Authority:

- Approved by the President
- Act on Management of Official Documents, etc. (Document Management Act)
- Act on Access to Information Held by Incorporated Administrative Agencies (Information Access Act)
- Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Personal Information Protection Act)
- School Education Act

Chapter 12. Document and Records Management

12.1. Policy

The OIST Graduate University (the University) is committed to achieving efficient business operations and ensuring accountability to its stakeholders and the general public by managing its documents and records in a systematic and logical manner. All practices and procedures concerning document and record management within the University, including their preparation, preservation, disclosure, and disposal, are to be in accordance with this policy as well as the related laws and regulations. This policy applies to all documents and records – whether electronic or on paper and whether in English or Japanese – prepared and acquired by University officers or employees, and held in the course of their duties for the purpose of organizational use.

In addition, proper management of personal information is a particularly important legal obligation in modern society, and it can be publicly damaging and costly for an organization if it fails in that responsibility. As an institution dealing with a variety of personal information such as information of students (including applicants), alumni, employees, donors, event participants and etc., the University recognizes its social responsibility to use and protect such personal information appropriately and to comply with all relevant laws and regulations.

12.2. General Considerations

12.2.1. Legal Obligations

As a Japanese educational institution established with a special government law and supported by Japanese tax-payers, the University is subject to the laws listed below, which require a higher level of transparency and accountability to the general public than is required of private universities. The University is committed to meeting its responsibilities under these laws.

- Act on Management of Official Documents, etc. (Act No. 66 of

2009) (Document Management Act)
- Act on Access to Information Held by Incorporated Administrative Agencies (Act No.140 of 2001) (Information Access Act)
- Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003) (Personal Information Protection Act)

This chapter itself is subject to the legal disclosure requirement and will be posted on the University's external website.

12.2.2. General Principles

All documents and records related to the business operations of the University, regardless of their contents, must be treated with caution.

12221. In particular, when bringing out the documents and records from the office for business trips or other reasonable purposes, the documents should be treated with utmost care and attention. When an employee uses a portable electronic devise to store documents and records, he/she should make sure that no copies are left in the devise after their use or when sharing such device with other individuals.

12222. When leaving a position at the University, employees must transfer all documents and records that they store to their successor or immediate supervisor.

12.2.3. Electronic Documents and Records

The University is committed to introducing electronic systems in order to conduct business transactions accurately and efficiently. In addition, promotion of paper-less business operations helps the University meet its environmental protection objectives. University officials and employees are expected to prepare and store documents and records electronically whenever it is possible. In principle, internal announcements and notices should be sent via e-mails or posted on the internal portal.

Any electronic document and record, regardless of form, is regarded equally important as paper-based documents under this policy. At the same time, it will require greater attention to protect from the risks particularly associated with electronic documents and records, such as falsification, leakage, and deletion (Refer to 12.3.6.3, 12.3.6.4 of this chapter, and Chapter 17, Information Technology and Security [link: 12.3.6.3, 12.3.6.4 and 17]) .

12.2.4. Documents and Records in Laboratories

Scope of this policy is not limited to the administrative groups/sections of the

University. While flexibility in education and research activities is advocated within the University, all faculty and other employees working in support of the academic and research functions of the University are responsible for following this policy when they prepare, acquire, and/or preserve any of the documents subject to this policy, known as Corporate Documents[link: 12.8.2].

Examples of Corporate Documents prepared or managed in laboratories includes, but is not limited to:

- Purchase requests of research equipment
- Plans and reports about budget execution
- Grant applications
- Records of research evaluations
- Minutes and distributed materials of the Faculty Assembly or other committees

Research data, lab notebooks, research papers, and other similar documents and records that are prepared in research activities and which are not intended for the organizational use of the University are not regarded as Corporate Documents.

12.3. Rules

The University recognizes the value of documenting institutional decisions – not only decisions themselves but also the process of making them – and recording of its business transactions; it also recognizes the importance of preserving these records traceable and available for current business purpose, for external and internal reviews and audits, and for future historical research.

