(Annex 8)

Information Security Standards for Procurement

1 Purpose

Information Security Standards for Procurement (hereinafter referred to as the "Standards") stipulates the countermeasures required by the Bio-oriented Technology Research Advancement Institution (hereinafter referred to as "BRAIN") with the aim of the appropriate management of information that is to be protected by the corporation (hereinafter referred to as "contractor") that undertakes procurement from BRAIN, and the contractor shall implement information security countermeasures in accordance with the Standards.

In the case that information security countermeasures are already being implemented, in line with the Standards, new additions or enhancements shall be implemented as necessary. Also, if there are reasonable grounds for the countermeasures indicated in the Standards, contractor shall be able to receive confirmation of exemption from application from BRAIN.

2 Definitions

In the Standards, the definitions of the terms listed in the following items are as provided in each relevant item.

i. "Information that should be protected" refers to information related to the operations of BRAIN that has not been made public, and of which particularly information that requires thorough information management by the contractor may interfere with the execution of operations in case of leakage of such information to parties other than BRAIN employees
ii. "Documents that should be protected, and others" refers to documents (including portable storage mediums on which data that should be protected are stores), images and objects that belong to information that should be protected.
iii. "Data that should be protected" refers to electronic data belonging to information that should be protected.
iv. "Information security" refers to maintaining the confidentiality, integrity and availability of information that should be protected.
v. "Confidentiality" refers to the characteristics of information, which is only accessible by those who are permitted to have access.
vi. "Integrity" refers to the characteristics of information, which is neither destroyed, falsified, or lost.
vii. "Availability" refers to the characteristics of information, which those who are permitted to access information can access the information when needed without interruption.
viii. "Information security implementation procedures" refers to the stipulated implementation procedures related to information security countermeasures

regarding the received business undertaken by the contractor based on the Standards.

ix. “Information security incidents” refers to incidents such as the leakage, loss or destruction of information that should be protected.

x. “Information security events” refers to a situation in which there is a risk of the violation of information security implementation procedures or a situation that may lead to an information security incident.

xi. “Manager, and others” refers to a manager or a department head who processes the procurement by BRAIN.

xii. “Subcontractor” refers to all companies that are engaged in works related to the accomplishment of the contract (excluding those who have a direct contractual relationship with BRAIN).

xiii. “A third party” refers to all but those who are in a direct contractual relationship with BRAIN as a corporation or an individual, including those who carry out guidance, supervision, business support, advice, or audits, and so on for parties in a direct contractual relationship with BRAIN such as parent companies, sister companies, local subsidiaries, brand licensers, franchises, and consultants.

xiv. “A parent company, and others” refer to a parent company as stipulated in Article 2-4 (2) of the Corporation Law (Act No. 86 of 2005).

xv. “A sister company” refers to more than two subsidiaries which have the same parent company, with the relevant subsidiary being a “wholly-owned subsidiary” as stipulated in Article 847- 2 (2) of the Corporation Law, a “consolidated subsidiary” as stipulated in Article 2-3 (19) of the Ordinance of Company Accounting (Ordinance of the Ministry of Justice No. 13 of 2005) or a “non-consolidated subsidiary” as stipulated in (20) of the same Article.

xvi. “A portable storage medium” refers to portable media or devices that can store information by inserted or connected to a computer or a peripheral device.

xvii. “An information system” refers to a system comprising hardware, software (a collection of programs), a network or a storage medium and that performs business processing.

xviii. “A handling facility” refers to a facility where information that should be protected is handled or stored.

xix. “A protection system” refers to an information system that handles information that should be protected.

xx. “A user” refers to a party that uses the information system.

xxi. “Malicious code” refers to a computer virus or spyware, and others, which is a general term for a program that damages the functions provided by the information system.

xxii. “Transmission” refers to the conveyance of knowledge to another party that is not accompanied by the delivery of a tangible object such as a document.

xxiii. “Delivery” refers to the physical transfer of a tangible object such as a document.

xxiv. “E-mail, and others” refers to the transmission and reception of e-mails, sharing files and the transmission and reception of files.
xxv. “e-Government recommended ciphers, and others” refers to the ciphers, and others” stated on the e- Government recommended ciphers list, or another means of encryption that is as resilient or even more resilient against decipherment than the e-Government recommended ciphers after the evaluation based on the evaluation of e-Government recommended cipher selection.
xxvi. “Encryption” refers to the conversion of information to conceal the content of the information or the existence of the information.
xxvii. “Administrator right” refers to rights conferred for the management of information systems (user registration, removal of registration, and user access rights, etc.).

