Translation Date February 15, 2010
Nagoya University Translated Information Archiving Database (NUTRIAD)
http://nutriad.provost.nagoya-u.ac.jp

Nagoya University Rules on the Protection of Personal Information

Revisions
Rule No. 353 of March 22, 2005
Rule No. 383 of March 22, 2005
Rule No. 20 of September 27, 2005
Rule No. 26 of September 4, 2006
Rule No. 32 of September 21, 2006
Rule No. 34 of October 2, 2006
Rule No. 41 of October 23, 2006
Rule No. 107 of March 28, 2007
Rule No. 117 of March 31, 2008

Contents

Chapter 1 General Provisions

(Purpose)

Article 1 (1) These Rules prescribe matters necessary for the appropriate management of personal information retained by Nagoya University ("the University" or "our University"), for the purpose of the proper and efficient performance of the University's obligations and the protection of individual rights and interests.

(2) The handling of personal information in the University is subject to the provisions of these Rules in addition to the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc. (Act No. 59 of 2003; "the Act") and other relevant legislation.

(Definitions)

Article 2 In these Rules, the terms listed in each of the following items are defined as prescribed in those items:

(i) "Independent administrative agency, etc." means an independent administrative agency prescribed in Article 2, paragraph 1 of the Act on General Rules for Independent Administrative Agencies (Act No. 103 of 1999) or a juridical person listed in the table appended to the Act;

(ii) "Personal information" means information about a living individual which can identify a specific individual by name, date of birth or other description contained in that information (including information that can be cross-checked against other information so as to enable the identification of a specific individual);

(iii) "Retained personal information" means Personal Information created or obtained by an employee (including an executive; the same applies below) of the University in the course of their duties that is held by the University for organizational use by its employees.
Provided that this is limited to Personal Information recorded in official documents provided for in Article 2, paragraph 2 of the Act on Access to Information held by Independent Administrative Agencies etc. (Act No. 140 of 2001);

(iv) "Personal information file" means the collections of information including Retained Personal Information listed below:

(a) A collection of information systematically arranged in such a way that specific Retained Personal Information can be retrieved by a computer in order to accomplish a certain administrative purpose;

(b) In addition to what is listed in (a), a collection of information systematically arranged in such a way that specific Retained Personal Information can be easily retrieved by name, date of birth or other description in order to accomplish a certain administrative purpose;

(v) "Division, etc." means divisions prescribed in the Nagoya University Administrative Organization Rules (Rule No. 31 of 2004), including the administrative divisions prescribed in Article 2, the divisions of the Student Affairs Department prescribed by Article 3 and the administrative departments prescribed by Article 4 (for the School of Medicine and Graduate School of Medicine, the School of Engineering and Graduate School of Engineering, and the University Library, each undergraduate department, graduate school or division).

Chapter 2 Systems for the Protection of Personal Information

(Information Protection Superintendent)
Article 3 (1) The University has one Information Protection Superintendent and this post is filled by a Trustee nominated by the President.
(2) The Information Protection Superintendent oversees work relating to the management of Retained Personal Information in the University.

(Information Protection Managers)
Article 4 (1) Each Division, etc. that handles Retained Personal Information has one Information Protection Manager and this post is filled by the head of the Division, etc. concerned.
(2) The Information Protection Managers in the preceding paragraph are listed in the appended table.
(3) In addition to the preceding paragraph, in cases where Personal Information pertaining to education, research and medical treatment is retained by academic staff members, department heads prescribe separate Information Protection Managers.
(4) Information Protection Managers manage the Retained Personal Information in their respective Divisions, etc. as appropriate.
(5) Information Protection Managers, either periodically or as needed, conduct inspections of the recording media, processing systems and storage methods, etc. for the Retained Personal Information for which they have managerial responsibility, and, when considered necessary, report the results of the inspections to the Information Protection Superintendent.