12.3.1. Acquired Corporate Documents

All documents and records – whether electronic or on paper – acquired by University officers and employees during their course of work through business communication with external entities are treated as Corporate Documents. Typical examples include notifications or inquiries from the central and local authorities, business letters from other institutions, and proposals from companies.

Information regarding titles, sender, and destination must be appropriately recorded.

12.3.2. Prepared Corporate Documents

All institutional decisions and business transactions must be documented except for those on trivial matters. Corporate Documents must be prepared at the time of or as soon as practicable after the event to which they relate.

12.3.2.1. Corporate Documents recording institutional decision-making are to certify that the decisions have been made by the individuals with the authority to approve the concerned matters. (Refer to the Chapter 2, Governance and Organization [link:2].)

12.3.2.2. Any such approval should be made in a way in which the authenticity is assured – affixing his/her own seal, writing his/her signature, or recording the approval through the related electronic system – after completing necessary work flows.
The "Guideline for Document-based Approval Process" [link: Main body, Attachment 1] developed and updated by the Chief Operating Officer (COO) will provide standardized formats and procedures to be used.

12.3.3. Principles Applied to Preparation of Corporate Documents

Preparation. The following principles are applied to preparation of any of Corporate Document:

12.3.3.1. Must be Accurate. Any Corporate Document prepared by University officers or employees must provide a correct reflection of what was done, communicated or decided. They must be simple, explicit, and using easy-to-understand words and phrases.

12.3.3.2. Must be Identifiable. Every Corporate Document must be uniquely identified by a document number, the date of preparation, and a title appropriately representing its contents and version information (if the document has been revised or is expected to be revised) based on the identification standard of Corporate Document established and maintained by the COO.

12.3.3.3. Must be Bilingual. Any Corporate Document is to be prepared both in English and Japanese. While the internal official and governing language is English, accurate Japanese translation should be added in side-by-side or other appropriate formats in order to be accountable for the University's business operations and its budget executions to the Japanese funding source, local stakeholders, and the general public in Japan.

12.3.3.3.1. However, in one of the following circumstances, a Corporate Document may be prepared in either English or Japanese and at

least with a translated title. (It is still encouraged to make translation of its summary in the other language.)

- The document is routinely prepared.
- The need for preparation of the document is immediate and urgent.
- It is impractical or significantly inefficient to translate the document.

12.3.4. Classification and Preservation

12.3.4.1. Classification of Corporate Documents

12.3.4.1.1. Any Corporate Document must be annotated with the document title, the date of preparation or acquisition, the preservation periods and the preservation period expiration dates when the documents are prepared or acquired.

12.3.4.1.2. Preservation periods (from "less than one year" to "30 years") is set based on the criteria [link:] established and periodically reviewed by the COO.
The preservation period is calculated from the first day (April 1st) of the following fiscal year (or of the following academic year, if it is deemed appropriate by the department head) when the Corporate Documents were prepared, except for when the preservation period is less than one year, in which case the date of preparation or acquisition is the starting date of calculation.
If there is any specific statutory requirement regarding preservation periods and/or the preservation period expiration dates, such requirement must be met.

12.3.4.2. Corporate Document Files

12.3.4.2.1. Any Corporate Document must be classified based on its content and medium (such as electronic, on paper, etc.) as well as preservation periods, and kept together with closely related Corporate Documents that have the same preservation periods, as a collection of Corporate Documents ("Corporate Document File" or "File.").
When there is no such related Corporate Documents, the concerned Corporate Document may constitute an independent File.

12.3.4.2.2. Any Corporate Document File must be classified systematically and logically based on its content in accordance with the "Classification Standard of Corporate Documents" [link:] developed and periodically reviewed by the COO in consultation with each department head. Each File is given a recognizable title, the preservation periods, and thepreservation period expiration dates.

