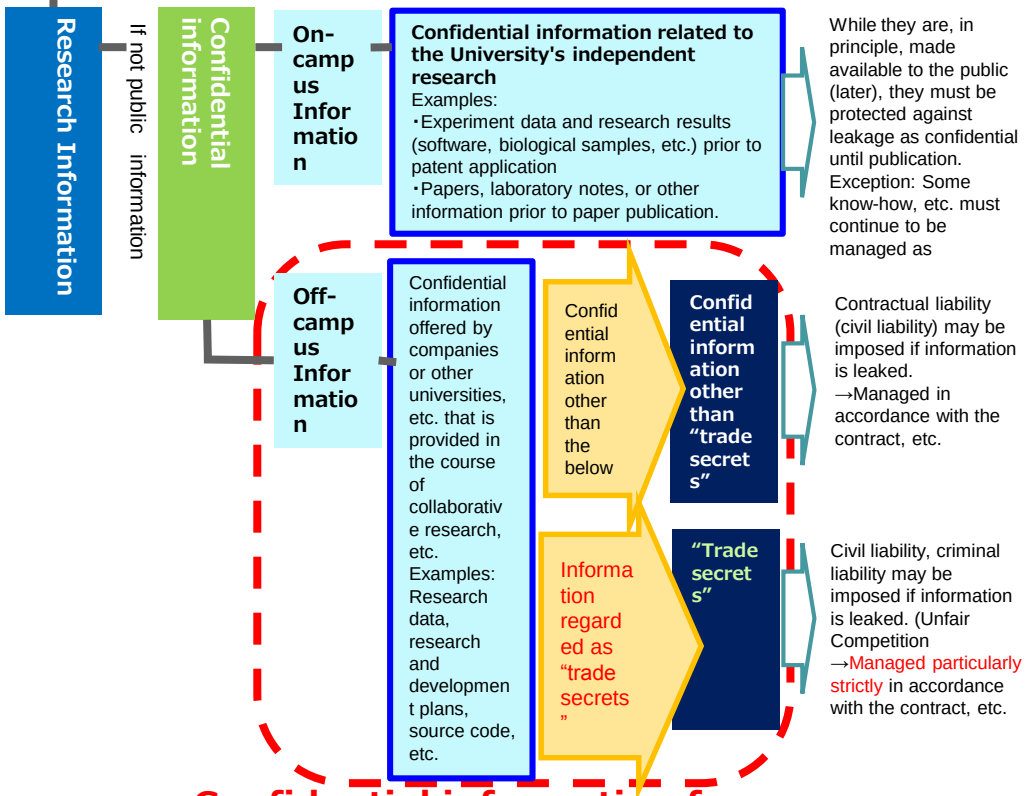
Confidential Information Management for Industry-Academia Collaborations

Academic Research and Industry-Academia-Government Collaboration Administration Office (AR&IAGC)

Importance of the Confidential Information Management in the University

●Public Information, etc. (Not Confidential)

(1) Information which has already been made known to the public (patent applications or papers that have been published).
(2) Information which has already been made known to the public when disclosed by companies, etc.
(3) Information for which it can be proven that the University developed or acquired it on its own.
(4) Information for which the University has obtained written consent from the other party in advance of the disclosure.



Confidential information from companies must be given sufficient attention!!

In cases like these, you must pay attention to the management of confidential information.

●When confidential information is obtained and a confidential information agreement is entered into while meeting with a company or other institution.

●When research data, research and development plans, or other information from companies is received during collaborative research with the companies.

●When having students participate in collaborative research with companies.

