Information Security Management Criteria for Our Business Partners

Ver. 2.11

March 1, 2019

Global Procurement Company
Information Security Department
Panasonic Corporation

Table of Contents

I. Information Security Policy of the Panasonic Group

Panasonic Corporation and its affiliated companies (hereinafter collectively referred to as "Panasonic") intend to gain customer satisfaction and trust through our advanced technologies, products and services, in accordance with our Basic Management Philosophy. In order to achieve this goal, Panasonic fully recognizes the importance of securing information, including, but not limited to, our customers' general, personal and proprietary information, and regard the information security as one of our most important management strategies. We will, therefore, strive to contribute to the sound information-oriented society by implementing the Information Security Management Criteria as described below.

1. Information Security Structure

We shall build a structure responsible for securing information in each organization, and focus on the proper management of the secured information (hereinafter "Information Security") by creating and implementing appropriate rules.

2. Management of Information Assets

We shall properly manage information to ensure its security by clarifying how to handle such information in accordance with its importance and risk level.

3. Education and Training

We shall provide continuous education and training on Information Security to all of our executives and employees in order to raise their awareness level and thoroughly implement various rules on Information Security among them. Personnel who violate those rules will be strictly dealt with, and it may result in a disciplinary action.

4. Provision of Secure Products and Services

We shall strive to provide our customers with products and services that can be used securely, by paying special attention to the security of the customers' information.

5. Compliance with Laws and Continuous Improvement

We shall comply with relevant laws and other regulations, and strive for the continuous improvement and reinforcement of Information Security, in accordance with the changes in social environment.

II. Execution of Non-Disclosure Agreement

Whenever Panasonic and its business partners share confidential information, a general business agreement with a non-disclosure clause, or a stand-alone non-disclosure agreement, which includes the provisions described below, shall be executed.

a) Confidentiality obligation

b) Scope of information subject to non-disclosure

c) Period of compliance (including unlimited duration)

d) Limitation on the intended use of confidential information

e) Limitation on the personnel with access to confidential information to those who need to know such information for business purposes

f) Procedures for the management of confidential information

g) Restriction on duplication and copying of confidential information

h) Rules on return or disposal of confidential information at the end of the compliance period

i) Procedures for verification by Panasonic on how confidential information is stored or handled, such as a hearing or an audit

j) Measures to be taken in case of a breach of the agreement, such as inserting provisions for Panasonic's right to seek injunction in the market as well as compensation for damage

k) Prohibition of re-commissioning to outsourced companies without Panasonic's prior consent

l) Prohibition of the use of privately-owned PCs for business purposes

III. Information Security Management Criteria for Business Partners

1. Objectives

The objectives of these criteria are to provide business partners, who share Panasonic's confidential information (hereinafter “Business Partners”), of the guidelines to be followed in order to implement the appropriate measures for Information Security, so that Panasonic can further promote its Information Security and proper handling and management of our customers' information, personal information, and our own proprietary information with respect to technologies, products, quality of products, and services. Panasonic can thereby accomplish its social responsibilities as a global company and contribute to build a sound information-oriented society.

The establishment of an environment to manage and use information properly enables both Panasonic and its Business Partners to conduct effective and secure business, and to achieve the stable business continuity and mutual prosperity.

2. Application

These criteria shall be applied to the entire operations of handling and managing the relevant information, and the general business operations (technology transfer, outsourcing, material procurement, etc.), conducted by Business Partners who share confidential information specified by Panasonic.

The scope of application of these criteria shall include confidential information shared with Panasonic and confidential information originated from such confidential information (hereinafter "Confidential Information").

The forms of Confidential Information include, but not limited to, papers which contain Confidential Information (hereinafter “Papers”), digitized Confidential Information, (hereinafter “Digitized Information”, objects embodying Confidential Information (hereinafter “Embodiments”), and know-how.

Additional management measures, such as a memorandum of understanding and a non-disclosure agreement, shall be applied to strictly confidential information or important information which requires particularly strict management.

3. Information Security Requirements for Business Partners

Business Partners are required to implement the five Information Security Criteria, described in (1) to (5) below.

It should be noted that Panasonic may restrict the sharing of Confidential Information with any Business Partners who are unable to meet the level of Information Security specified by Panasonic. Thus, Panasonic hereby requests your company to ensure the implementation of these Information Security Criteria.

(1) Establishment of Structure for Information Security Management

An organizational structure to promote Information Security shall be established.

