* The Japanese version is the authoritative version, and this English translation is intended for reference purposes only. Should any discrepancies or doubts arise between the two versions, the Japanese version will prevail.

The University of Tokyo Rules on Measures for Proper Management of Retained Personal Information, etc.

Established on March 17, 2005
Board Resolution
The University of Tokyo Rules No. 333

Chapter 1. General Provisions

(Purpose)

Article 1.

The purpose of these Rules is to protect the rights and interests of individuals while ensuring the proper and smooth operation of affairs and businesses of The University of Tokyo (hereinafter referred to as the "University"), in view of a significant increase in the use of personal information at the University.

(Definitions)

Article 2.

The definitions of the terms used in these Rules shall be as defined by Article 2 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003; hereinafter referred to as the "Incorporated Administrative Agencies Personal Information Protection Act") and Article 2 of the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013; hereinafter referred to as the "Numbers Act").

Chapter 2. Management System

(Senior Protection Manager)

Article 3.

One senior protection manager shall be appointed at the University, and an executive staff designated by the president shall serve as the senior protection manager. The senior protection manager shall take charge of supervising affairs related to the management of retained personal information and Individual Numbers (hereinafter referred to as the "retained personal information, etc.") at the University.

(Organization Senior Protection Managers)

Article 4.

One organization senior protection manager shall be appointed at each organization or any other division (i.e. university academic organizations, university-wide centers, university library systems, research institutions established at the University of Tokyo Institutes for Advanced Study (UTIAS), the Secondary School attached to the Faculty of Education, the University of Tokyo Hospital, Research Hospital, Institute of Medical Science and

divisions; the same shall apply hereinafter), and heads of the respective organizations or other divisions or substitute persons (general managers and the manager of internal audit group in the case of divisions) shall serve as organization senior protection managers. Organization senior protection managers shall take charge of ensuring the proper management of retained personal information, etc. at each organization or any other divisions.

(Protection Managers)

Article 5.

One or more protection managers shall be appointed at each organization or any other division, who shall be designated by each organization senior protection manager. Protection managers shall assist organization senior protection managers and take charge of the proper management of retained personal information, etc. relating to the relevant organizations or other divisions for which they are responsible. When handling retained personal information, etc. on information systems, protection managers shall perform their duties in cooperation with administrators of such information systems.

(Protection Officers)

Article 6.

One or more protection officers shall be appointed at each organization or any other division, who shall be designated by the protection manager of each such organization or any other division. Protection officers shall assist protection managers, and be in charge of affairs related to the management of retained personal information at each organization or any other division.

(Administration Officers)

Article 7.

1. Protection managers shall appoint one or more staff members (hereinafter referred to as the "administration officer") who handle Individual Numbers and specific personal information (hereinafter referred to as "specific personal information, etc.") and specify their duties.
2. Protection managers shall specify the extent to which specific personal information, etc. is to be handled by each administration officer.

(Establishment of Systems for Specific Personal Information, etc.)

Article 8.

Protection managers shall establish the following systems for specific personal information, etc.:

(1) a communication system that allows an administration officer, who has become aware of facts relating to the breach (or signs of the occurrence of a breach) of the provisions of related laws, regulations, rules and the like, to report the matter to the protection manager

(2) a communication system that allows executive, academic and administrative staff members (including dispatched workers; hereinafter referred to as "academic and administrative staff"), who have become aware of the occurrence or signs of occurrences of incidents such as leaks, loss

or damage of specific personal information, etc. (hereinafter referred to as "information leakage, etc."), to report to the protection manager

(3) clarification of the allocation of duties and responsibilities of the respective organizations where specific personal information, etc. is handled by multiple departments, and

(4) a response system when becoming aware of the occurrence or sign of incidents such as information leakage, etc. of specific personal information, etc.

(General Auditor)

Article 9.

One general auditor shall be appointed at the University, and the director of internal audit office shall serve as the general auditor. The general auditor shall take charge of audits of the management status of the retained personal information, etc.