3 Scope

i. The target information is information that should be protected that is handled by the contractor.
ii. The subjects are all persons in the contractor that contact information that should be protected (including executive employees (including employees of holding companies; same hereinafter), managerial personnel, dispatched personnel, contract employees, part-time workers, temporary workers, and others that meet information that should be protected; hereinafter referred to as “handlers.” In this case, it is irrespective of whether the relevant persons are aware of contacting the information that should be protected or not.

4 Information security implementation procedures

i. The contractor that produces the information security implementation procedures shall produce information security implementation procedures that include the content from 5 to 12, and in so doing or in the case of changes, confirmation shall be received from BRAIN regarding consistency with the Standards
ii. Familiarization of information security implementation procedures
Managers, and others must familiarize all parties (including handlers) that may handle information that should be protected with information security implementation procedures. Also, subcontractors that handle information that should be protected must be familiarized with the procedures.
iii. Review of information security implementation procedures
For the information security implementation procedures to be appropriate, effective, and valid, the contractor must carry out regular reviews, and in the case of any major changes or information security incidents related to information security, reviews must be implemented each time and the information security implementation procedures must be altered as necessary.

5 Organization security

i. Internal organization

A) Responsibilities of managers, and others to information security

Managers, and others shall ceaselessly endeavor to ensure information security in the organization through the clear directionality of information security responsibilities, the specification of involvement by themselves, clear role-division for responsibilities and the approval and so on of information security implementation procedures. And within the organization, regarding all members including executive personnel, managerial personnel and other employees' persons who are not handlers must not meet information that should be protected nor request to subordinates to provide such the information.

B) Division of responsibilities

To clarify the responsibility for all information security related to information that should be protected, the contractor must specify the general responsible personnel related to the general management of information that should be protected, and the responsible manager for each information that should be protected (hereinafter referred to as "administrator").

C) Duty of keeping confidentiality and prohibition of use other than for intended purpose

The contractor shall make a contract or an agreement with handlers stating the duty of keeping confidentiality and prohibition of use other than for intended purpose and must carry out regular reviews, and in the case of any changes to the status of information security or in the case of happening information security incidents, after implementing reviews each time, the requirements must be altered as necessary.

D) Investigation of information security implementation status

The contractor must implement an investigation and store the results regularly and in the case of a major change to the implementation of information security regarding its implementation status. Also, when necessary, corrective measures must be taken.

ii. Subcontractors handling information that should be protected

The contractor, on the occasion of the implementation of the relevant contract, in the case of consigning business to subcontractors handling information that should be protected, must make a contract with the relevant subcontractor for the implementation of information security countermeasures based on the Standards, and, prior to the start of the relevant business, based on the confirmation items stated by BRAIN, must make a report to BRAIN after confirming that information security will be maintained by the subcontractor.

iii. Prohibition of disclosure to a third party

A) Prohibition of disclosure to a third party

The contractor must not disclose or leak information that should be protected to a third party unless the party contracts for the business in which

it handles the relevant information that should be protected. In the case of unavoidable disclosure of information that should be protected to a third party unless the party has been contracts for the business in which it handles the relevant information that should be protected, in advance, based on the confirmation items stipulated by BRAIN, after confirming that information security will be secured in the target for disclosure, the approval of BRAIN must be received in writing.

B) Prohibition of entry into handling facility by third party
The contractor, after clarifying potential risks, must not allow the entry of third parties into the handling facility except in the case of taking countermeasures against such risks.

6 Management of information that should be protected

i. Classification guidelines
The Contractor must state a system of information classification according to which information that should be protected can be classified.

ii. Handling information that should be protected

A) Catalog of information that should be protected
The Contractor must create and maintain a catalog showing the status (storage, location, and others) of information that should be protected.

B) Management policy for handling

(i) The contractor must record any receipt, creation, production, duplication, taking out (including rental), disposal or deletion of the information that should be protected.