(Information Protection Officers)
Article 5 (1) Each Division, etc. that handles Retained Personal Information has one or more Information Protection Officers, nominated by the Information Protection Manager in the Division, etc. concerned.
(2) Information Protection Officers assist the Information Protection Manager and perform work concerning the management of Retained Personal Information in their respective Divisions, etc.

(Audit Officer)
Article 6 (1) The University has one Audit Officer, and this post is filled by the Auditor responsible for business audits.
(2) The Audit Officer, either periodically or as needed, conducts audits on the management of Retained Personal Information in the University and reports the results of the audits to the Information Protection Superintendent.

(Committee)
Article 7 (1) The University has a Committee composed of relevant employees for the purposes including decisions and communicating about and coordinating important matters pertaining to the management of Retained Personal Information.
(2) Necessary matters concerning the Committee are prescribed separately.

(Education and Training)
Article 8 (1) The Information Protection Superintendent shall conduct information campaigns and other necessary education and training for employees engaged in the handling of Retained Personal Information in an effort to deepen understanding of the handling of Personal Information and raise awareness concerning the protection of Personal Information.
(2) The Information Protection Superintendent shall conduct necessary education and training on information systems management, operation and security measures for employees engaged in the management of information systems that handle Retained Personal Information, in order to contribute to the appropriate management of that information.
(3) The Information Protection Manager must provide employees of the Division, etc. concerned opportunities to participate in education and training under the preceding two paragraphs, and institute other measures necessary for the purposes of the appropriate management of Retained Personal Information.

Chapter 3 Handling of Retained Personal Information

(Responsibilities of Employees)
Article 9 (1) Employees must handle Retained Personal Information in compliance with the spirit of the Act and the provisions of relevant legislation and these Rules, etc., and in accordance with the directions of the Information Protection Superintendent, Information Protection Managers, and Information Protection Officers.
(2) Employees (including those formerly employed) may not recklessly disclose to a third party the existence or content of Personal Information to which they have become privy in the course of their work, or use such information for improper purposes.

(Restrictions on the Retention of Personal Information)
Article 10 (1) Employees shall limit the retention of Personal Information to the degree necessary for performance of their work, and must specify the purpose for which the information will be used, as far as is possible.
(2) Employees may not retain Personal Information beyond the scope necessary for accomplishing the purpose for which the information will be used ("Purpose of Use") specified under the preceding paragraph.
(3) Employees may not alter a Purpose of Use beyond the scope reasonably considered to have a substantial connection to the Purpose of Use before the alteration.

(Express Statement of Purpose of Use)
Article 11 When obtaining Personal Information in writing (including records made using electronic methods, magnetic methods and other methods imperceptible to other persons) directly from the person who is the subject of that information, employees must expressly state the Purpose of Use to that person in advance, except in the cases prescribed in each item of Article 4 of the Act.

(Proper Acquisition of Information)
Article 12 Employees may not obtain information by deceit or other improper methods.

(Ensuring Accuracy)
Article 13 (1) Employees must endeavor to ensure that Retained Personal Information is consistent with past or present facts, within the scope necessary for accomplishing the Purpose of Use.
(2) Employees must, upon discovering any errors, etc. in the content of Retained Personal Information, make corrections or modifications under the direction of the Information Protection Manager.