Chapter 3. Education and Training

Article 10.

The senior protection manager shall provide all academic and administrative staff who handle retained personal information, etc. with awareness-related training and other necessary education and training, aiming to deepen their understanding of the handling of retained personal information, etc. and increase awareness about the protection of personal information and specific personal information, etc.

Article 11.

The senior protection manager shall provide all academic and administrative staff engaged in affairs relating to the administration of information systems handling of retained personal information, etc. with the education and training necessary for the administration, operation and formulation of security countermeasures of information systems for the proper management of retained personal information, etc.

Article 12.

The senior protection manager shall provide organization senior protection managers, protection managers, protection officers and administration officers with the education and training for the proper management of retained personal information, etc. at the sites of organizations or other divisions.

Article 13.

Organization senior protection managers and protection managers shall take necessary measures for the proper management of retained personal information, etc. for the benefit of academic and administrative staff of organizations or other divisions including the granting of opportunities to participate in the education and training provided by the senior protection manager.

Chapter 4. Responsibilities of Academic and Administrative Staff

Article 14.

1. Academic and administrative staff must handle retained personal information, etc. in conformity with the purport of the Incorporated Administrative Agencies Personal Information Protection Act and the Numbers Act, and in compliance with the provisions of related laws, regulations, rules and the like, as well as the instructions of the senior protection manager, organization senior protection managers, protection managers, protection officers and administration officers.

2. When becoming aware of the occurrence or sign of an occurrence of an incident such as information leakage, etc. of specific personal information, etc. and when becoming aware of the occurrence or sign of an occurrence that an administration officer is in breach of the related laws, regulations, rules and the like, academic and administrative staff must promptly report the facts thereof to a protection manager.

Chapter 5. Handling of Retained Personal Information, etc.

(Access Restriction)

Article 15.

Protection managers shall, according to the nature of retained personal information, etc. including the confidentiality thereof, limit the academic and administrative staff authorized to access such retained personal information, etc. and the details of such authority to the minimum extent necessary for such academic and administrative staff to perform their duties.

Article 16.

Academic and administrative staff who have no access authority may not access the retained personal information, etc.

Article 17.

Academic and administrative staff may not access the retained personal information, etc. for any purpose other than the business purposes even if he/she has access authority.

(Restriction on Reproduction, etc.)

Article 18.

With respect to the following acts, protection managers shall, according to the nature of the retained personal information, etc. including the confidentiality thereof, limit the cases in which such acts are permitted to be conducted even in cases where academic and administrative staff handle such retained personal information, etc. for business purposes. Academic and administrative staff shall perform the following acts in compliance with the instructions of protection managers:

(1) reproduction of retained personal information, etc.;

(2) transmission of retained personal information, etc.;
(3) sending or taking the media containing retained personal information, etc. outside; and
(4) any other act that is likely to interfere with the proper management of retained personal information, etc.

(Corrections of Errors, etc.)
Article 19.
If academic and administrative staff find errors or other inaccuracies in the content of retained personal information, etc., he/she shall make corrections or other revisions according to the instructions of a protection manager.

(Media Management, etc.)
Article 20.
Academic and administrative staff shall store media containing retained personal information, etc. in the designated place as instructed by a protection manager, and when deemed necessary, store the same under lock and key in a fireproof safe.

(Destruction, etc.)
Article 21.
If any retained personal information, etc. or medium containing retained personal information, etc. (including those built into terminals and servers) becomes redundant, academic and administrative staff shall delete such information or destroy such medium in a manner that renders it impossible to recover or decipher such retained personal information, etc., according to the instructions of a protection manager.

(Restriction on Use of Individual Numbers)
Article 22.
Protection managers shall take measures to limit the use of Individual Numbers to those functions already specified by the Numbers Act.

