(Exhibit 8)

# Information Security Standards for Procurement

1 Purpose

Information Security Standards for Procurement (hereafter, "the Standards") stipulates the countermeasures required by the Bio-oriented Technology Research Advancement Institution (hereafter, "BRAIN") with the aim of the appropriate management of information that is to be protected by the corporation (hereafter, "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, regarding the countermeasures shown in the Standards, in the case that there are reasonable grounds, confirmation may be received from BRAIN for exemption from application.

2 (Definitions)

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

(1) Information to be protected refers to information related to the operations of BRAIN that has not been made public but needs to be thoroughly managed especially by the Contractor, as the leakage of such information to parties other than BRAIN employees may interfere with the performance of operations.

(2) Documents that are to be protected, etc. refers to documents (including portable storage mediums on which data that is to protected is stores), images and objects that are pertinent to information that is to be protected.

(3) Data that is to be protected refers to electronic data that is pertinent to information that is to be protected.

(4) Information security refers to maintaining the confidentiality, integrity and applicability of information that is to be protected.

(5) Confidentiality refers to the feature of information only being accessible by those who are permitted to have access.

(6) Integrity refers to the feature of information being neither destroyed, falsified or lost.

(7) Applicability refers to the feature of those who are permitted to access information being able to access the information when needed without interruption.

( 8 ) Information security implementation procedures refers to the stipulated implementation procedures related to information security countermeasures in connection to the business undertaken by the Contractor based on the Standards.

( 9 ) Information security incidents refers to incidents such as the leakage, loss or destruction of information that is to be protected.

(10) information security events refers to 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.

(11) Manager, etc. refers to a manager or a department head that processes procurement for BRAIN.

(12) Subcontractors refers to all businesses that engage in work related to the accomplishment of the accomplishment of the contract (excluding those who have a direct contractual relationship with BRAIN).

(13) A third party refers to all persons other than those who are in a direct contractual relationship with BRAIN as a corporation or a natural person, including those that carry out guidance, supervision, business support, advice or audits, etc. for parties in a direct contractual relationship with BRAIN such as parent companies, sister companies, local subsidiaries, brand licensers, franchises, and consultants.

(14) A parent company, etc. refers to a parent company as stipulated in Article 2-4 (2) of the Corporation Law (No. 86, 2005).

(15) A sister company refers to a fellow subsidiary to 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 (No. 13, 2005) or a “non-consolidated subsidiary” as stipulated in (20) of the same Article.

(16) A portable storage medium refers to portable media or devices that are capable of storing information that are inserted or connected to a computer or a peripheral device.

(17) An information system comprises hardware, software (the program as a whole), a network or a storage medium and that performs business processing as a whole.

(18) A handling facility refers to a facility where information that is to be protected is handled or stored.

(19) A protection system refers to an information system that handles information that is to be protected.

(20) A user refers to a party that uses the information system.

(21) Malicious code refers to a computer virus or spyware, etc. that is a general term for

a program that damages the functions provided by the information system.

(22) 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.

(23) Delivery refers to the physical transfer of a tangible object such as a document.

(24) E-mail, etc. refers to the transmission and reception of e-mails, sharing files and the transmission and reception of files.

(25) e-Government recommended ciphers, etc. refers to the ciphers, etc. 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.

(26) Encryption refers to the conversion of information in order to conceal the content of the information or the existence of the information.

(27) Manager right refers to rights conferred for the management of information systems (user registration, removal of registration, and user access rights, etc.).

3 Scope

( 1 ) The target information is information that is to be protected that is handled by the contractor.

( 2 ) The subjects are all persons in the contractor that contact information that is to be protected (personnel that come into contact with information that is to be protected (including employees of member companies; same hereafter) executive employees, dispatch personnel, contract employees, part-time workers, and temporary workers, etc. In this case, it is irrespective of whether the relevant parties are aware that the information that is to be protected. Hereafter, “handlers”.).

4 Information security implementation procedures

( 1 ) 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.

( 2 ) Familiarization of information security implementation procedures

Managers, etc. must familiarize all parties that may handle information that is to be protected with information security implementation procedures (including handlers.). Also, subcontractors that handle information that is to be protected must be familiarized with the procedures.

( 3 ) Review of information security implementation procedures

In order 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

( 1 ) Internal organization

A Responsibilities of managers, etc. related to information security

Managers, etc. shall endeavor to ensure consistency of information security in the organization through the clear directionality of information security responsibilities, the specification of personal involvement, clear role-division for responsibilities and the awareness, etc. of information security implementation procedures, and within the organization, regarding those officers who are not handlers, management staff and other employees as well as all members, persons who are not handlers must not come into contact with information that is to be protected and such information must not be offered to subordinates in the course of work duties, etc.

B Division of responsibilities

In order to clarify the responsibility for all information security related to information that is to be protected, the Contractor must specify the general responsible parties related to the general management of information that is to be protected, and the responsibly manger for each information that is to be protected (hereafter, “manager”.).

C Duty of 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 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 or information security incidents related to information security, 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 in connection to its implementation status. Also, when necessary, corrective measures must be taken.