(Restrictions on Provision and Use)
Article 14 (1) Employees may not personally use, or provide, Retained Personal Information for any purpose other than the Purpose of Use, except where such use or provision is pursuant to legislation.
(2) Notwithstanding the provisions of the preceding paragraph, employees may personally use, or provide, Retained Personal Information for a purpose other than the Purpose of Use when the Information Protection Manager considers that the personal use, or provision, falls under any of the items of Article 9, paragraph 2 of the Act.
Provided that, this will not apply when it is considered that the personal use, or provision, of Retained Personal Information for a purpose other than the Purpose of Use might unduly infringe the rights and interests of the person concerned or a third party.
(3) The provisions of the preceding paragraph do not prevent the application of other legislation restricting the use or provision of Retained Personal Information.
(4) The Information Protection Superintendent shall, in cases considered particularly necessary for the purpose of protecting individual rights and interests, limit the use of Retained Personal Information within the University, for purposes other than the Purpose of Use, to specific employees.
Article 15 (1) When providing Retained Personal Information, the Information Protection Manager shall, in principle, issue a written statement of matters including the Purpose of Use at the place to which the information is provided, the legislation authorizing the use, the scope and items of the records to be used, and the usage format.
(2) When providing Retained Personal Information, the Information Protection Manager shall demand measures necessary to ensure security, and, if considered necessary, confirm that these measures are in place by conducting inspections, etc. either before provision or as required, record the results of the inspections, and adopt measures such as demanding improvements.
(3) When providing Retained Personal Information to an administrative organ, an Independent Administrative Agency, etc., a local public entity, or a local independent administrative agency pursuant to Article 9, paragraph 2, item (iii) of the Act, the Information Protection Manager shall, if considered necessary, adopt the procedures and measures provided for in the preceding two paragraphs.

(Outsourcing)
Article 16 (1) Where work relating to the handling of Retained Personal Information is outsourced to an external party, necessary measures must be instituted to ensure that the person chosen is not incapable of managing Personal Information appropriately.
(2) When outsourcing work to an external party under the preceding paragraph, the following matters must be stated expressly in the outsourcing contract and in addition, necessary matters including the management systems within the outsourcing provider, such as the persons in charge of the outsourcing and matters concerning inspections of the management of Personal Information must be confirmed in writing:
(i) The duty of confidentiality, etc. in relation to Personal Information;
(ii) Matters concerning restrictions or conditions on subcontracting;
(iii) Matters concerning restrictions on duplication, etc. of Personal Information;
(iv) Matters concerning responses when Personal Information is leaked, etc.;
(v) Matters concerning the deletion of Personal Information and return of media on the termination of the outsourcing;
(vi) Contractual cancellation and other necessary measures in cases of infringement
(3) Where work related to the handling of Retained Personal Information is carried out by temporary workers, the duty of confidentiality and other matters concerning the handling of Personal Information must be expressly stated in the temporary worker dispatch contract.

(Personal Information File Register)
Article 17 (1) When the Information Protection Superintendent takes possession of Personal Information Files, the Information Protection Superintendent shall immediately create and officially announce a register ("Personal Information File Register") as prescribed in Article 11 of the Act.
(2) The Personal Information File Register shall consist of a single register for all Personal Information Files held by the University.
(3) When there is a change to an item to be entered in the Personal Information File Register, the Information Protection Superintendent shall immediately amend the Personal Information File concerned.
(4) When the University no longer retains a Personal Information File entered in the Personal Information File Register or when the number of specified individuals identified by means of Personal Information included in that Personal Information File falls below 1000 persons, the Information Protection Superintendent shall delete the entries relating to the Personal Information File concerned, without delay.
(5) When the Information Protection Superintendent has created the Personal Information File Register, the Information Protection Superintendent shall, without delay, make it available for general perusal in an appropriate place in the University and officially announce it by means such as a statement on the University's website.

(Restrictions on Handling)
Article 18 (1) Information Protection Managers must, in accordance with the nature of Retained

Personal Information, including the degree of confidentiality, restrict the number of employees authorized to handle that Personal Information to the minimum number necessary to accomplish the Purpose of Use.
(2) Employees who are not authorized may not handle Retained Personal Information.
(3) Even employees who are authorized may not handle Retained Personal Information for purposes other than work purposes.

(Restrictions on Duplication)
Article 19 Even where handling Retained Personal Information for work purposes, employees must follow the standards prescribed by and directions of Information Protection Managers when engaging in the following conduct:
(i) Duplication of Retained Personal Information;
(ii) Transmission of Retained Personal Information;
(iii) Sending or removing from University premises media on which Retained Personal Information is recorded;
(iv) Other conduct that might hinder the proper management of Retained Personal Information

(Management of Media)
Article 20 (1) Employees must store media on which Retained Personal Information is recorded in prescribed locations in compliance with the directions of Information Protection Managers, and when considered necessary, use means such as fire resistant safes and locks for storage.
(2) Where Retained Personal Information or media on which Retained Personal Information is recorded (including terminals and servers) is no longer needed, employees must comply with the directions of Information Protection Managers in deleting the Personal Information or destroying the media using a method that makes it impossible to restore or read the Personal Information.