(Restriction on Request for Provision of Specific Personal Information)
Article 23.
Unless it is necessary in the handling of affairs related to Individual Numbers or unless otherwise set out in the Numbers Act, administrative and academic staff of the University shall not request for provision of Individual Numbers.

(Restriction on Production of Specific Personal Information Files)
Article 24.

Unless it is necessary in the handling of affairs related to Individual Numbers or unless otherwise set out in the Numbers Act, administrative and academic staff of the university shall not produce specific personal information files.

(Restriction on Collection/Storage of Specific Personal Information, etc.)
Article 25.
Administrative and academic staff may not collect or store personal information containing Individual Numbers of other persons except for cases that fall under any of the items of Article 19 of the Numbers Act.

(Clarification of Handling Areas of Specific Personal Information, etc.)
Article 26.
Protection managers shall clarify the areas in which affairs relating to the handling of specific personal information, etc. are to be conducted, and take physical security control measures related thereto.

(Recording of Handling Status of Retained Personal Information, Specific Personal Information Files)
Article 27.
1. Protection managers shall, according to the nature of the retained personal information including the confidentiality thereof, organize ledgers and other documents and record the status of handling, including the use and storage of such retained personal information.
2. Protection managers shall organize the methods used to confirm the handling status of specific personal information files and record the status of handling, including the use and storage of such specific personal information, etc.

Chapter 6. Ensuring Security of Information Systems, etc.

(Access Control)
Article 28.
Protection managers shall take measures necessary for access control, including the setting up of functions to identify the level of authority (hereinafter referred to as the "authentication functions") using passwords and other information (i.e. passwords, IC cards, biological information and the like; the same shall apply hereinafter), according to the nature of retained personal information, etc. including the confidentiality thereof (limited to those handled on information systems; the same shall apply hereinafter in this Chapter (excluding Article 43)).

Article 29.

When taking the measures mentioned in the preceding article, protection managers shall organize the provisions concerning the management of passwords and other information (including the review thereof conducted periodically or as needed) and take measures necessary to prevent passwords and other information from being read, etc.

(Access Records)

Article 30.

Protection managers shall, according to the nature of retained personal information, etc. including the confidentiality thereof, record the status of access to such retained personal information, etc., keep the records thereof (hereinafter referred to as "access records") for a certain period, and take measures necessary to analyze Access Records on a regular basis and from time-to-time as necessary.

Article 31.

Protection managers shall take measures necessary to prevent the alteration, theft or unauthorized deletion of access records.

(Monitoring of Access Status)

Article 32.

Protection managers shall, according to the nature of (including the confidentiality and amount of) retained personal information, etc., take necessary measures for the monitoring of inappropriate access to retained personal information, etc. including setting up a function that displays a warning message when more than a certain amount of information that contains or may possibly contain retained personal information, etc. is downloaded from an information system, with periodic checking of such settings also taking place.

(Setting Up of Administrative Privileges)

Article 33.

Protection managers shall, according to the nature of retained personal information, etc., including the confidentiality thereof, take necessary measures to minimize damage when privileges of authority for information system administrators are stolen, and shall take measures to prevent any internal unauthorized operation or other activities (including the minimizing of such privileges).

(Prevention of Unauthorized Access from Outside)

Article 34.

Protection managers shall take necessary measures to prevent unauthorized access from the outside to information systems handling retained personal information, etc. (including path control via firewall setups).

(Prevention of Information Leakage, etc. by Malicious Programs)

Article 35.
In order to prevent information leakage, etc. of retained personal information, etc. by malicious programs, protection managers shall take necessary measures for the resolution of disclosed vulnerabilities in software and the prevention of infection by detected malicious programs (including keeping all installed software up-to-date).

(Handling of Retained Personal Information, etc. on Information Systems)
Article 36.
When making reproductions or other copies of retained personal information, etc. to perform temporary processing of the data, academic and administrative staff shall limit the copying of retained personal information, etc. to the minimum necessary extent, and promptly delete any information that becomes redundant promptly after the completion of the processing. Protection managers shall perform checks with a focus on the status of implementation (such as deleted statuses) as needed according to the nature of such retained personal information, etc. (including the confidentiality thereof).