(1-1) Establishment of structure for Information Security Management

(1-2) Establishment of basic policies and rules on how to manage Information Security

(2) Confidentiality Management of Information Assets

Information requiring confidentiality management shall be identified and managed appropriately.

(2-1) Identification of Confidential Information

(2-2) Management of exchange/return procedure of Confidential Information

(2-3) Physical security controls

(2-4) Management of user IDs and passwords of the IT system users

(2-5) Management of installation/usage/disposal of the IT systems, such as PCs and servers

(2-6) Countermeasures against malicious programs

(2-7) Implementation of data backups

(2-8) Management of outsourced companies which share Confidential Information with

(3) Controls for Personnel Security

Controls for personnel security, such as an execution of non-disclosure agreement, shall be implemented to prevent information leakage.

(3-1) Conducting education and training on Information Security

(3-2) Obtaining signed agreements for confidentiality obligation from employees, etc.

(4) Responses to Information Security Incidents

Procedures for responding to Information Security incidents shall be clarified and implemented.

(4-1) Establishment of an organizational structure for incident reports/responses

(4-2) Clarification of procedures for incident responses

(5) Implementation of Information Security Management

Information Security Management shall be implemented for continuous

improvement.

(5-1) Periodical verification of the implementation of Information Security activities

(5-2) Implementation of activities for improvement based on the verified results

4. Details of Requirements

The details of requirements in "**3. Information Security Requirements for Business Partners**" are further specified below. Hereinafter, Business Partners are referred to as "Your Company."

(1) Establishment of Structure for Information Security Management

1-1	Establish an organizational structure for Information Security Management, and clarify and document its responsibilities/assignments.
1-2	Establish and document basic policies and rules on Information Security.

(2) Confidentiality Management of Information Assets

(2-1) Identification of Confidential Information

2-1-1	Identify information assets and create a list of information assets for Confidential Information, and update such list regularly.
2-1-2	Manage the reproductions or copies of Confidential Information in the same manner as the originals, in case such reproductions are made pursuant to a contract with Panasonic.
2-1-3	Distinguish Confidential Information clearly from other information, and manage it separately.

(2-2) Management of exchange/return procedure of Confidential Information

2-2-1	Exchange Confidential Information pursuant to the rules agreed upon between Your Company and Panasonic.
2-2-2	Establish rules for taking Confidential Information out of the designated areas, and implement all applicable procedures in a) to d) below. a) When taking Confidential Information out, obtain an approval from the responsible management personnel. b) While being taken out, always keep Confidential Information at hand. c) When Digitized Information on PCs, PDAs, or storage media are taken out, or sent by e-mail, encrypt such information. d) When Embodiments (molds, prototypes, etc.) are taken out, keep them out of sight of outsiders.

2-2-3	Return Confidential Information to Panasonic in accordance with the procedures agreed upon between Your Company and Panasonic at the completion of the contracted business. When Your Company disposes of Confidential Information, follow all applicable procedures described in a) to d) below, pursuant to the agreement with Panasonic. Provide records of the disposal upon request by Panasonic. a) Completely delete Digitized Information that is stored on servers, PCs, PDAs, or storage media. b) Shred, dissolve or incinerate Papers (documents, drawings, etc.). c) Destroy Embodiments (molds, prototypes, etc.) to make the original information unrecognizable. d) When outsourcing the disposition of waste to an industrial waste disposal contractor, etc., require such a contractor to execute a non-disclosure agreement.

(2-3) Physical security controls

2-3-1	Restrict the outsiders from entering the areas, including company premises, buildings and rooms, where Confidential Information is handled, by setting up physical measures.
2-3-2	Ensure that only the personnel who need to know the relevant information for business purposes will be given a permission to enter the areas where Confidential Information is handled.
2-3-3	Establish a procedure to distinguish employees from outside visitors.
2-3-4	Keep records, including the images of surveillance cameras, for both or either entry to/exit from the areas where Confidential Information is handled, and regularly review the status of such logs to confirm that they are properly taken.
2-3-5	Prohibit anyone from bringing privately-owned PCs, mobile phones, PDAs, storage media (SD cards, USB memories, etc.), communication devices (wireless LAN, etc.) into the areas where Confidential Information is handled. If bringing such devices into such areas is necessary, follow the procedures a) and b) below. a) Obtain an approval for bringing in such devices from the responsible management personnel. b) Establish and implement the rules to prohibit the connection of such devices with company PCs and networks, and the use of the camera function of mobile phones or PDAs, even if bringing in such devices is approved.
2-3-6	Limit the accessibility to Papers (documents and drawings, etc.) and Embodiments (molds, prototypes, etc.) to the personnel who need to know such Confidential Information for business purposes, and implement the anti-theft measures.