12.3.4.3. Preservation at Department

12.3.4.3.1. Any Corporate Document File must be stored at the physical or electronic storage space under the control of the department head (Document Management Supervisor) responsible for the File until the preservation period expiration (5 years after the starting date of calculation, if the preservation periods is longer than 5 years.).

12.3.4.3.2. Under supervision of the department heads, the Document Management Administrator(s) (an employee(s) assigned by the department head) is responsible for management of preserved Corporate Documents within the department.

12.3.4.3.3. The Corporate Document Files must be transferred from each Section to the University Archive after the certain period of preservation at the Section. However, if a Section needs to preserve some Corporate Documents Files under the control of the Section for more than 5 years provided that the File contains some Corporate Documents frequently used for daily business, or for other appropriate reasons, the Section shall request for permission to the University Archivist (s) (an employee(s) assigned by the COO).

12.3.4.4. Preservation at the University Archive

12.3.4.4.1. The Corporate Document Files, which were transferred from the Department to the University Archive, must be preserved at the physical or electronic storage space designated to the University Archive until the preservation period expiration dates.

12.3.4.4.2. The Corporate Document kept in the Corporate Document Files preserved by the University Archive is accessible

for the department that originally preserved the File before transfer or any employees permitted by the said department.

12.3.4.4.3. Under supervision of the COO, the University Archivist (s) (an employee(s) assigned by the COO) is responsible for management of preserved Corporate Documents within the University Archive and administrative matters necessary for the operations of the University Archive.

12.3.5. Extension of Preservation Periods, Disposal, and Transfer

12.3.5.1. At a time reasonably before the preservation period expiration, the department heads (the University Archivist when the Corporate Document File is preserved at the University Archive) must propose the action to take upon the preservation period expiration for each File among the following three actions:

- Extend the preservation periods,
- Dispose of the Corporate Documents in the Corporate Document File,
- Transfer the Corporate Documents in the Corporate Document File to the National Archive.

Any such proposal must be made in accordance with the guideline[link :] provided by the COO, and must be approved by the COO (as well as endorsed by the concerned department head when the proposal is made by the University Archivist.).

12.3.5.1.1. When the preservation periods are extended, the length of the extended periods must be specified and informed to the University Archivist (s).

12.3.5.1.2. Any Corporate Document that is relevant to any pending claim, audit, investigation, or disclosure requests must be preserved at least until final resolution of the matter. If there are any concerns or questions, the department in charge of the document must consult with the University Archivist(s).

12.3.5.2. Corporate Documents to be disposed after the preservation period expiration must be disposed by the Document Management Administrator (the University Archivist when the Corporate Document is preserved in the University Archive) promptly after the preservation period expiration. When the said Corporate Documents

contain Non-disclosure Information prescribed by the Information Access Act, those Documents must be shredded or incinerated to ensure that such information will not leak.

12353. The University Archivist (s) must transfer the Corporate Documents in the File to be transferred to the National Archive promptly after the preservation period expiration.

12.3.6. Confidential Documents

Confidential Documents. Employees may have to prepare or acquire Corporate Documents that contain information to be protected by government laws and regulations or the University's policies. Such Corporate Documents must be treated with special care in accordance with the following rules to protect their confidentiality.

12361. Corporate Documents that contain confidential information and that should have only limited access must be designated as Confidential Corporate Documents by the department head. Typical examples of confidential information include, but not limited to:

- Medical records
- Student records
- Personnel and payroll records
- Personal finance information
- Information whose disclosure could damage the competitive position of the University
- Information identified by government laws and regulation to be treated as confidential
- Information provided by a third party under a non-disclosure agreement

In this designation, the criteria for Non-Disclosure Information prescribed in the Information Access Act [link: 12.3.7.3.3] should be taken into consideration.

12362. Any Confidential Document must be identified by being clearly labeled as "Confidential."

12363. Any Confidential Document must be stored separate from other documents and records and in a locked drawer or file cabinet or at other secure places (or electronically locked with passwords). Such documents should not be left lying on desks, workbenches, photocopiers, printers, or any other places where other people easily

access.