(Encryption)
Article 37.
According to the nature of the retained personal information, etc. including the confidentiality thereof, protection managers shall take the measures necessary for encryption. Based on the above, Academic and administrative staff shall properly encrypt the retained personal information, etc. they are handling in accordance with the nature of such retained personal information, etc. including the confidentiality thereof.

(Restriction on Connecting Devices/Media with Recording Functions)
Article 38.
According to the nature of retained personal information, etc. including the confidentiality thereof, protection managers shall take necessary measures to prevent information leakage, etc. of such retained personal information, etc. including the restriction of connecting devices/media with recording functions such as smartphones and USB memory sticks to the information system terminals or other devices (including connecting such devices for updates).

(Limitation of Terminals)
Article 39.
Protection managers shall take necessary measures to limit the terminals that handle retained personal information, etc., according to the nature of such retained personal information, etc. including the confidentiality thereof.

(Preventing Theft of Terminals, etc.)

Article 40

Protection managers shall take necessary measures for the prevention of theft or loss of terminals including fixing terminals or locking offices.

Article 41.

Unless a protection manager deems it necessary, academic and administrative staff must not take any internal terminals to areas outside the organization, or bring in any terminals from outside of the organization.

(Preventing Browsing by Third Party)

Article 42.

When using terminals, academic and administrative staff shall take necessary measures to ensure that retained personal information, etc. cannot be browsed by a third party, including ensuring that they log off from the information systems depending as and when necessary depending on the conditions of use.

(Verification of Entered Information, etc.)

Article 43.

Academic and administrative staff shall, according to the importance of the retained personal information, etc. handled using the information systems, shall compare and verify source documents and the entered details, confirm details of such retained personal information, etc. before and after handling, verify the content thereof using existing retained personal information, etc.

(Backup)

Article 44.

Protection managers shall make backups and take necessary measures to store the data in a separate location according to the importance of the retained personal information, etc.

(Managing the Design Specifications etc. of the Information System)

Article 45.

Protection managers shall take necessary measures for the storage, reproduction, disposal and other arrangements of documentation such as the design specification of the information system and configuration diagrams relating to retained personal information, etc. to prevent them being known by unauthorized persons.

Chapter 7. Managing the Security of the Information System Offices, etc.

(Controlling Entrance and Exit)

Article 46.

Protection managers shall specify the persons authorized to enter an office where devices (including the main server that handles retained personal information, etc.) are installed or other areas (hereinafter referred to as "information system offices, etc."), and take measures including the confirmation of business, recording of instances of entrances and exits, means of identifying external entities, accompaniment of external entities by academic and administrative staff, or their monitoring by monitoring devices, restrictions on bringing in, use and removal from the premises or inspection of external electromagnetic recording media or other media. In addition, in cases where facilities to store media recording retained personal information, etc. are established, protection managers shall take similar measures when deemed necessary.

Article 47.

Protection managers shall, when deemed necessary, take necessary measures including installation of entrance and exit controls by specifying the doorways to the information system offices, etc., and limiting the display of its locations.

Article 48.

Protection managers shall, when deemed necessary, take measures necessary for setting up an authentication mechanism for entrance, and organizing the provisions regarding the management of passwords and other information (including the review of such conducted periodically or as needed), means to prevent passwords and other information from being read, and for conducting other arrangements in relation to the control of entrance to, and exit from the information system offices and its storage facilities.

(Control of Information System Offices, etc.)

Article 49.

In order to prevent illegal intrusion from outside parties, protection managers shall take measures that include the installation of locking units, alarm systems and monitoring devices in the information system offices, etc.

Article 50.

In preparation for disaster and other events, protection managers shall take necessary measures within the information system offices, etc. including measures for earthquake resistance, fire prevention, smoke prevention, water resistance, as well as take measures which include the securing of standby power supplies for devices (including servers) and the prevention of wiring from being damaged.