(ii) The contractor must not handle information that should be protected on personal information systems or personal portable storage media, if in unavoidable cases, in advance, the permission of BRAIN must be received in writing.

(iii) Unless there are special instructions from BRAIN, the contractor must return, submit, discard, or delete information that should be protected after the end of the contract. However, in the case that there is a need to continue possessing information, a request of consultation can be made to BRAIN with the reason.

C) Safekeeping information that should be protected, and others
The contractor must store information that should be protected in a locked locker, etc., and the key must be managed appropriately. Also, in the case of storing information that should be protected as data that should be protected, it is recommended that encryption is used.

D) Taking out of information that should be protected
The contractor must not take out information that should be protected from the handling facility except when its managers, and others deem that the risk caused by taking out can be avoided.

E) Disposal and deletion of information that should be protected

The contractor shall dispose or delete using a reliable method such as shredding any information that should be protected that has been received, created, produced, or duplicated so that it cannot be retrieved, and shall make a record of that method. The same applies when disposing of portable storage media on which data that should be protected was stored.

F) Specification of corresponding parts

(i) The contractor, in the case of the production, manufacture or duplication of information that should be protected, shall take measures to make specifications, such as underlining or opening and closing sentences using parentheses.

(ii) Until the information is confirmed by BRAIN as information that should not be protected, if the objective material of the contract includes information that should be protected, the contractor must treat as information that should be protected all information collected, organized and created as part of the performance of the contract. However, in the case that it is necessary to remove the specification of information that should be protected, a request of consultation can be made to BRAIN with the reason.

7 Human security

i. Responsibilities of managers, and others

Managers, and others must minimize the scope of designation of handlers of information that should be protected as far as possible, assign persons considered to be appropriate, and must make them observe information security implementation procedures. Also, managers shall not consider a person as relevant one to be appropriate who cannot be legally guaranteed to put into practice the right to refuse in the case that there is a request to act in a way that violates the contract with BRAIN.

ii. Handler's list

The contractor must produce or renew the handlers list (a document that describes name, date of birth, affiliated post, job title, nationality, and other details of handlers; same hereinafter) and must notify and receive consent from BRAIN each time before handling information that should be protected. Also, the contractor must take the same measure for subcontractors and registering handlers in third parties to whom information that should be protected is disclosed.

iii. Responsibilities of handlers

The handler must not disclose information that should be protected to a third party that is known in the implementation of the contract while in office or after retirement (unless the party contracts for the business in which it handles the relevant information that should be protected).

iv. Return of information that should be protected

If a handler no longer needs access to the information that should be protected due to the termination of the handler's employment contract or a change in the content of the contract agreement with the handler, the contractor shall make the handler return/submit the handler's possessing information that should be protected to administrator.

8 Physical and environmental security

i. Handling facility

A) Designation of handling facilities

The Contractor must clarify facilities that handle information that should be protected (limited to be located within Japan.).

B) Physical security limits

The contractor must use physical security limits to protect the boundaries of information that should be protected and protection systems (for example, barriers, card control entry, and manned reception).

C) Physical entry and exit control measures

The contractor must limit entrance to handling facilities to those who are permitted to do so by means of appropriate entry and exit control measures and must record and store the entrance of any third parties to handling facilities.

D) Work at handling facilities

The contractor must ensure confidentiality of work related to information that should be protected. Also, in the case that communications devices (mobile telephones, and others) and recording equipment (voice recorders and digital cameras, and others) is used in the handling facility, the permission of manager, and others must be obtained.

ii. Physical security countermeasures for protection system

A) Protection system installation and protection

The contractor, in the case of installing a protection system, must take measures to install it using a lockable rack, and others or to fix it using wire, and others to protection from unlawful access or theft.

B) Taking out of protection system

The contractor must not take out protection systems from the handling facility except when managers, and others deem that the risk caused by taking out can be avoided.

C) Maintenance and inspection of protection system

The contractor, in the case that a third-party conducts maintenance or inspection of the protection system, must take measures such as ensuring that the information that should be protected cannot be retrieved or taken out, as necessary.