♦ If confidential information is leaked…

・Collaborative research partners may file lawsuits

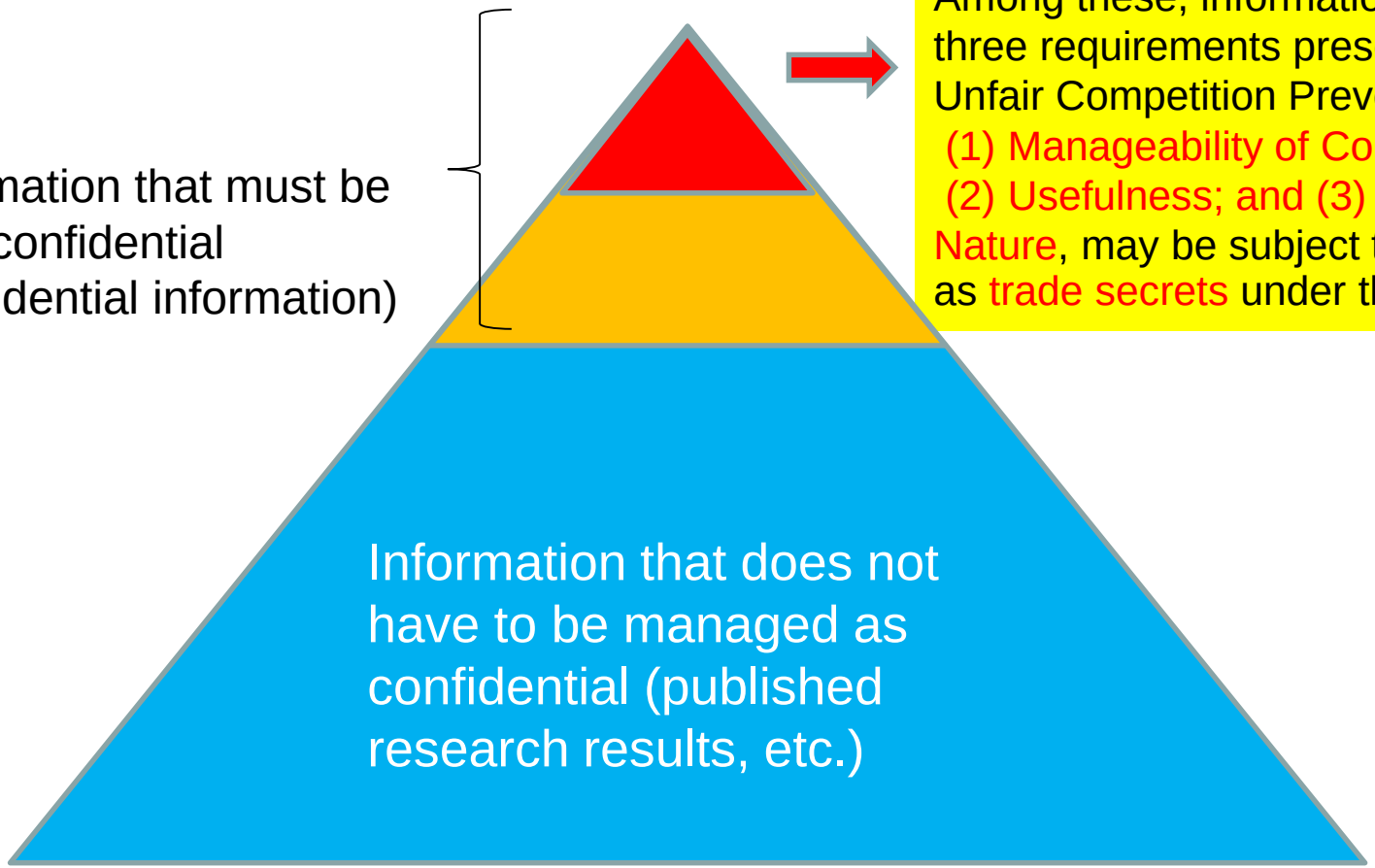
・Social criticism may arise and credibility may be destroyed

The trust of collaborative research partners, etc. may be lost.
→Such an occurrence will greatly impede future collaborative research efforts.

Relationship Between Confidential Information and Trade Secrets

Research Information at the University

Information that must be kept confidential (confidential information)



Among these, information meeting all three requirements prescribed in the Unfair Competition Prevention Act:
(1) Manageability of Confidentiality;
(2) Usefulness; and (3) Non-Public Nature, may be subject to legal protection as trade secrets under the Act.

Concerning Confidential Information, What is a "Trade Secret"?

"Trade secrets" are practical technological information and management information from which the rights holders may obtain economic profit, that have not been made available to the public and for which measures have been taken in order to keep confidential. The following three requirements have been defined in the Unfair Competition Prevention Act.

Manageability of Confidential Information: Persons who may access the information must be limited, and some measures must be taken so that persons who access the information are aware that the information they have accessed is confidential.

(Examples) ・Information recorded in documents or in data on digital media, the confidentiality of which is labeled.
・Information disclosed orally or visually, explicitly stated as being confidential.

Usefulness: Information should be objectively useful to business activities, such as production, sales, or research and development.

(Notice) This applies not only to information directly used for business activities, but also to information having indirect value.
(Examples) Experiment data prior to patent application, information on matters related to new discoveries, personal information, customer data, company development plans, etc.

Non-public Nature: Information that is not generally known to or cannot be easily known to the public under the information holders' management, by means such as the information is not described in the publications.

(Notice) This does not necessarily conform to the interpretation of "Publicly Known Inventions" (Article 29 of the Patent Act) in judging the novelty of an invention.