( 2 ) Subcontractors handling information that is to be protected

With the accomplishment of the contract, the contractor, in the case of consigning the handling of information that is to be protected to subcontractors, 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 duties, 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.

( 3 ) Prohibition of disclosure to a third party

A Prohibition of disclosure to a third party

The contractor must not disclose or leak information that is to be protected to a third party (unless the other party has been contracted to handled the relevant information that is to be protected.). In the case of unavoidable disclosure of information that is to be protected to a third party (unless the other party has been contracted to handled the relevant information that is to be protected), in advance, based on the confirmation items stipulated by BRAIN, after confirming that information security will be maintained by 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 is to be protected

( 1 ) Classification guidelines

The Contractor must state a system of information classification so that there is a clear classification of information that is to be protected.

( 2 ) Handling information that is to be protected

A Catalog of information that is to be protected

The Contractor must create and maintain a catalog showing the status of information that is to be protected (storage location, etc.).

B Management policy for handling

(i) The Contractor must record any receipt, creation, production, duplication, removal (including loans), disposal or deletion of the information that is to be protected.

(ii) The Contractor must not handle information that is to be protected on personal information systems or portable storage media, but, 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 is to be protected after the end of the contract. However, in the case that there is a need to continue storing information, a request for a consultation may be made to BRAIN along with the reason.

C Storage of information that is to be protected, etc.

The Contractor must store information that is to be protected in a locked locker, etc., and the key must be managed appropriately. Also, in the case of storing information that is to be protected as data that is to be protected, it is recommended that encryption is used.

D Removal of information that is to be protected

The contractor must not remove information that is to be protected from the handling facility except when it Managers, etc. deem that the risk caused by removal can be avoided.

E Disposal and deletion of information that is to be protected

The contractor shall dispose or delete using a reliable method such as shredding any information that is to be protected that has been received, produced, manufactured 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 is to be protected was stored.

F Specification of corresponding parts

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

(ii) The Contractor, in the case that the deliverables of the contract include information that is to be protected, with regard to any information that is gathered, organized or produced, etc. in connection to the accomplishment of the contract, must not handle the information as information that is to be protected until is has been confirmed that the information does not fall under the scope of information that is to be protected by BRAIN. However, in the case that it is necessary to remove the specification of information that is to be protected, consultation with BRAIN can be requested along with a statement of the reason.

7 Human security

( 1 ) Managers, etc. responsibilities

Managers, etc. must minimize the scope of designated handlers of information that is to be protected as far as possible, assign persons considered to be appropriate, and must enforce information security implementation procedures. Also, approval must not be given to a person 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.

( 2 ) Designating handlers

The Contractor must produce or renew the registry of handlers (handler's name, date of birth, affiliated post, job title, nationality and other details; Same hereafter), and must notify and receive consent from BRAIN each time before handling information that is to be protected. Also, the Contractor must take the same measure for subcontractors and registering handlers in third parties to whom information that is to be protected is disclosed.

( 3 ) Responsibilities of handlers

The handler must not disclose information that is to be protected to a third party that is known in the accomplishment of the contract while in office or after retirement (unless the other party has been contracted to handled the relevant information that is to be protected.).

( 4 ) Return of information that is to be protected

In the case that the employment contract of the handler ends, or when there is a change to the agreement with the handler, and there is no longer any needs for contact with information that is to be protected, the handler must return stored information that is to be protected to the manager.

8 Physical and environmental security

( 1 ) Handling facility

A Designation of handling facilities

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

B Physical security limits

The Contractor must use physical security limits in order to protect the boundaries of information that is to 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 is to be protected. Also, in the case that communications devices (mobile telephones, etc.) and recording equipment (voice recorders and digital cameras, etc.) is used in the handling facility, the permission of a manager, etc. must be obtained.

(2) 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, etc. or to fix it using wire, etc. in order to protection from unjust access or theft.

B Removal of protection system

The contractor must not remove protection systems from the handling facility except when Managers, etc. deem that the risk caused by removal 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 is to be protected cannot be retrieved or removing it, 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 retrieval of data that is to 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 is to be protected cannot be retrieved.

9 Communication and application management

(1) Operation procedure form

The Contractor must produce and maintain protection system operation procedure forms, and must ensure a situation that allows for use by users.

(2) Protection from malicious code

The Contractor must protect the protection system from malicious code using antivirus software that is updated to the most recent status, and by performing scans at least once a week. These measures shall also be taken when turning on the power

to a server or computer (hereafter, “server, etc.”) that has been turned off for one week or more.

( 3 ) 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 ( 4 ) .

( 4 ) Handling of portable storage media

A Management of portable storage media

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

B Storage on portable storage medium

The Contractor must use encryption when storing data that is to 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 is to be protected, after inspecting that the situation does not allow for the retrieval of data that is to 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 is to be protected cannot be retrieved.

( 5 ) information transmission and delivery

A Transmission of information that is to be protected

In the case of transmitting information that is to be protected using communication device (mobile telephone, etc.), the Contractor must provide protection from risk as necessary based on the judgment of managers, etc. regarding the risks accompanying transmission.