(Articles 2-4 to 2-7 shall be applied for Business Partners who share Digitized Information with Panasonic.)

(2-4) Management of user IDs and passwords of the IT system users

2-4-1	Establish rules to manage user IDs for the IT system, and follow all measures in a) to d) below. a) Prohibit sharing of user IDs with other users of the IT system. b) Establish procedures to issue and approve user IDs. c) Immediately delete unused IDs, such as the IDs issued to resigned, retired or transferred staff and the temporary IDs. d) Periodically verify that unmanaged IDs do not exist.
2-4-2	Establish rules to manage passwords for the IT system, and follow all measures in a) to c) below. a) Set a password which cannot easily be guessed by an unauthorized person. b) Change passwords regularly. c) Manage passwords so that they will not be known to others.
2-4-3	Implement access controls for the servers containing Confidential Information, and establish a system to limit the access to only the personnel who need to know the information for business purposes.
2-4-4	Obtain records (logs) of personnel who accessed Confidential Information, and properly store such records (logs) during the period agreed upon with Panasonic.

(2-5) Management of installation/usage/disposal of IT system, such as PCs and servers

2-5-1	Isolate the company's internal network from external networks, including the Internet, with router, firewall, etc.
2-5-2	Establish and implement procedures to introduce and install PCs, PDAs, and servers.
2-5-3	Store Confidential Information on servers. Protect the servers with adequate security measures.
2-5-4	Prohibit the use of privately-owned PCs, PDAs, or storage media for business purposes.
2-5-5	Establish and implement rules for disposing of and recycling PCs, PDAs, servers and storage media, which include the following: • Completely delete data on disks or storage media or physically destruct hardware in order to prevent data recovery.
2-5-6	Install the servers storing Confidential Information in secure places, and follow the procedures a) and b) below. a) Limit the entry to areas where servers are installed only to the personnel who need the access to such areas for business purposes.

	b) Take anti-theft measures for the servers.

(2-6) Countermeasures against malicious programs

2-6-1	Establish rules for countermeasure against malicious programs and computer viruses, and follow all measures in a) to d) below. a) Install anti-virus software of the type and version specified by the responsible management personnel of the IT system. b) Make anti-virus software resident and active at all times on the PCs and keep the PCs defensible against computer viruses. c) Regularly update virus pattern files. d) Scan all stored files regularly.
2-6-2	Establish and implement procedures, including physical measures against virus infection and reporting/notification/responding methods, to minimize the damages caused by computer viruses.
2-6-3	Prohibit the installation and use of file-swapping software, including software which poses high-risks of information leakage, such as Kazaa, LimeWire, and verify regularly that such software programs are not installed.
2-6-4	Prohibit the transmission and sharing of Confidential Information by free e-mail services (Yahoo mail, Gmail, etc.) or data storage services (Google docs, etc.).

(2-7) Implementation of data backups

2-7-1	Review the necessity for and frequency of taking backups together with Panasonic, and if such backups are necessary, establish and implement rules on taking backups of Digitized Information.
2-7-2	Establish rules to store backup data, and properly manage such data in accordance with the confidentiality classification.

(Article 2-8 shall be applied only if Your Company shares Confidential Information with outsourced companies.)

(2-8) Management of outsourced companies which share Confidential Information with (hereinafter “Outsourced Companies”)

2-8-1	Notify Panasonic in writing prior to sharing Confidential Information with Outsourced Companies.

2-8-2	Execute a non-disclosure agreement (or any signed document which contains confidentiality obligation clauses) that includes the provisions for a) to l) below, with Outsourced Companies, and establish and implement rules on how to handle or exchange Confidential Information. a) Confidentiality obligation b) Scope of information subject to non-disclosure c) Period of compliance (including unlimited duration) d) Limitation on the intended use of Confidential Information e) Limitation on the personnel with access to Confidential Information to those who need to know such information for business purposes f) Procedures for the management of Confidential Information g) Restriction on the duplication and copying of Confidential Information h) Rules on return or disposal of Confidential Information at the end of the compliance period i) Procedures for verification on how Confidential Information is stored or handled in Outsourced Companies, such as a hearing or an audit. j) Measures to be taken in case of a breach of the agreement, such as inserting provisions for Your Company's right to seek injunction in the market as well as the compensation for damages. k) Prohibition of re-commissioning to the outsourced companies without Your Company's prior consent l) Prohibition of the use of privately-owned PCs for business purposes
2-8-3	When Digitized Information is sent by e-mail to Outsourced Companies, encrypt the files containing Confidential Information.
2-8-4	Keep records of the exchange of Confidential Information between Your Company and Outsourced Companies and manage such records.
2-8-5	Require Outsourced Companies to obtain from their employees signed agreements that are equivalent to the agreements signed by the employees of Your Company.
2-8-6	Require Outsourced Companies to implement Information Security Management, equivalent to that of Your Company, and verify the implementation status of such periodically.
2-8-7	Require Outsourced Companies to conduct education and training on Information Security for their employees.