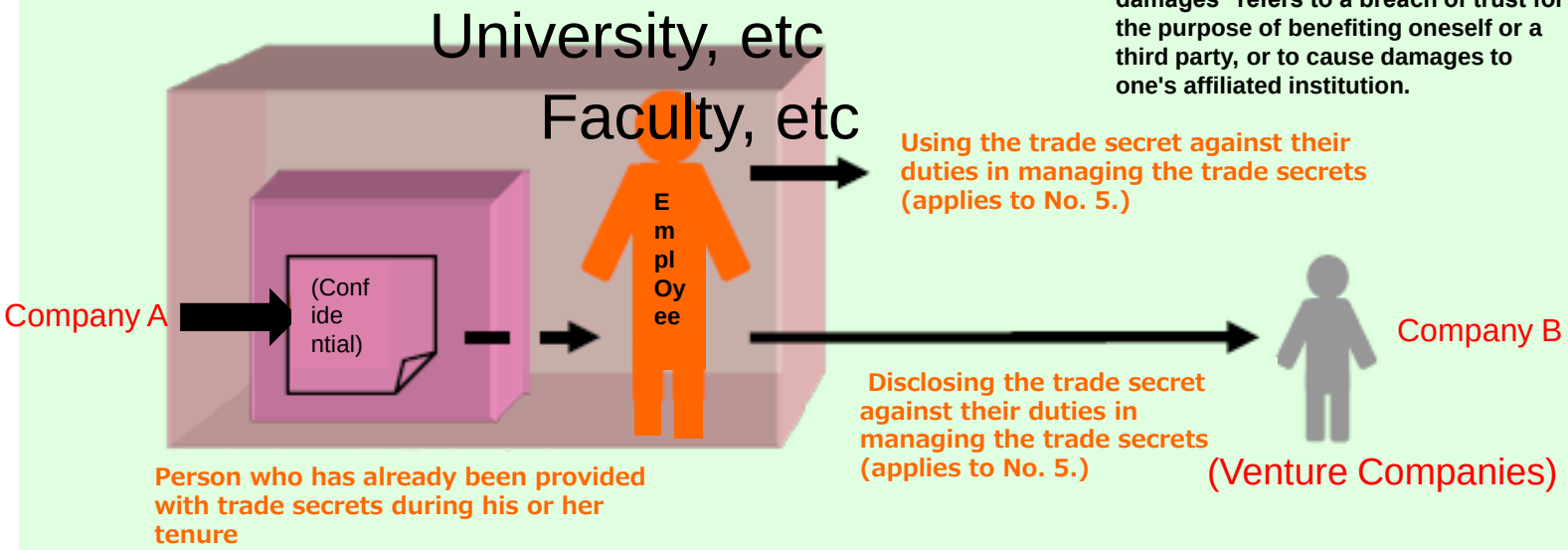
A Case of Confidential Information Leakage

The case to requiring the most attention at the University

The pattern by which persons who have been rightfully provided with a trade secret commit an act of betrayal

(No. 5)Behavior through which current executives or employees who have been entrusted with trade secrets by the owners of the secrets use or disclose the secrets for the purpose of profit-making or causing damages*, against their duties in managing the trade secrets.

※)*"Profit-making or causing damages" refers to a breach of trust for the purpose of benefiting oneself or a third party, or to cause damages to one's affiliated institution.



Persons who have committed the acts of betrayal: "Prison sentence of up to 10 years, and/or a fine of up to 20 million yen (30 million for international leaks) (10 million prior to revision)."

Affiliated Corporation: "A fine of up to 500 million yen (one billion for international leaks) (300 million prior to revision)."

Source: Intellectual Property Policy Office, Ministry of Economy, Trade and Industry, "Unfair Competition Prevention Act 2015"

Examples of Confidential Information Obtained from Companies

Information that possibly falls into trade secrets

Information from companies

"Intellectual property constituting the company's strength"	"Information assets constituting the company's strength"
Technology/know-how used to create their unique products, etc.	・Information related to manufacturing processes and arrangements ・Information related to research and development (technological development, test records, etc.) ・Product specifications (construction, components description, specifications, etc.) ・Information related to proprietary technology ・Information related to factory equipment and layouts ・Information related to manufacturing partners and subcontractors
Products backed by trust based on product quality, mid- and long-term stable business presence, mid- and long-term trade relationships, etc. / company's brand strength	・Information related to primary retailers ・Information related to market trend analysis ・Business logs (visit history, reports, etc.) ・Amount or rate of profits from products, goods, and services ・Information related to suppliers, retailers, items, their quantity and price, etc. ・Information related to retail partners (agencies, franchises, etc.) ・Information related to competitors or competition analysis (trends, selling prices, etc.) ・Sales documents (estimates, presentation materials, etc.)
The business strength to provide products, etc. which meet customer needs	・Materials related to meetings with customers ・Materials and information obtained from customers ・Information related to and details of contracts entered into with customers ・List of customers' information (companies or individuals) and information related to their representatives ・Documents related to claims from customers ・Information and history of selling or providing products, goods, and services associated with each customer ・Information related to customers' management plans, etc.
Highly skilled employees	Information related to the education and continued development of technicians (training programs, materials, etc.)

Construction of a System for Top Management

Nagoya University has been selected for participation in the risk management model project of the Ministry of Education, Culture, Sports, Science and Technology of Japan (MEXT), and thus the following management systems have been constructed in order to prevent the leakage of technology.