(Recording the Handling of Retained Personal Information)
Article 21. Information Protection Managers must, in accordance with the nature of the Retained Personal Information, including the degree of confidentiality, prepare logbooks, etc. and keep records in relation to the handling of the Personal Information, including its use and storage.
Chapter 4 Ensuring the Security of Information Systems

(Controls on Access)
Article 22 (1) Information Protection Managers must, in accordance with the nature of Retained Personal Information, including the degree of confidentiality (limited to Personal Information handled by information systems; the same applies from the following article through to Article 29), adopt measures necessary to control access, such as the installation of systems for identification of access rights ("ID Systems") using passwords, IC cards, or biometrical data, etc. ("Passwords").
(2) When instituting the measures in the preceding paragraph, Information Protection Managers must establish regulations on the management of Passwords (including their periodical or ad hoc revision), and institute measures necessary to prevent Passwords being read etc.

(Access Records)
Article 23 (1) Information Protection Managers must, in accordance with the nature of the Retained Personal Information, including the degree of confidentiality, create records of the circumstances of access to Retained Personal Information ("Access Records") and store them for a set period of time, as well as instituting measures necessary for the periodical or ad hoc analysis of these access records.
(2) Information Protection Managers must institute measures necessary to prevent falsification, theft and improper deletion of access records.

(Preventing Improper Access)
Article 24 (1) Information Protection Managers must institute measures necessary to prevent improper access by external parties to information systems that handle Retained Personal Information.
(2) Information Protection Managers must institute measures for the prevention of infection by computer viruses etc. to prevent leaks or loss of, or damage to Retained Personal Information.
(3) Information Protection Managers must, in accordance with the nature of the Retained Personal Information, including the degree of confidentiality, institute measures necessary for the encryption of Personal Information.

(Cross-checking of Information Entered)
Article 25 Employees must, in accordance with the degree of importance of the Retained Personal Information concerned, carry out checks including cross-checking information entered against the original source of that information; confirming the content of Retained Personal Information before and after processing; and cross-checking information entered against existing Retained Personal Information.

(Backups)
Article 26 Information Protection Managers must, in accordance with the degree of importance of the Retained Personal Information, create backups and institute measures necessary for decentralized storage.

(Management of Information System Specifications)
Article 27 Information Protection Managers must institute measures necessary for the storage, duplication, and disposal etc. of documents containing specifications and configuration diagrams for information systems relating to Retained Personal Information to ensure that these do not become known to external parties.

(Management of Computer Terminals)
Article 28 (1) Information Protection Managers must, in accordance with the nature of the Retained Personal Information, including the degree of confidentiality, institute measures necessary to restrict

the number of computer terminals used for the processing of such information.
(2) Information Protection Managers must institute measures necessary to prevent theft or loss of computer terminals including securing computer terminals in a fixed location and locking offices.
(3) Employees may not take computer terminals outside the University or bring them in to the university except if Information Protection Managers consider it necessary.
(4) When using computer terminals, employees must institute the necessary measures to prevent perusal of Retained Personal Information by third parties, including making certain to log off from information systems in accordance with usage conditions.