B Agreement regarding transmission and delivery

In the case of the transmission or delivery of information that is to be protected, the Contractor must do so in line with the contract stating the duty of confidentiality or by another agreed means.

C Control measures during delivery

In the case of the delivery of documents that are to be protected, etc. the Contractor must protect against unauthorized access or misuse, etc. during delivery.

D Transmission of data that is to be protected

In the case of transmission of data that is to be protected, the Contractor must protect the data that is to be protected by either storing the data that is to be protected using the existing encryption, using an encryption for the circuit line of the telecommunications carrier, or using an encryption by e-mail, etc. 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.

( 6 ) External connection

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

( 7 ) Use of e-Government recommended ciphers, etc.

In the case of using encryption, the Contractor must use e-Government recommended ciphers, etc. In the case that it is difficult to use e-Government recommended ciphers, etc. the information that is to be protected must be protected by using some other encryption technology, etc.

( 8 ) Software introduction management

In the case of installing software on the protection system, the Contract must receive a confirmation of the safety of the software in advance from the system manager.

( 9 ) Use of system utilities

The Contractor must control the use of system utilities that are capable of invalidating control by the OS and software on the protection system.

(10) 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, etc.

(11) Monitoring

A Log acquisition

The contractor must acquire a log recording access, etc. to information that is to 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 Corresponding date and time

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

E　Continuous monitoring

In the case that the protection system is not physically or logically disconnected from the internet or information systems (cloud services, etc.) that share the same internet point, the contract must carry out continuous monitoring.

10　Access rights

(１) User management

A　User registration management

In order to permit access to the protection system by handlers and to confer appropriate access rights, the Contractor must perform registration and registration cancellation for protection system users.

B　Password assignment

In the case of assigning a short-term or temporary password for protection system users, the Contractor shall assign a password that is not easily guessed, and shall assign the password using a method with consideration for confidentiality. In the case of using or jointly using a more secure means (biometrics authentication, etc.) of password, the adoption of this item may be annulled.

C　Management of manager rights

Manager 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.

(２) User responsibilities

A　Use of passwords

The contractor must set passwords that are not easily guessed to users of the protection system, must not reuse the same password for multiple devices or services, and must change it immediately after any leakage.　In the case of using or jointly using a more secure means (biometrics authentication, etc.) of password, the adoption of this item may be annulled.

B　Countermeasures for unmanned protection systems

In the case of leaving a protection system in an unmanned situation, the contractor must take measures with consideration for confidentiality.

( 3 ) Network access rights

A Restriction of functions

The contractor must restrict the usable functions according to the work duties of the users of the protection system.

B Network connection control

The contractor must protect against risks associated with connections to shared networks (internet, etc.) with the protection system.

( 4 ) Operating system access rights

A Login procedures with consideration for security

In the case of a user using a protection system, the Contractor must ensure login is performed by means of procedures with consideration for security.

B User identification and authentication

The Contractor must provide each protection system user with a unique identifier (User ID, Username, etc.).

C Password management system

The protection system must have a function (function to prevent the reuse of passwords, etc.) that prevents the unauthorized use of passwords.

11 Management of information security incidents, etc.

( 1 ) Reporting information security incidents, etc.

A When an information security incident occurs the Contractor must take appropriate measures and must promptly report all of the known details to BRAIN immediately after they are known.

B In the cases stated below, the Contractor must take appropriate measures and must promptly report all of the details immediately after they are known to BRAIN.

(A) In the case that infection by malicious code or unauthorized access to a server, etc. on which information that is to be protected is stored

(B) In the case that there is the risk of infection by “malicious code” or unauthorized access on a server, etc. that stores information that is to be protected when an infection by “malicious code” or unauthorized access is found on a server, etc. that is connected to the same Internet as the server, etc. that stores information that is to be protected

C In the case that there is the risk of an information security incident or a risk that may 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 is to be protected has occurred or will occur, the Contractor must immediately report the factual details to BRAIN with all content that has been understood including the relevant potentiality and the veracity of the risk.

( 2 ) Responding to information security incidents, etc.

A Response systems and procedures

In the case of information security incidents or if such is suspected, and in order to respond to information security events, the Contractor must specify response systems, responsibilities and procedures.

B Collecting evidence

In the case that an information security incident occurs, or if such is suspected, and in the case of (1) B (a), 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 to information security implementation procedures, etc.

12 Compliance status, etc.

( 1 ) Confirmation of compliance status, etc.

A Confirmation of compliance status

The Contractor must confirm the compliance status of information security implementation procedures within the scope of responsibilities of the manager.

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 manager.

( 2 ) Information security record

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

( 3 ) Audit tool management

The Contractor must restrict the use of tools used for auditing the protection

system to the minimum level in order to prevent misuse.

(４) Audit 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 of an inspection implemented by BRAIN, the Contractor must cooperate as necessary with the request by BRAIN (entrance of staff or persons designated by BRAIN to the handling facility, cooperation in document inspection, etc.).