Approved by the Executive Council, Reported at the Deans & Directors Committee

◆ **Established, Formulated, and Constructed Items:**

- **Policies and guidelines** — **Established**
- **Process for classifying confidential information into appropriate level** — **Established**
- **Methods for level management according to the level of risk** — **Established**
- **Informed consent requirements for students** — **Formulated**
  Process for obtaining informed consent — **Established**
- **University-wide confidential information management system** — **Constructed**

◆ **Education and Awareness**

- **Holding of a briefing for awareness activities** → Raising of awareness among researchers and administrative staff, etc.
- **Holding of research meetings on and off campus** → Cultivation of personnel in charge of risk management.
- **Tools to increase awareness (offer the e-learning course)**→ Information sharing and accumulation of examples
- **Establishment of a one-stop consultation counter** → Practical and efficient confidential information management system

- **Information sharing among NU MIRAI Working Group, departments, and executives**

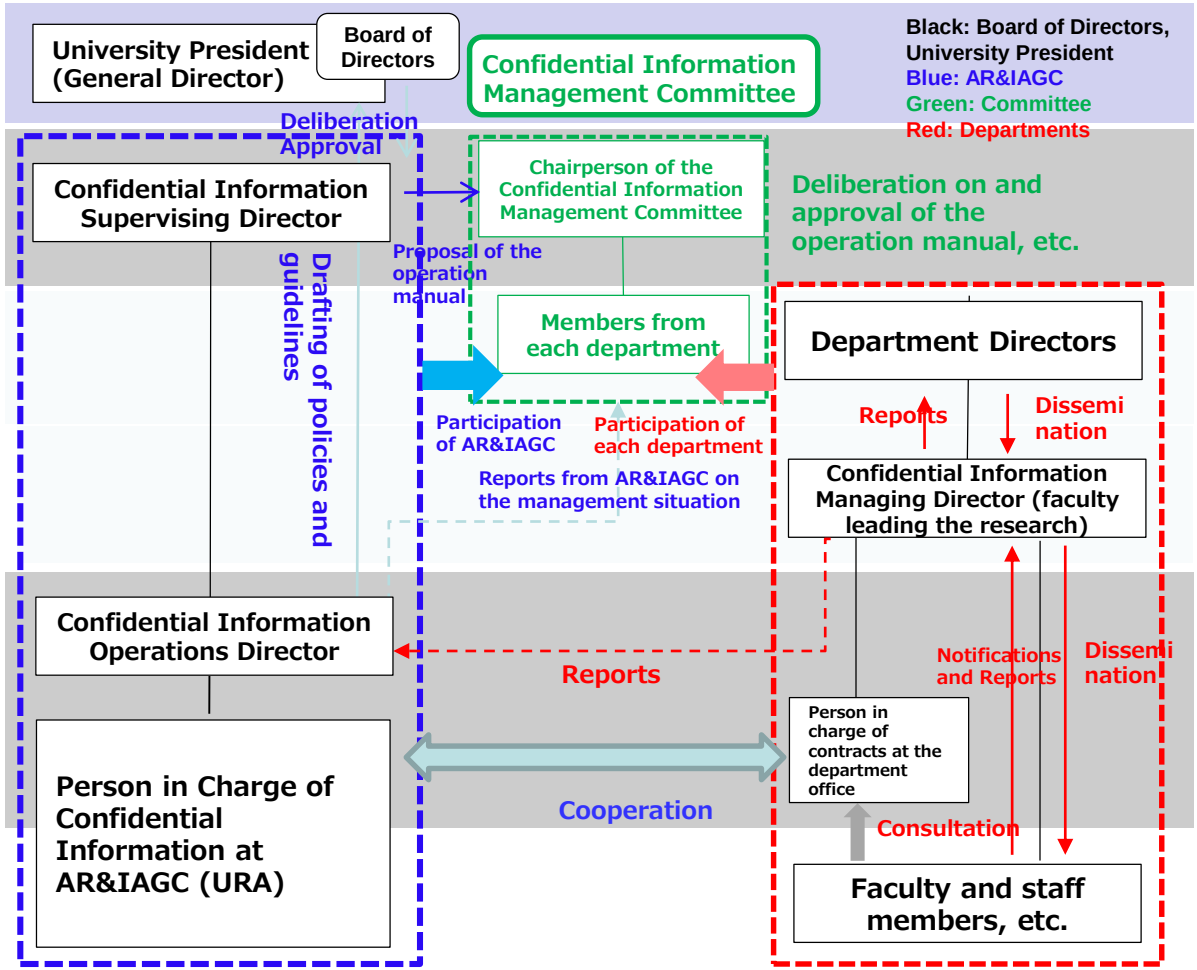
→ **Transfer of the information to top management consisting of the president and top executives**

Nagoya University's Confidential Information Management Policy for Industry-Academia Collaborations