12364. Employees who need to copy (either physically or electronically) Confidential Documents as part of their duties must obtain a prior approval from the department head in charge of the document.

12.3.7. Disclosure

12371. Corporate Document File Registry

It is a legal requirement to prepare a Corporate Document File Registry as described in the following paragraphs and to disclose it on the University's external website for convenience of internal and external stakeholders.

12.3.7.1.1. The University Archivist, with supervision by the COO and cooperation from the Document Management Administrators of each department, must prepare an electronic database of the Corporate Document Files ("Corporate Document File Registry" or "Registry.") The Registry must contain the following information:

- Classification
- Title
- Preservation periods
- Preservation period expiration date
- Location
- Medium
- The job title of the department head in charge of the activities during which the Corporate Documents in the File was prepared or acquired.
- Action to be taken upon the preservation period expiration

12.3.7.1.2. The Registry must be updated at least once a year by the University Archivist(s).

12.3.7.1.3. The Registry must be opened to the public on the external website and at the administrative office on the University campus, pursuant to the Document Management Act.

12372. Proactive Disclosure

Any university operating in Japan is required to publish the information

regarding status of educational and research activities, and results of the self and external evaluations, in accordance with the School Education Act (Act No. 26 of 1947).
In addition, the University is responsible for proactively providing the information regarding its organization and activities on its website and through other communication tools to meet the disclosure requirements by the Information Access Act.

12.3.7.2.1. Information to Be Disclosed. The information which must be disclosed on the University website and at the administrative office is listed on the Government Ordinance Concerning the Implementation of The Information Access Act. Such information includes:

- Objectives of the institution and a description of its businesses.
- Information of Officers (including information such as the number, names, titles, term of office, and career background of Officers)
- The number of employees
- Standards for paying compensation and retirement allowances to Officers and employees.
- Latest Business Plan and Business Report
- Latest Balance Sheet, Profit and Loss Statement, and other financial documents
- Rules and procedures regarding contracting
- Latest opinions of Auditors
- Latest reports of a certified public accountant or an auditing firm

The COO is responsible for ensuring that all of the information listed in the ordinance is appropriately disclosed. These documents must be disclosed in Japanese.

12.3.7.2.2. The University conducts a wide range of activities, some of which are subject to information disclosure requirements other than those stated above. In such case, the information must be disclosed in compliance with the applicable laws, regulations and government guidelines. The information must be disclosed by the department in charge of the concerned activities. The status of such disclosure will be monitored by the University Archivist (s).

12373. Disclosure upon Request

Individuals and other entities, regardless of nationality, may have the right to access the Corporate Documents in possession of the University under the conditions prescribed by the Information Access Act. All disclosure requests must be received and processed in accordance with the applicable provisions of the Act.

12.3.7.3.1. All disclosure requests must be in writing. Disclosure Requests will be received and processed by the COO in close cooperation with General Counsel.

12.3.7.3.2. The departments related to the documents pertaining to the Disclosure Requests will be informed about the request by the University Archivist (s) and must submit the concerned Corporate Documents that they store to the University Archivist (s) immediately.

12.3.7.3.3. Any Corporate Document pertaining to the Disclosure Requests must be disclosed to the Disclosure Requester, unless it contains the Non-disclosure Information prescribed by the Article 5th of the Information Access Act [link:] (Japanese website).

If the Corporate Document contains information subject to non-disclosure/confidentiality restrictions, applicability of the Partial Disclosure (Article 6) and the Discretionary Disclosure for Public Interest (Article 7) prescribed by the Act must be examined.

12.3.7.3.4. Any decision concerning disposition of a Disclosure Requests will be proposed by the COO, based on the Review Standard, with consent from General Counsel. The decisions are notified to the Disclosure Requester in the applicable written form.