D) Disposal or reuse of protection system

The contractor, in the case of disposing of the protection system, after inspecting that the situation does not allow for the reconstruction of data

that should be protected, and after physically destroying the storage medium, must make a record of so doing. Also, in the case of reuse, it must not be reused if, after inspection, the situation is not such that the data that should be protected cannot be reconstructed.

9 Communication and operations management

i. Operation procedure manual

The contractor must produce and maintain protection system operation procedure manual and must ensure a situation that allows for use by users.

ii. Protection from malicious code

The contractor must protect the protection system from malicious code by using anti-virus software, and others which is updated to the latest status, and by performing a full scan at least once a week. For servers or personal computers (hereinafter referred to as "servers, and others") that have been powered off for one week or more, the relevant measures above-mentioned shall be taken when the power is turned on again.

iii. Protection system backup management

In the case of backing up the protection system to a portable storage medium, the contractor must handle the portable storage medium in line with iv.

iv. Handling of portable storage media

A) Management of portable storage media

The contractor must centrally store a portable storage medium containing data that should be protected in a locked locker, and others, and the key must be managed appropriately. Also, measures must be taken so that the information that should be protected is easily distinguishable from other information in the portable storage medium.

B) Storage on portable storage medium

The contractor must use encryption when storing data that should be protected on a portable storage medium. However, in the case of items to be submitted or presented to BRAIN, the instructions from BRAIN shall be followed.

C) Disposal or reuse of portable storage medium

In the case of disposing of a portable storage medium containing data that should be protected, after inspecting that the situation does not allow for the reconstruction of data that should be protected, and after physically destroying the storage medium, the contractor must make a record of so doing. Also, in the case of reuse, it must not be reused if, after inspection, the situation is not such that the data that should be protected cannot be reconstructed.

v. Information transmission and delivery

A) Transmission of information that should be protected

In the case of transmitting information that should be protected by using communication device (mobile telephone, and others), the contractor must

provide protection from risk as necessary based on the judgment of managers, and others regarding the risks accompanying transmission.

B) Agreement regarding transmission and delivery
In the case of the transmission or delivery of information that should be protected, the contractor must do so only to the party with the contract stating the duty of confidentiality or another agreement.

C) Control measures during delivery
In the case of the delivery of documents that should be protected, and others the contractor must protect against unauthorized access or misuse, and others during delivery.

D) Transmission of data that should be protected
In the case of transmission of data that should be protected, the contractor must protect the data that should be protected by either storing the data that should be protected by using the existing encryption, by using an encryption for the circuit line of the telecommunications carrier, or by using an encryption by e-mail, and others. However, in handling facilities in which it is recognized that there is no risk of leakage, this does not apply in the case of wire transmission.

vi. External connection
In the case of permitting an external connection to the protection system (mobile computing, teleworking, and others), the contractor must perform user authentication and use encryption.

vii. Use of e-Government recommended ciphers, and others
In the case of using encryption, the contractor must use e-Government recommended ciphers, and others. In the case that it is difficult to use e-Government recommended ciphers, and others the information that should be protected must be protected by using some other encryption technology, and others.

viii. Software introduction management
In the case of installing software on the protection system, the contractor must receive a confirmation of the safety of the software in advance from administrator of the system.

ix. Use of system utilities
The contractor must restrict the use of system utilities that are capable of invalidating control by the OS and software on the protection system.

x. Management of technical vulnerability
The contractor must acquire information about technical vulnerability without losing time, and make an appropriate response based on the decision of managers, and others.

xi. Monitoring

A) Log acquisition
The contractor must acquire a log recording access, and others to information that should be protected on the protection system.

B) Log storage
The contractor must store the acquired logs for at least three months from the date of the recording and conduct regular inspections.

C) Log protection
The contractor must protect the log from falsification and unauthorized access.

D) Synchronization of date and time
The contractor must regularly ensure that the date and time of information systems that can access the protection system are synchronized through the protection system and the network.

E) Constant monitoring
In the case that the protection system is not physically or logically disconnected from the internet or information systems (including cloud services, and others) with connection to the internet, the contractor must carry out continuous monitoring.

10 Access control

i. User management

A) User registration management
To permit access to the protection system by handlers and to confer appropriate access rights, the contractor must perform registration as protection system users and eliminate it.