Purpose	With the enforcement of the revised Unfair Competition Prevention Act (Act No. 47 of 2015), corporations in addition to individuals, such as faculty and staff members, may now be subject to criminal penalties for behavior in violation of the act relating to confidential information kept at universities. In the event that inappropriate management conditions for research information are discovered at Nagoya University (hereinafter referred to as "the University"), it is predicted that the University's social reputation would be greatly affected. Accordingly, the University shall manage any important knowledge obtained from companies, etc. through industry-academia collaboration activities as confidential information (hereinafter referred to as "confidential information") in order to protect faculty, staff members, students, etc. from violating any laws, work regulations, or other rules in the event of a leak, whether intentional or accidental. Therefore, remaining grounded in its public role as a contributor to education and research, the University is engaged in the systematic management of confidential information so that companies, etc. can provide their important knowledge without worry, thereby enabling researchers to produce the best results from their collaborative research endeavors, etc. Moreover, with the aim of further promoting industry-academia collaboration activities and contributions to society, the University hereby establish the Confidential Information Management Policy for Industry-Academia Collaborations to clarify the basic concepts of its confidential information management system.
Persons Subject to the Policy and Its Scope	(1) Faculty and staff members, etc., and students shall be subject to this policy. "Faculty and staff members, etc." refers to faculty, staff members, or researchers of the University, or other persons employed or bestowed with a job title by the University; they are separately defined in the Confidential Information Management Guidelines for Industry-Academia Collaborations (hereinafter referred to as "the Guidelines".) "Students" refers to those students who have participated in collaborative research with companies and obtained or are expected to obtain confidential information (limited to students 20 years of age or older.) (2) The applicable scope of this policy is as prescribed below: However, confidential information including personal information that is related to clinical research, etc. is not included in this policy's applicable scope. Collaborative research, etc. limited to collaborations with other universities or public organizations is also not included. (i) Confidential information obtained from the other party during collaborative research, etc. (including the non-disclosure agreement preceding the collaborative research.) (ii) Collaborative research contracts entered into for collaborative research, etc. (limited to information set to be treated as "confidential".) (iii) Know-how generated during collaborative research, etc., in which confidential information obtained from companies is included, and its contents and attribution are designated. (3) This policy shall carefully and appropriately respond to requests for disclosure in accordance with the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc.

Management System and Administrative Roles for Confidential Information Management at Nagoya University

Operational Structure for Confidential Information Management



Academic Research and Industry-Academia-Government Collaboration Administration Office (AR&IAGC)

Each department, etc.

Management Committee

- Deliberate on and establish an operation manual and other operational rules.
- Receive reports on the management situations of each department from AR&IAGC.

Each Department, etc.

- Establish operational rules for confidential information management in each department.
- Designate and manage confidential information.
  (Level 1, Level 2)
- Disseminate information on confidential information management.

Academic Research and Industry-Academia-Government Collaboration Administration Office (AR&IAGC)

- Establish the Confidential Information Management Policy, Guidelines, etc.
- Oversee confidential information management operations.
- Provide consultation regarding confidential information management.
- Designate and manage confidential information (Level 3).
- Carry out inspections.
- Conduct activities to disseminate information and raise awareness.

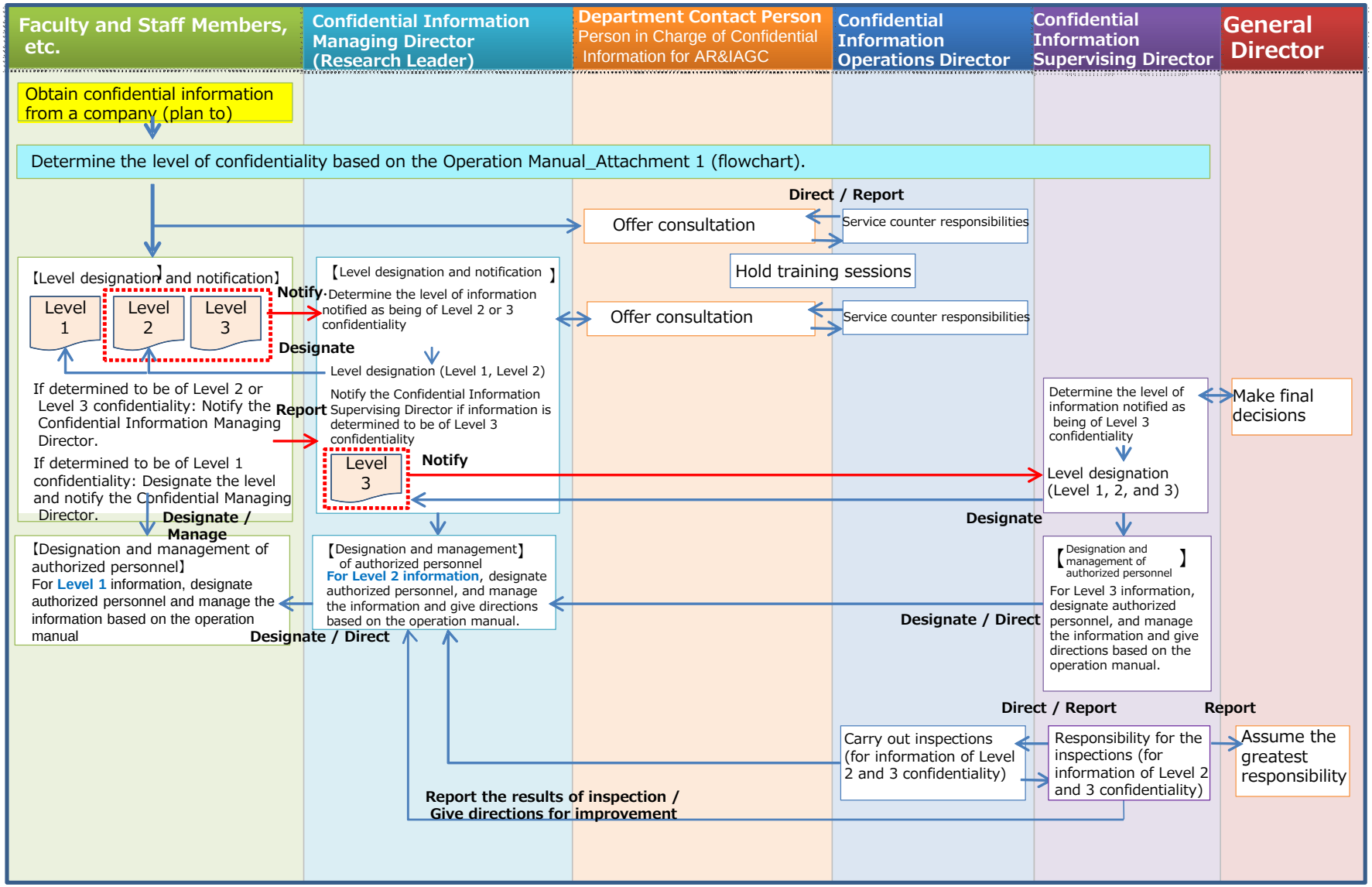
Confidential Information Management Guidelines for Industry-Academia Collaboration at Nagoya University