(3) Controls for Personnel Security

(3-1) Conducting education and training on Information Security

3-1-1	Regularly provide education and training on Information Security for all employees.

3-1-2	Regularly provide education and training on Information Security for all responsible management personnel.
3-1-3	Conduct a periodical review of all employees on the compliance of Information Security rules by self check, etc. If any non-compliance is found, the responsible management personnel must provide instructions for improvement to such employees.
3-1-4	Conduct education/training on APT attacks for all employees.

(3-2) Obtaining of signed agreement for confidentiality obligation from employees, etc.

3-2-1	Include a provision for confidentiality obligation in the employment regulations, etc., and obtain a signed agreement for confidentiality obligation from each employee.
3-2-2	Obtain signed agreements for confidentiality obligation from temporary staff upon hiring.

(4) Responses to Information Security Incidents

(4-1) Establishment of an organizational structure for incident reports/responses

4-1	Appoint a manager in charge of communication and responses at the occurrence of an incident, and establish the structure for incident reporting, including the measures in a) to c) below. a) Report immediately to the responsible management personnel upon discovery of a problem with Information Security or a possibility of a problem, witnessing an incident, or finding an evidence of such incident. b) If a problem or a possibility of a problem as described above is discovered, report to Panasonic within the time agreed with Panasonic. c) If a device, which contains Panasonic's information, is infected with a virus through an APT attack, report it to Panasonic within the time period agreed with Panasonic.

(4-2) Clarification of procedures for incident responses

4-2	Thoroughly implement throughout Your Company the procedures for an incident response, including all of the measures in a) to f) below. a) Emergency response to grasp the damage and minimize its effects b) Investigation on the cause and tentative measures c) Measures to enable relevant personnel to take defensive actions and responses, including reporting to the relevant third party, in case of information leakage d) Procedures for public statements or reports to the relevant government offices, if necessary

	e) Recording of the background, development and progress of each incident f) Implementation of preventive measures, and building a structure for publicizing and raising awareness internally

* Examples of information security incidents: theft/loss of information (documents, PCs, storage media, Embodiments, etc.), information leakage, erroneous transmission of e-mail/FAX, unauthorized access to information, unauthorized acquisition of information, loss of availability (system failure, data corruption, etc.), loss of integrity (data falsification or deletion), etc.

(5) Implementation of Information Security Management

(5-1) Periodical verification of the implementation of Information Security activities

5-1	Periodically verify the implementation of organizational activities for Information Security.

(5-2) Implementation of activities for improvement based on the verified results

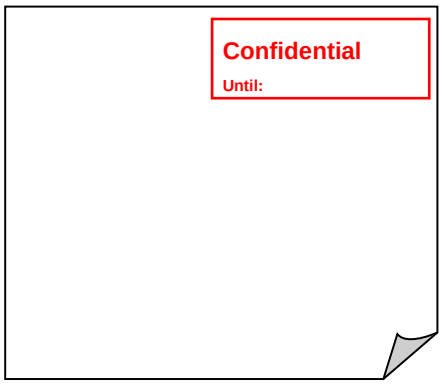
5-2	Develop an improvement plan and take necessary actions for improvements on nonconformity found upon verification.

Supplementary Information

1. These criteria shall be effective as of March 1st, 2019.

2. Method for Panasonic to specify Confidential Information that these criteria are applied to.

<Samples for labeling>



Panasonic specifies Confidential Information in either of the methods 1 to 3 below.

1. Information such as documents, drawings, files, digitized data, etc., marked as “Confidential.”
2. Electronic date with file names as “Confidential – [file name]”, or “C – [file name].”
3. Information specified as Confidential Information by Panasonic by other means.

3. Check Sheet

Your Company is required to implement the self-check of Information Security regularly,

by using “Check Sheet for ISM Criteria for Business Partners,” and report the results when requested by Panasonic.