Chapter 8. Provision of Retained Personal Information, Restrictions on the Provision of Specified Personal Information and Outsourcing, etc.

(Provision of Retained Personal Information)

Article 51.

When providing retained personal information to a person other than the administrative agencies and incorporated administrative agencies and such, pursuant to the provisions of Article 9, paragraph 2, items 3 and 4 of the Incorporated Administrative Agencies Personal Information Protection Act, protection managers shall, as a rule, exchange documents with regard to the purpose of use by a person to which such information is provided, the laws and regulations on which the services using such information are based, scope and matters of records to be used, utilization form, and other matters.

Article 52.

When providing retained personal information to a person other than administrative agencies and incorporated administrative agencies and the like pursuant to the provisions of Article 9, paragraph 2, item 3 and item 4 of the Incorporated Administrative Agencies Personal Information Protection Act, protection managers shall request measures to ensure security, and when deemed necessary, conduct on-site examinations or other inspections either before the data is handed over or as needed, confirm the status of measures taken and record the result thereof, as well as take measures that include requests for improvement.

Article 53.

When providing retained personal information to administrative agencies or incorporated administrative agencies and the like pursuant to the provisions of Article 9, paragraph 2, item 3 of the Incorporated Administrative Agencies Personal Information Protection Act, protection managers shall, when deemed necessary, take measures set forth in the preceding two (2) Articles.

(Restriction on Provision of Specific Personal Information, etc.)

Article 54.

Protection managers may not provide specific personal information, etc. except for cases specified in detail by the Numbers Act.

(Outsourcing, etc.)

Article 55.

1. When outsourcing services related to the handling of retained personal information, protection managers shall take necessary measures so as not to select a person who is incapable of performing proper management of personal information. In addition, the following matters shall be expressly stated in contracts (as well as necessary matters which include those pertaining to the management of persons responsible, and service workers at the

service provider and implementation systems) with inspection of the management status of personal information being confirmed in writing:

(1) obligations relating to personal information such as confidentiality, prohibition of utilization other than for intended purposes;

(2) matters concerning restrictions on subcontracting or terms for subcontracting such as prior approval;

(3) matters concerning restrictions on reproduction or other copies of personal information;

(4) matters concerning response upon the occurrence of an incident of information leakage, etc. of personal information;

(5) matters concerning the deletion of personal information and return of media at the time of termination of outsourcing; and

(6) cancellation of contracts, liability for damages and any other necessary matters where there has been a breach.

2. When outsourcing all or a part of Individual Numbers related affairs, protection managers shall confirm in advance whether or not the service provider will take the measures equivalent to the security control measures to be fulfilled by the University pursuant to the Numbers Act.

Article 56.

1. When outsourcing services relating to the handling of retained personal information, protection managers shall confirm the management status of personal information at the service provider by means of regular inspection and other inspection at least once a year in accordance with the nature of retained personal information to be outsourced, including the confidentiality thereof.

2. When outsourcing all or a part of affairs related to Individual Numbers, protection managers shall exercise necessary and proper supervision to ensure that the service provider takes the measures equivalent to security control measures to be fulfilled by the University.

Article 57.

1. Where the service provider subcontracts services relating to the handling of retained personal information, protection managers shall make the service provider take the measures set forth in Article 55 as well as implement through the service provider or the outsourcing party itself, the measures set forth in Article 56 in accordance with the nature of retained personal information relating to the services to be subcontracted, including the confidentiality thereof. The same shall apply thereafter where the subcontractor re-subcontracts services related to the handling of retained personal information.

2. When the service provider subcontracts all or a part of affairs related to Individual Numbers, protection managers shall determine the approval or disapproval of the subcontracting after confirming that proper security will be ensured with respect to the control of specific personal information handled in connection with affairs related to individual numbers to be outsourced. The same shall apply thereafter in the cases where the subcontractor re-subcontracts.