Grades of Secret Information	The following levels shall be established for the purpose of confidential information management; confidential information to be treated as trade secrets as agreed upon by the University and any organizations who disclose such confidential information (hereinafter referred to as "company, etc.") shall be managed as information with Level 3 or 2 confidentiality. **2** Criteria for designating confidential information within each level shall in principle be as below. However, level designation not based on the following is also possible. 1. Level 3 Information for which the strictest management is required, as the company, etc. has designated that its leakage may result in serious losses or disadvantages for the company and considerably affect the company's value, such as stock prices. 2. Level 2 (a) Confidential information obtained from a company, etc. with certain restrictions imposed by the company, etc. (Confidential information labeled as "Confidential", on which indication of the level of confidentiality that corresponds to the trade secrets, specific access limitations, a distribution record, etc. have been imposed.) (b) Know-how generated through collaborative research, etc., including the confidential information obtained from companies, etc. as described in item (a) above, and for which its contents and attribution are designated, and on which restrictions have been imposed by the other party. (Knowhow labeled as "Confidential", on which indication of the level of confidentiality that corresponds to the trade secrets, specific access limitations, a distribution record, etc. have been imposed.) 3. Level 1 Information on which the obligation of maintaining confidentiality under the care of a prudent manager is strictly imposed by companies, etc., and which falls under any of the following categories (except for information falling under Level 2 described above.) (a) Confidential information obtained from companies, etc. (Confidential information labeled as "Confidential") (b) Contract documents such as collaborative research agreements (those for which "Confidential" handling has been deemed necessary.) (c) Know-how generated through collaborative research, etc., including the confidential information obtained from companies, etc. as described in Level 2, item (a) above, and for which its contents and attribution are designated.