The Review Standards [link:] for Disclosure Requests will be developed, pursuant to the Administrative Procedure Act (Act No. 88 of 1993), by the COO and made available to the public on the University website.

12.3.7.3.5. The University is required to establish and publish detailed rules and procedures regarding disclosure methods and fees. The COO is responsible for developing and maintaining such rules and procedures in light of practices of similar public institutions

in Japan, and place them on the University website.

12.3.8. Protection of Personal Information

The University's rules of personal information management, as prescribed by the following paragraphs, are intended to ensure that personal information will be appropriately protected.

12.3.8.1. Scope of This Policy. This policy is applied to personal information contained by Corporate Documents, defined by12.8.2 [link: 12.8.2].

12.3.8.2. General Policy. The University will use and hold personal information only when it is necessary for carrying out its businesses and for achieving its missions. Any proposed or intended University use of personal information must be specifically explained to the extent possible at the time of retention.

12.3.8.3. Handling of Personal Information

12.3.8.3.1. Access to personal information. Employees who may have access to personal information must be designated by the department heads and shall be limited in number to the minimum staff necessary. Even designated individuals may access such information only for stated business purposes. Unauthorized access to personal information is strictly prohibited.

12.3.8.3.2. Copy and Distribution. The following actions related to personal information require a prior approval by the department head.

- Copying
- Distribution (electronically and physically)
- Bringing out media containing personal information
- Other actions which could impede the proper management of personal information

12.3.8.3.3. Errors. Errors in personal information should be corrected promptly upon instruction by the department head.

12.3.8.3.4. Store. Any media containing personal information must be stored at the location designated by the department

head and, when deemed necessary, stored in a locked and fireproof safe. (Refer to 12.3.6.3 for electronic records [link: 12.3.6.3].)

12.3.8.3.5. Disposal. When personal information, or media (including those built in a server or terminal) containing personal information, is no longer needed, the department head must instruct the staff (who have been designated by the department head to be responsible for the said information or media) to delete relevant information and/or destroy relevant media in a manner which makes impossible the restoration or deciphering of the personal information.

12.3.8.3.6. Recording. The status of use and hold of personal information within each department must be recorded in writing in a systematic way by the department head.

12.3.8.4. Outsourcing

12.3.8.4.1. Business operations in which personal information is handled must not be outsourced to a party lacking the capacity to appropriately manage personal information. When outsourcing such business operations in which personal information is handled, the departments in charge must take all necessary measures, such as confirming the management structure, etc., to avoid selection of inappropriate or incompetent parties to manage personal information.
Any contracts for outsourcing must be made in accordance with the guideline provided by the COO and separately set forth by the CISO. The Procurement Section [link: 28] is responsible for ensuring that any contracts meet the guideline. The department in charge shall enter into a contract in accordance with the guideline and consult with the Rules and Procedures Section as needed. Especially, any contracts for outsourcing all of or part of operations related to the handling of Specific Persona l Information shall be made in accordance with the "OIST Regulations on Handling Individual Numbers and Specific Personal Information".

12.3.8.4.2. Any contracts for staff from agencies providing temporary staff must include explicit provisions regarding management and handling of personal information,including

confidentiality obligations.

12.3.8.5. IT System and Server Room Security

Most personal information at the University is prepared and held as electronic records. The Chief Information Officer (CIO) [link: 17.4.7], in cooperation with the COO [link: 2.4.6.2], is responsible for ensuring the appropriate protection of personal information in electronic records. The CIO must take necessary actions [link:] in accordance with the guideline published by the government. Such actions include the following:

- Establish internal guidelines for the management of passwords
- Record access to personal information and store such records
- Prevent unauthorized external access to personal information
- Prevent the unauthorized disclosure and destruction of personal information by infection of IT system by computer virus
- Access management of the server room

For additional security matters regarding IT, refer to Chapter 17, Information Technology and Security [link: 17].