(Management of Access to Information System Areas)
Article 29 (1) Information Protection Managers must prescribe the persons authorized to enter rooms containing core servers and other equipment that handles Retained Personal Information ("Information System Areas"), as well as instituting measures including confirmation of the purpose of entry, the keeping of entry and exit records, the identification of external parties, and the presence of employees when external parties enter the rooms.
Similar measures must also be instituted when considered necessary in relation to facilities established for the storage of media on which Retained Personal Information is recorded ("Storage Facilities").
(2) Information Protection Managers must, when considered necessary, institute measures for simplifying the management of entry and exit to Information System Areas by means including specifying entry and exit points, and limit displays of the location of these areas.
(3) Information Protection Managers must, when considered necessary in the management of Information System Areas and Storage Facilities, establish ID Systems for entry and regulations concerning the management of Passwords (including periodical or ad hoc revision), as well as instituting measures necessary to prevent Passwords being read etc. by third parties.

(Management of Information System Areas)
Article 30 (1) Information Protection Managers must guard against unlawful infiltration by external parties by instituting measures such as the installation of locks, alarms and monitoring devices in Information System Areas.
(2) Information Protection Managers must prepare for disasters, etc. by instituting necessary measures such as earthquake-proofing, fire-proofing, smoke-proofing and waterproofing in Information System Areas, as well as measures such as securing backup power supplies for servers and other equipment and preventing damage to wiring.

Chapter 5 Responding to Problems

(Responding to Security Problems)
Article 31 (1) Where a security-related problem arises, including leaked Retained Personal Information, the employee who becomes aware of the incident must promptly report it to the Information Protection Manager who manages the Personal Information concerned.

(2) The Information Protection Manager must institute necessary measures, including to prevent the damage spreading or to repair the damage, as well as investigate the incident, including the course of events leading to it and the damage, and promptly report the incident to the Information Protection Superintendent.
Provided that, if an incident that is considered particularly serious arises, the Information Protection Manager must report the details of the incident to the Information Protection Superintendent immediately.
(3) When the Information Protection Superintendent has received a report pursuant to the provisions of the preceding paragraph, the Information Protection Superintendent shall report promptly to the President, including on the details of the incident, the course of events leading to it and the damage.
(4) The Information Protection Manager must analyze the causes of the incident and institute measures necessary to prevent its recurrence.

(Public Disclosure)
Article 32 When an incident in the preceding article has arisen, the President shall, in accordance with nature of the incident, including the details and its impact, make the facts surrounding the incident and the steps taken to prevent recurrence public, and institute measures including response to the persons concerned.

(Processing Complaints)
Article 33 The Information Protection Superintendent shall endeavor to process all complaints or opinions concerning the handling of Retained Personal Information in the University appropriately and swiftly.

(Miscellaneous Provisions)
Article 34 Necessary matters concerning Personal Information other than those prescribed in these Rules will be separately prescribed.

Supplementary Provisions
These Rules will come into effect from April 1, 2005.

Supplementary Provisions (Rule No. 353 of March 22, 2005)
These Rules will come into effect from April 1, 2005.

Supplementary Provisions (Rule No. 383 of March 22, 2005)
These Rules will come into effect from April 1, 2005.

(Rule No. 20 of September 27, 2005)
These Rules will come into effect from September 27, 2005 and applicable from July 25, 2005.

(Rule No. 4 of April 18, 2006)

These Rules will come into effect from April 18, 2006 and apply from April 1, 2006.

Supplementary Provisions (Rule No. 26 of September 4, 2006)
These Rules will come into effect from September 4, 2006 and apply from September 1, 2006.
These Rules will come into effect from October 1, 2006.
These Rules will come into effect from October 2, 2006 and apply from October 1, 2006.

Supplementary Provisions (Rule No. 41 of October 23, 2006)
These Rules will come into effect from October 23, 2006

Supplementary Provisions (Rule No. 107 of March 28, 2007)
These Rules will come into effect from April 1, 2007

Supplementary Provisions (Rule No. 117 of March 31, 2008)
These Rules will come into effect from April 1, 2008

Supplementary Provisions (Rule No. 91 of March 30, 2009)
These Rules will come into effect from April 1, 2009

■ The Appended Table (related to Article 4) ■

Reference:
Article-by-Article Commentary on the Nagoya University Rules on the Protection of Personal Information
[See attached]