Information Security Countermeasure Standard for Our Business Partners

December 2017

KUBOTA Corporation

1. Introduction

This Countermeasure Standard shows information security countermeasure items which ask business partners that are shared classified information owned by KUBOTA Corporation and its subsidiaries and affiliates (hereinafter referred to as "Our Company") in promoting CSR management.

Through proper management of classified information, we aim for the continuous and synergetic development of Our Company, business partners and society by achieving stable business continuity.

We would like to take this opportunity to express our gratitude for your cooperation towards our efforts and we ask for your continued understanding and cooperation.

2. Scope of application

Scope of application of this Countermeasure Standard shall be in accordance with the scope of application of "Kubota Group CSR Procurement Guidelines".

3. What is classified information?

Classified information generally means information disclosed by documents, etc. (including data information recorded magnetically or optically) which are agreed to be confidential, or information disclosed orally after notifying its confidentiality.

4. Target

This Countermeasure Standard shall not only include classified information shared with us but shall also include classified information created using that classified information.

In addition, the format of classified information shall not only include paper and electronic media but shall also include intangible assets, such as items (mold, etc.), knowhow and technology which are created by using the classified information.

5. Information Security Countermeasure Standard

It is important to check the countermeasure situation of information security from the four standpoints of "Organization", "Personnel", "Technology" and "Physical environment" to lead to continuous improvement.

The Information Security Countermeasure Standard required for business partners is shown below.

Information Security Countermeasure Standard required for our business partners

[Organizational countermeasure]

Items		Standard
1	Information security management system	The information security management system is established. The responsibilities and roles are clearly defined. They are documented and understood by employees.
2	Information security-related regulations	The information security basic policy and countermeasure standard are prepared and clearly documented and understood by employees.
3	Subcontractor management (recommission)	When you share classified information with a subcontractor, you are imposing the same confidentiality obligation on the subcontractor.
4		When you share classified information with a subcontractor, you are recording and managing acceptance and delivery of such information.
5	Clarification of classified information	Classified information (including reproduction or copy of classified information) is managed using the ledger and is clearly specified as confidential.
6		Classified information is stored by distinguishing it from other information.
7	Classified information take-out management	(1) As a rule, it is prohibited to take classified information outside the company (including transmission of information via a network, such as email). (2) When it is unavoidable to take classified information outside the company for business reasons, the rules for taking out information is formulated including all of the following correspondences. 1) When taking out classified information, manage the information using the ledger after gaining approval from the supervisor. 2) If it is digitalized, take information leakage countermeasures, such as use of encryption. 3) Be careful that classified information is not seen by someone outside the company, and always stay near the information.
8	Transmission of information to the outside of the company	A process to examine and approve information to be transmitted to the outside the company is prescribed.
9	Use of third-party services	A selection standard for using third-party services, such as rental servers and cloud services is stipulated. It is confirmed that the standard is equivalent to or higher than your information security countermeasure standard.
10	Correspondence to information security accidents/ incidents	The correspondence procedure and correspondence framework of information security accidents/incidents, such as virus infection, classified information leakage, and flow-out are clearly defined. They are documented and understood by employees.
11	Audit	An information security audit is being carried out and information security management situation is being checked on a regular basis (once or more per year). Issues found are being adequately improved.

Items		Standard
12		When you share classified information with a subcontractor, you request the subcontractor for information security management at the same level as your company.
13		Field validation is executed by visiting the subcontractor.

[Countermeasure for personnel]

Items		Standard
14	Education/training	Information security education and training are given to for all employees on a regular basis (once or more per year). The attendance is recorded and stored.
15		When you share classified information with a subcontractor, you request the subcontractor for implementation of information security education and training at the same level as your company on a regular basis (once or more per year).
16	Acquisition of confidentiality pledge	An item about confidentiality is added to the company rules and other regulations, and you have your employees sign the confidentiality pledge?
17		When you share classified information with a subcontractor, you request the subcontractor to have their employees sign a confidentiality pledge equivalent to your company.

