. (1). Concrete procedure for making the matters described below in a) to f) readily accessible by the individual is established, and the business is conducted accordingly. a) Name of the applicant business entity and a person to contact for resolution of complaints b) Name or title, section and contact information of the personal information protection manager (or his/her alternate) c) Purpose of use of all of personal information subject to disclosure d) Person to contact for complaints regarding handling of personal information subject to disclosure e) Name of the authorized personal information protection organization, and person to contact for resolution of complaints f) Procedure for responding to requests for disclosure and other requests
5.4	Notification regarding purpose of use of personal information subject to disclosure	When notification of purpose of use is requested from an individual concerning personal information subject to disclosure that leads to identification of the individual, the applicant business entity shall respond thereto without delay. However, when any of (3) a) to (3) c) of "3.5 Measures for acquiring personal information by methods other than direct acquisition with documentation" is applied, or when the purpose of use of personal information subject to disclosure which leads to the identification of the individual is clear in accordance with (1) c) of "5.3 Making the matters concerning personal information subject to disclosure widely known," it is not necessary to inform the individual of the purpose of use, while the business entity shall inform the individual to such effect without delay and explain the relevant reason. The following conditions regarding the issue shall be fulfilled. (1). The applicant business entity establishes regulations to respond without undue delay when notification of the purpose of use is requested by an individual, and the business is conducted accordingly. (2). Procedure for approving the content of the reply to the individual (including cases in which the request is to be denied) is established, and such procedure is clearly indicated. (3). Notification regarding the purpose of use is always provided except for the cases stipulated above. (4). Procedure for approving not to notify the purpose of use according to the exceptional provisions stipulated above is established, and the business is conducted accordingly.
5.5	Disclosure of personal information subject to disclosure	When disclosure of personal information is requested from an individual concerning personal information subject to disclosure that leads to identification of the individual, unless there are any relevant laws prohibiting the disclosure, the applicant business entity shall disclose the personal information subject to disclosure without delay via document to the individual. However, when any of a) to c) given below is applicable upon disclosure, it is not necessary to disclose all or part of the relevant information, while the business entity shall inform the individual to such effect without delay and explain the relevant reason. a) Cases in which disclosure may harm the life, body, property, or other rights or interests of the individual or a third party b) Cases in which disclosure may seriously disturb the appropriate execution of the business of the business entity c) Cases in which disclosure violates relevant law The following conditions regarding the issue shall be fulfilled. (1). The applicant business entity establishes regulations to respond without undue delay when disclosure of personal information subject to disclosure that leads to the identification of the individual is requested by an individual, except when a special procedure is stipulated by relevant

		law and the business is conducted accordingly. (2). Procedure for approving the content of the reply to the individual (including cases in which the request is to be denied) is established, and such procedure is clearly indicated. Approval of a manager in charge regarding the content of the reply to the individual is obtained in accordance with the procedure. (3). Response to a request for disclosure is always provided except for the cases stipulated in a) to c) above. (4). Procedure for approving not to disclosure all or part of the relevant information according to the exceptional provisions stipulated above is established, and the business is conducted accordingly.
5.6	Correction, addition, or deletion of personal information subject to disclosure	When correction, addition, or deletion of personal information subject to disclosure is requested from an individual claiming that content of the personal information is unfounded, except in cases in which there is any legal basis, the applicant business entity shall execute a necessary investigation without delay within the scope of the purpose of use, and make corrections, etc. The following conditions regarding the issue shall be fulfilled. (1). The applicant business entity established regulations to execute the necessary investigation without delay within the scope necessary for achievement of the purpose of use and make a correction, etc. based on the result when correction, etc., of personal information subject to disclosure that leads to the identification of the individual is requested by an individual, except when a special procedure is stipulated by relevant law, and the business is conducted accordingly. (2). Procedure for approving the content of the reply to the individual (including cases in which the request is to be denied) is established, and such procedure is clearly indicated. Approval of a manager in charge regarding the content of the reply to the individual is obtained in accordance with the procedure. (3). Procedure for approving not to make a correction, etc. is established, and approval of a manager in charge is obtained when personal information is not corrected, etc.
5.7	Veto of use or provision of personal information subject to disclosure	When stopping use of, erasing, amendment, or stopping provision to a third party of personal information subject to disclosure that leads to the identification of the individual is requested by an individual, the applicant business entity shall respond thereto. Also, the business entity, after taking relevant measures, shall inform the individual of the result providing a copy on correction of personal information including deletion and amendment ~~to such effect~~ without delay. However, when any of (3) a) to (3) c) of "3.5 Measures for acquiring personal information by methods other than direct acquisition with documentation" is applied, it is not necessary to execute the stopping of the use, etc. while the business entity shall inform the individual to such effect without delay and explain the relevant reason. (1). The applicant business entity establishes regulations to respond to a request from an individual regarding stopping use, etc., of personal information subject to disclosure that leads to the identification of the individual and the business is conducted accordingly. (2). The applicant business entity establishes regulations to inform the individual after taking relevant measure without delay, and the business is conducted accordingly. (3). Procedure for approving the content of the reply to the individual (including cases in which the request is to be denied) is established, and such procedure is clearly indicated. Approval of a manager in charge regarding the content of the reply to the individual is obtained in accordance with the procedure. (4). Response to a request for stopping the use, etc. is always provided except for the cases stipulated above. (5). Procedure for approving not to stop the use, etc., according to the exceptional provisions is established, and approval of a manager in charge is obtained when stopping the use, etc. is not carried out according to the exceptional provisions.
6	Training of employees	The applicant business entity shall periodically provide employees with appropriate training, and establish and maintain a procedure for making employees understand necessary matters for each relevant function and level. The following conditions regarding the training shall be fulfilled.