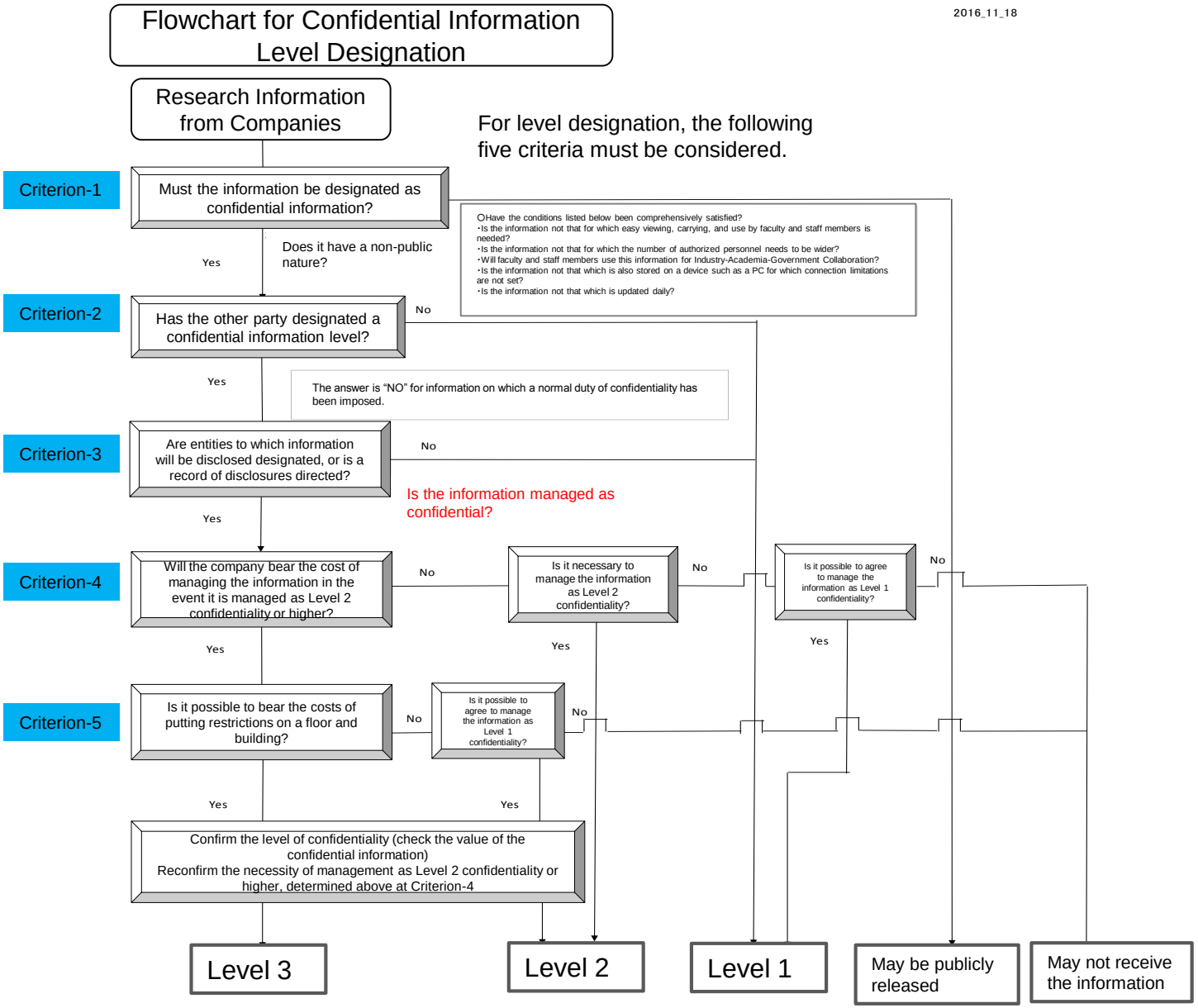
Confidential Information Management Guidelines for Industry-Academia Collaborations at Nagoya University

Designation of Confidential Information Level	1. Confidential information level designation prescribed in the preceding article shall be carried out in accordance with the methods below. However, confidential information possessed by faculty and staff members, etc. who have been transferred from other organizations shall be discussed separately. (i) Designation and notification by faculty and staff members, etc. (a) Faculty and staff members, etc. shall classify confidential information obtained from companies, etc. into each level following the flowchart for Confidential Information Level Designation found in the Operation Manual. (b) When faculty and staff members, etc. obtain information judged to be of Level 1 confidentiality, they shall designate it as confidential information and at the same time notify their Confidential Information Managing Director about the case after designating the confidential information level (Level 1) as prescribed in the preceding article. (c) When faculty and staff members, etc. obtain information judged to be of Level 2 or 3 confidentiality, they shall notify their Confidential Information Managing Director. The Confidential Information Managing Director notified shall designate the confidential information level (Level 1 or 2) as prescribed in the preceding article for information judged to be of Level 1 or 2 confidentiality, while for information judged to be of Level 3 confidentiality, he or she shall notify the Confidential Information Supervising Director (hereinafter referred to as the “Supervising Director”). The Supervising Director notified shall designate the confidential information level (Level 1, 2, or 3) as prescribed in the preceding article. (ii) Faculty and staff members, etc., in accordance with procedures (a) to (c) above, shall complete the procedures for changing or removing the confidential information level which are prescribed in the preceding article whenever confidentiality is no longer required, the level of confidentiality has decreased, or confidential information management level is required to be changed due to the passage of time or other circumstances. (d) When a company who will disclose confidential information does not hold the proper authority to do so, or there is doubt whether it holds the proper authority, faculty and staff members, etc. shall decline the information disclosure and notify their Confidential Information Managing Director of their doubts. 2. In addition to what is prescribed in these Guidelines, procedures for level designation shall be separately stipulated in the Operation Manual for Confidential Information Management for Industry-Academia Collaborations (hereinafter referred to as "the operation manual”.)

Confidential Information Management Flowchart



Confidential Information Level Designation Flowchart



Confidential Information Management Guidelines for Industry-Academia Collaboration at Nagoya University