[Technological countermeasure]

Items		Standard
18	Account and password management	Proper access rights are set for classified information so that the information can only be handled by persons who are required to know the information for business reasons.
19		An account (user IDs for the system and server, etc.) is provided to each individual. The password is long enough (8 digits or more) so that cannot be easily guessed.
20		Rules and procedures for issuance, registration and deletion of an account due to joining, retirement. or relocation of employees and periodical inventory (once or more per year) are clearly specified, documented, and properly operated.
21	Network security	The in-house network is separated from external networks, such as the Internet, by means of network equipment including firewall. Proper access control is implemented so that external networks are prohibited from connecting to the in-house network.
22	Vulnerability countermeasures	The latest security patches are always applied to the OS installed on the PCs, server, smart devices (smart phones and tablets), etc.
23		The latest security patches are always applied to the software installed on the PCs, server, smart devices, etc.
24	Malicious program countermeasures	Anti-virus software is installed on to the PCs, servers, smart devices, etc. and the equipment always uses the latest pattern files (detection and defense rules) for protection.
25		Inspection (full scan) by anti-virus software is executed on a regular basis (once or more per week) for all files that are saved on the PCs, servers, smart devices, etc.

Items		Standard
26		Correspondence procedures for minimizing damages when infected with a virus (initial response, such as disconnection from the network, reporting method, etc.) are clearly defined, documented and understood by employees.
27		The types of software which is prohibited to use from the viewpoint of information leakage risks is clearly specified, documented and understood by employees.
28		You check on a regular basis (everyday) that the software prohibited to use from the viewpoint of information leakage risks is not used.
29		File sharing and exchange software such as Winny, etc. is prohibited to be used.
30	Use of Internet/email	A system that limits access to websites that are irrelevant to work is installed.
31		Use of email addresses or on-line storage services* that are not permitted by the company is prohibited. *File sharing service on the Internet (Google Drive, OneDrive, etc.)
32	Usage limitation of personal devices	Use of personally-owned PCs, smart devices, and personally-owned data storage media (USB) are prohibited. Only the information equipment which is permitted by the company is used.
33	Use of data storage media	Data storage media that is allowed to use for work designated. The usage is managed using the management ledger.
34	Management of classified information	Classified information is being managed only on the specified servers and systems. Proper security management, such as access control, is implemented.
35	Erasure of classified information	When discarding PCs, servers, smart devices, and data storage media, a data erasure tool or other tool to completely erase internal information is used so that data recovery of saved data will not be possible. Or they are destroyed physically.
36		When outsourcing the disposal to a third-party operator, such as an industrial waste disposal operator, a confidentiality agreement is obtained from the third-party operator.
37		It is possible to submit a disposal certificate to Our Company on our request.
38	Log management	The log of access (when, who, what operation executed) to classified information is acquired. It is kept for a period of time you specified.
39	Backup	Backup data of classified information is properly acquired. Proper security management, such as access control is also implemented for the acquired backup data.

[Physical measure]

Items		Standard
40	Management of entering/exiting from rooms	Physical measures, such as locking, for controlling the entrance and exit of people are taken in the location installed with a server or a system in which classified information is saved.
41		The entrance and exit of people to/from the location installed with a server or a system in which classified information is saved is managed using the management ledger.

Items		Standard
42		Necessity and validity of the device brought into the location installed with a server or a system in which classified information is saved are confirmed in advance.
43	Locking control of classified information	Printed classified information (design drawing information, etc.) and items created based on classified information (mold, etc.) are kept in a locked storage so that they can only be handled by persons who are required to know the information for business reasons.

6. Requirements to Our Business Partners

(1) Information security countermeasure and implementation of self-diagnosis

We would like to ask our business partners to implement countermeasures prescribed in this Countermeasure Standard as well as self-diagnosis regarding periodical implementation status (Use the attached "Information Security Countermeasure Check Sheet for Partners"). We also ask our business partners to submit the self-diagnosis result data (Excel file) to us on our request.

In addition, when the countermeasure implementation status of a partner is not at the level prescribed by Our Company regarding this Countermeasure Standard, sharing of classified information with the partner may be limited.

(2) Correspondence to audit

Our Company may execute an audit in order to confirm the countermeasure implementation status. Please cooperate with the audit process when requested by Our Company.

7. Other

This Standard will be reviewed and revised from time to time as a result of change in the circumstances which surround information security, revision of internal regulations, etc.

December 2017, First Version