		(1). The applicant business entity establishes regulations to periodically provide all employees with appropriate training concerning personal information protection, and the training is provided in accordance with a training plan. (2). All employees are provided with appropriate training concerning personal information protection. (3). The regulation or training plan includes at least the contents of a) to c) below. a) Importance and advantage of being conformity with the personal information protection management system b) Role and responsibility to conform with the personal information protection management system c) Results to be anticipated when the personal information protection management system is violated (4). Training materials include the contents of a) to c) above. (5). Procedure for checking the participants' level of understanding is established, and the business is conducted accordingly. (6). Procedures for determining the responsibility and authority regarding the training plan and the implementation thereof, reporting of results of the training and their review, review of the training plan, and retention of records thereof are established, and the business is conducted accordingly.
7.1	Document control	The applicant business entity shall establish, implement, and maintain a procedure for controlling all relevant documents (except for records). The procedure for document control shall include the following items, and the business is conducted accordingly. a) Matters related to issuance and revision of documents b) Clarification of correlation between the content of a revision and the version number of the relevant document c) Enabling of easy reference to necessary documents as necessary
7.2	Record control	The applicant business entity shall make and maintain records necessary for validating conformance of its personal information protection management system with the requirements of the certification standards. The business entity shall establish, implement, and maintain a procedure for record control, and the business is conducted accordingly.
8	Responses to complaints and consultation	The applicant business entity shall establish and maintain a procedure and system for implementing proper and prompt actions when receiving complaints from an individual and undertaking consultation with the individual. The following conditions regarding the issue shall be fulfilled. (1) Procedures for accepting and appropriately and promptly responding to complaints from an individual and undertaking consultation with the individual with regard to the handling of personal information as well as the personal information protection management system of the entity are established. (2) Person to be contacted for complaints and requests for consultation is clearly identified. (3) Complaints and requests for consultation are accepted and responded in accordance with the procedures. (4) The procedures for accepting complaints and requests for consultation are functioning, and responses are made promptly. (5) Procedure for approving the content of the responses to be made to the individual is established, and the business is conducted accordingly, while approval of a manager in charge regarding the content of the responses is obtained. (6) Procedure for reporting on the details of complaints and consultation and the results of the responses thereto to representative of the entity is established, and the reporting is conducted accordingly.
9.1	Confirmation of operation of personal information protection management system	The applicant business entity shall establish and maintain a procedure for confirming periodically that the personal information protection management system is being operated properly in each section and at each level of the business entity, and the business is conducted accordingly.

9.2	Internal audit	The applicant business entity shall periodically conduct internal audit regarding the status of the conformance of its personal information protection management system with the requirements of the certification standards, and the operational status of the personal information protection management system. The following conditions regarding the internal audit shall be fulfilled. (1) The applicant business entity establishes regulations to conduct internal audit with regard to conformance with the requirements of the certification standards and the operating status thereof , and the internal audit is implemented in accordance with an audit plan. (2) Internal audit regarding the conformance and operating status is conducted at all sections of the entity. (3) The applicant business entity establishes regulations to let representative of the entity appoint a person within the entity whose position is fair and objective as the personal information protection auditor, and the business is conducted accordingly. (4) The applicant business entity establishes regulations to let the personal information protection auditor direct the internal audit, prepare an audit report, and submit it to representative of the entity, and the business is conducted accordingly. (5) The applicant business entity establishes regulations to ensure that objectivity and fairness of the internal audit and no auditor audits a section to which he or she belongs to, and the business is conducted accordingly. (6) Procedures for determining responsibility and authority regarding the audit plan and the implementation thereof are established, and the business is conducted accordingly.
10	Corrective actions and preventive actions	The applicant business entity shall establish, implement, and maintain a procedure for determining the responsibility and authority to ensure the implementation of corrective actions against non conformance and preventive actions, and the business is conducted accordingly. The procedure shall include the following items. a) Confirm the content of the non conformance. b) Identify the cause of the non conformance and propose corrective actions and preventive actions. c) Determine necessary period for the action, and implement the proposed actions. d) Record the results of the corrective actions and preventive actions that were implemented. e) Review the effectiveness of the corrective actions and preventive actions that were implemented.
11	Review by representative	Representative of the applicant business entity shall review the personal information protection management system of the entity periodically to maintain the proper protection of personal information. The applicant business entity shall establish regulations to conduct the review at specifically determined times, and the business is conducted accordingly. The following items shall be considered in the review. a) Report regarding internal audits and the operational status of the personal information protection management system of the entity b) Opinions from the outside, including complaints c) Follow-up on the results of previous reviews d) Revision status of laws, guidelines, and other codes stipulated by the government of Japan regarding the handling of personal information e) Changes in various environments, including changes of social situation, changes in a national consensus, and advances in technology f) Change of business scope of the entity g) Proposals for improvement from both inside and outside the entity