Article 58.
When using agency workers perform services related to the handling of retained personal information, etc., protection managers shall explicitly state in the contracts matters concerning the handling of personal information including the obligation of confidentiality.

Chapter 9. Response to Security Problems

(Incident Reporting and Measures to Prevent Recurrence)
Article 59.
When becoming aware of an incident that would become a problem in terms of security, such as cases where one becomes aware of the occurrence or sign of an occurrence of incident of information leakage, etc. of retained personal information, etc. and where being aware of a fact or signs pointing to facts that an affairs handling officer is in breach of the provisions of related laws and regulations and rules, academic and administrative staff shall immediately report the facts thereof to the protection manager who manages such retained personal information, etc.

Article 60.
Protection managers shall promptly take measures necessary for the prevention of escalation of damage or restorative actions or take other arrangements, as well as report to organization senior protection managers; provided, however, that protection managers shall immediately take (or cause academic and administrative staff to take) measures that can be taken immediately to prevent escalation of the damage, with such measures including the unplugging of LAN cables of the relevant terminals (or other devices) in which unauthorized access from the outside (or inspection by a malicious program) is suspected.

Article 61.
Organization senior protection managers shall investigate the background of the occurrence of incidents, damage situations and other matters and report the facts thereof to the senior protection manager. However, any incidents deemed to be specifically serious, the protection managers shall immediately report the details thereof and other information relating to such incidents to the senior protection manager.

Article 62.
When receiving a report under the provision of the preceding Article, the senior protection manager shall promptly report the details, background, damage situation, and other information of such incidents to the President in accordance with the nature of such incidents.

Article 63.
The senior protection manager shall promptly provide the relevant ministries and agencies with information including the details, background, and damage situation of an incident in accordance with the nature and other factors relating to the incident.

Article 64.
Protection managers shall analyze the causes leading to the incident and take measures necessary to prevent the recurrence thereof.

(Publication, etc.)
Article 65.
The senior protection manager shall, according to the nature, impact and other factors of an incident, take measures including the publication of facts and measures to prevent recurrence and responses to individuals relevant to retained personal information, etc. involved in such incidents. With respect to the incidents to be publicized, information which includes the details, background, and damage situation of such incidents shall be promptly provided to the relevant ministries and agencies.

Chapter 10. Implementation of Audit and Inspection

(Audits)
Article 66.
The general auditor shall perform an audit (including an external audit; the same shall apply hereinafter) on a regular basis and from time-to-time as needed with respect to the status of management of retained personal information, etc. at the University, including the status of measures set forth in Chapter 2 through Chapter 9, verify the proper management of retained personal information, etc. and report the results thereof to the senior protection manager.

(Inspections)
Article 67.
1. Protection managers shall perform an inspection on a regular basis and from time-to-time as needed with regards to recoding media, processing route, method of storage and other matters of Retained Personal Information, etc. at each organization or any other division, and when deemed necessary, report the result thereof to organization senior protection managers.
2. Any organization senior protection supervisor who received a report of the preceding paragraph must report the important parts of such report to the senior protection manager.

(Evaluations and Reviews)

Article 68.

The senior protection manager and organization senior protection managers shall evaluate the measures for proper management of the retained personal information, etc. in terms of effectiveness or other aspects based on the results of audits or inspections and other factors, and when deemed necessary, take measures including revision thereof.

Chapter 11. Cooperation with Administrative Agencies

Article 69.

The University shall properly manage the personal information held by it based on the "Basic Policy on the Protection of Personal Information" (Cabinet Decision 4 of April 2, 2004), by closely cooperating with relevant ministries and agencies.

Supplementary Provisions

These Rules shall come into force as from April 1, 2005.

Supplementary Provisions

These Rules shall come into force as from January 1, 2011.

Supplementary Provisions

These Rules shall come into force as from April 1, 2015.

Supplementary Provisions

These Rules shall come into force as from November 1, 2015.