12.3.8.6. Unauthorized Disclosure

12.3.8.6.1. Any person who is aware of unauthorized disclosure of personal information or other security problems related to personal information must immediately report to the department head and the CISO.

12.3.8.6.2. Department heads are responsible for taking all necessary measures to prevent any harm/damage from an unauthorized disclosure and for making a report on the incident to the COO and ensuring the CISO has been informed at the time of discovery.

12.3.8.6.3. The CISO is responsible for making a report to the President and analyzing the factors resulting in the incident and recommend necessary measures to prevent further recurrence in collaboration with the CIO and other relevant employees.

12.3.8.6.4. Unauthorized disclosures must be made public if warranted by an examination of the nature and impact of the incident, the measures implemented to prevent reoccurrence, and responses to persons whose personal information was involved.

12.3.8.7. Request for Disclosure, Correction and Suspension of Use.
The Personal Information Protection Act confers a right of access to personal information so that individuals can find out what personal information the University holds about them and check that it is accurate, up to date, and relevant to a function of the University.
All requests for disclosure, correction, and suspension of use are received and processed in accordance with the applicable provisions of the Act.

12.3.8.7.1. The COO is responsible for handling any requests regarding personal information in close cooperation with General Counsel. The requests are handled based on the same procedure specified for the information disclosure requests[link: 12.3.7.3].

The Review Standard for Personal Information Disclosure [link:]
The Detailed Rules and Procedures regarding Personal Information Disclosure Methods and Fees [link:]

12.3.8.8. Handling of Specific Personal Information
Handlings of Specific Personal Information are stipulated in "OIST Regulations on Handling Individual Numbers and Specific Personal Information."

12.3.8.9 It is designated by The Personal Information Protection Act that the University may prepare and provide the Incorporated Administrative Agencies' De-identified Information. The Vice President for Administrative Compliance regulate separately how to handle the ""De-identified Information" by the" Regulations for handling of De-identified Information[link:]."

12.3.9. Training

The University Archivist (s), with cooperation from the Training and Education Section must provide training to University employees as necessary to ensure they obtain (or improve) the knowledge and skills required for conducting proper and effective document management, including protection of personal information, in conformance with this policy.

12.3.10. Internal Auditing

The Auditing Manager appointed by the COO will conduct periodic inspections and audits of the status of implementation of this policy and make necessary reports to the COO. The COO will take necessary actions to maintain and improve a robust system for protection of information as required by this policy.

12.3.11. Transition from OIST Promotion Corporation

All Corporate Documents held by the OIST Promotion Corporation at the time of transition to the OIST School Corporation (OIST SC) must be transferred to the OIST SC and managed in accordance with this policy.

12.4. Responsibilities

12.4.1. Officers and Employees

All University officers and employees must recognize the importance of appropriate document and record management, including information disclosure and protection of personal information. They are responsible for managing Corporate Documents, including those with personal information, appropriately by following the instructions from their immediate supervisors and department heads and complying with the related laws and regulations as well as this policy.

12.4.2. COO

The COO is responsible for general administration of this policy within the University (Executive Supervisor of Document Management), including:
General

- Maintaining this policy and developing necessary guidelines to implement this policy,
- Appointing an Auditing Manager from among the employees in the COO and having the Auditing Manager inspect and audit the status of management of Corporate Documents and personal information within the University,
- Providing necessary supervision, training and guidance to University employees, and
- Making necessary written reports to the Prime Minister or other relevant ministers, pursuant to the related laws and regulations.

Document Management

- Preparing and updating the Corporate Document File Registry,
- Operating the University Archive, and
- Taking necessary actions to transfer Corporate Documents to the

National Archive.

Information Disclosure

- Receiving and processing of requests for information disclosure, and making decisions whether or not to accept those requests, and communicating with Disclosure Requesters.
- Establishing and publishing the review standards for the requests and the detailed rules and procedures regarding disclosure methods and fees.