B) Password assignment
In the case of assigning an initial or temporary password for protection system users, the contractor shall assign a password that is not easily guessed and shall assign the password by using a method with consideration for confidentiality. In the case of using or jointly using a stronger secure means (biometrics authentication, and others), the application of this item can be excluded.

C) Management of administrator rights
Administrator rights for the protection system must be kept to the minimum level.

D) Reviewing access rights
The contractor must implement reviews regularly and when needed of the assignment of access rights to users of the protection system.

ii. User responsibilities

A) Use of passwords
The contractor must make users of the protection system set passwords that are not easily guessed and must make them not reuse the same password for multiple devices or services and must make them change it immediately after any leakage. In the case of using or jointly using a stronger secure means (biometrics authentication, and others) of password, the application of this item can be excluded.

B) Countermeasures for unattended protection systems
The contractor shall take measures to ensure confidentiality when the protection system is left unattended situation.

iii. Network access control
A) Restriction of functions
The contractor must provide the usable functions in a restricted manner according to the job description of the users of the protection system.
B) Network connection control
The contractor must protect against the risks associated with connecting the protection system to a shared network (such as the Internet).

iv. Operating system access control
A) Login procedures with consideration for security
The contractor must make the users log on using a security-conscious procedures when their using the protection system.
B) User identification and authentication
The contractor must provide each protection system user with a unique identifier (User ID, Username, and others).
C) Password management system
The protection system must have a function (function to prevent the reuse of passwords, and others) that prevents the unauthorized use of passwords.

11 Management of information security incidents, and others

i. Reporting information security incidents, and others
A) When an information security incident occurs, the contractor must take appropriate measures and must immediately report all the matters able to be grasped, and then promptly report the details to BRAIN.
B) In the cases stated below, the contractor must take appropriate measures and must immediately report all the matters able to be grasped, and then promptly report the details to BRAIN.
(i) In the case that it is recognized the infection by malicious code in or unauthorized access to servers, and others on which information that should be protected is stored.
(ii) In the case that it is recognized the infection by malicious code in or unauthorized access to servers, and others that are connected to the same intranet as servers, and others that store information that should be protected and there is a risk of infection with malicious code in or unauthorized access to servers, and others on which information that should be protected is stored.
C) In the case that there is a suspicion of an information security incident or there is a risk to lead to such an incident, the contractor must take appropriate measures and report the details immediately to BRAIN.
D) In addition to the reports stipulated in A) to C), when there is a report either internally or externally to the contractor regarding concerns about the

possibility that an incident such as the leakage, loss or destruction of information that should be protected has occurred or will occur, the contractor must immediately report all the matters able to be grasped including the relevant possibility or the truth of the concern, and then promptly report the details of fact situation to BRAIN.

ii. Handling to information security incidents, and others

A) Response systems and procedures

The contractor must specify response systems, responsibilities, and procedures to deal with information security incidents, suspected cases, and information security events.

B) Collecting evidence

In the case that an information security incident occurs, or if such is suspected, or in the case of i B) (i), the evidence must be collected and promptly reported to BRAIN.

C) Reflection in information security implement procedures

The contractor must reflect information security incidents, suspected cases, and information security events in revisions, and others to information security implementation procedures, and others.

12 Compliance status, and others.

i. Confirmation of compliance status, and others

A) Confirmation of compliance status

The contractor must confirm the compliance status of information security implementation procedures within the scope of responsibilities of the administrator.

B) Confirmation of technical compliance status

The contractor must confirm the technical compliance status of information security implementation procedures within the scope of responsibilities of the protection system administrator.

ii. Information security record

The contractor, after specifying the storage period (at least 1 year after contract accomplishment) for important records regarding information that should be protected (duplication records, taking out records, audit records, and others), must provide strict protection by means of storage in a locked locker, and others or encryption, and must manage the key appropriately.

iii. Audit tool management

The contractor must restrict the use of tools used for auditing the protection system to the minimum level to prevent abuse.

iv. Inspections by BRAIN

A) Acceptance of inspections

The contractor must accept an inspection regarding information security countermeasures when requested by BRAIN.

B) Cooperation with inspections

In the case that BRAIN conduct inspections, the contractor must provide the necessary cooperation (entrance of staff or persons designated by BRAIN to the handling facility, cooperation in document inspection, and others) in response to the request by BRAIN.