Protection of Personal Information

- Facilitating the internal communication and coordination necessary to implement this policy and to determine important matters related to the protection of personal information. This includes organizing and chairing a committee consisting of the following members as necessary:
  - Chief Information Officer
  - General Counsel
  - Dean of the Graduate School
  - Vice President for Human Resource
  - Any other employees related to the matter to discuss
- Receiving and processing of requests for disclosure, correction and suspension of use of personal information, and communicating with Disclosure Requesters.
- Establishing and publishing the review standards for the requests of personal information and the detailed rules and procedures regarding disclosure methods and fees.

12.4.3. Department Heads

Each department head is responsible for implementation of this policy within the department in charge, including but not limited to the following:

Document Management

- Preparing and updating the Files for Corporate Documents prepared or acquired within the department,
- Taking necessary actions to transferring Corporate Documents to the University Archive or to dispose Corporate Document after the departmental preservation period expiration dates,
- Appointing a Document Management Administrator(s) and having the Administrator(s) carry out necessary tasks to follow this policy, and
- Review annually the status of document and record management within the department and report the results to the COO.

Information Disclosure

- Submit the Corporate Documents pertaining to the Disclosure Requests which are preserved in the department to the COO and provide necessary cooperation to handle Disclosure Requests.

Protection of Personal Information

- Designate staff members to handle personal information within the department,
- Provide necessary guidance and supervision regarding the protection of personal information within the department, and
- Submit the Corporate Documents containing personal information subject to a Disclosure Requests, correction or suspension of use, which are preserved in the department to the COO and provide necessary cooperation to handle the requests.

If a department head delegates the duties and authority to his/her staff, the department head must inform the COO of such delegation.

12.4.4. Document Management Administrator

Document Management Administrator is responsible for managing the Corporate Documents stored in the departments under the supervision of the department head.

12.4.5. University Archivist

University Archivist is responsible for managing the Corporate Documents preserved in the University Archive and preparing the Corporate Document File Registry under the supervision of the COO.

12.4.6. Chief Information Officer

Chief Information Officer is responsible for take necessary actions, in cooperation with the COO, to ensure that electronic records containing personal information is appropriately managed and protected.

12.5. Procedures

12.5.1. How to classify Corporate Documents [link:]

12.5.2. How to access the Corporate Documents preserved at the University Archive

12.6. Forms

12.6.1. Corporate Document Disclosure Request Form[link:]

12.6.2. Personal Information Disclosure Request Form [link:]

12.6.3. Personal Information Correction Request Form [link:]

12.6.4. Personal Information Suspension Request Form [link:]

12.7. Contacts

12.7.1. Policy Owner

COO

12.7.2. Other Contacts

University Archivist (Manager, Rules and Procedures Section)
Chief Information Officer
Chief Information Security Officer

12.8. Definitions

12.8.1. Personal Information

Personal information is information about a living individual, which can identify the specific individual by name, date of birth or other description contained in such information (including information that can be compared with other information and thereby identify the specific individual).

12.8.2. Corporate Document

Corporate Document is a document and record, including any graphics and electromagnetic record (referring to any record created in electronic, magnetic, or any other form that cannot be read without electronic assistance) that is prepared or acquired by University officers or employees and held by the University for organizational use.

Research data, lab notebooks, research papers, and other similar documents and records that are prepared in research activities and which are not intended for the organizational use of the University are not regarded as Corporate Documents.

The definition of Corporate Documents also excludes any official gazettes, white papers, newspapers, magazines, publications, or other materials that are published, and/or are sold, to a large numbers of unspecified persons.

12.8.3. Department

Departments are the basic business unit under the implementation of this policy.

12.8.4. National Archive

National Archive is an archive established by the Independent Administrative Institution National Archives of Japan.

12.8.5. Officers

Officers are: the Chief Executive Officer, Vice Executive Officer, Members of the Board of Governors, and Auditors.

12.8.6. Review Standards

The review standards are standards provide criteria for judgments on whether requests or applications are to be accepted or not, based on the provisions of related laws and regulations.