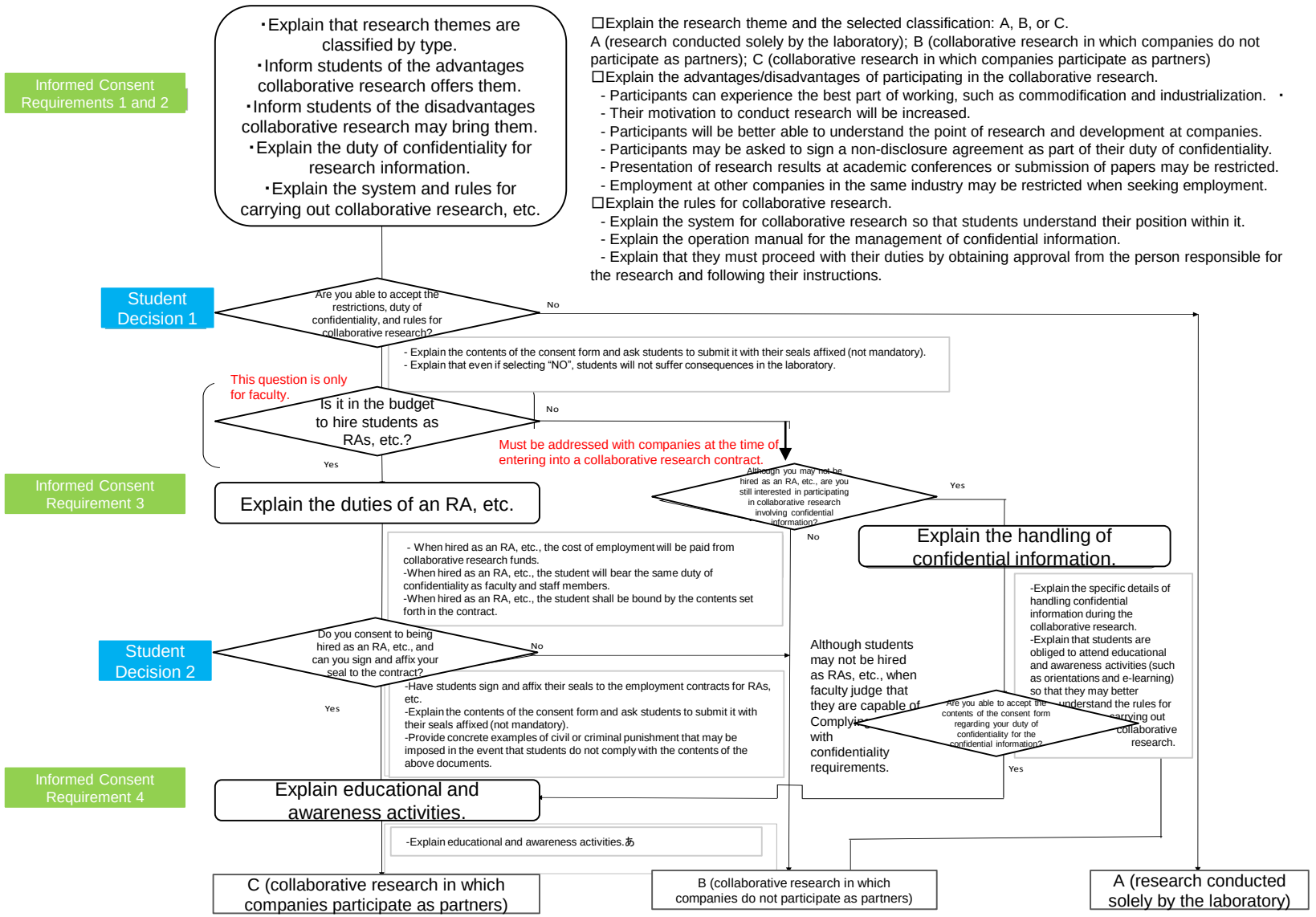
Students and Collaborative Researchers	1. When faculty and staff members, etc. have students participate in collaborative research, etc., they shall respect students' voluntary intentions following the obtainment of their informed consent as prescribed in the operation manual. 2. When faculty and staff members, etc. have students who do not have contractual relationships with the University, such as employment contracts, participate in collaborative research, etc., they can ask the students to sign a "Consent Form" detailing the handling of research results and confidential information prior to the start of their engagement in the collaborative research, etc. if the other party in the collaborative research requests them to do so. 3. When faculty and staff members, etc. have students who have contractual relationships with the University, such as employment contracts, participate in collaborative research, etc., the students will be under the confidentiality obligations of their contracts with the University. 4. Faculty and staff members, etc. shall have students who will graduate, complete their course of study, or withdraw from the University, reconfirm the legal mechanisms and practical action, etc. for the protection of confidential information, as well as the contents of the confidentiality obligation they must owe while they engaged in the collaborative research, etc. Furthermore, all confidential information obtained by such students shall be transferred to faculty and staff members, etc. 5. When faculty and staff members, etc. have students who do not have any contractual relationships with the University, such as an employment contract, participate in collaborative research, etc., the information they shall be allowed access to must be restricted to the minimum amount of Level 1 confidential information that is necessary for their research. 6. When faculty and staff members, etc. have students who have contractual relationships with the University, such as employment contracts, participate in collaborative research, etc., they shall be allowed access to all information of Level 1 confidentiality; however, in principle, access to Level 2 or 3 information is not granted. 7. When accepting collaborative researchers, the Confidential Information Managing Director may instruct the collaborative researchers, as is necessary, to sign a "Consent Form" detailing the handling of research results and confidential information prior to the start of their engagement in the collaborative research, etc.

Informed Consent Flowchart

暫定版

Informed Consent Flowchart for Students (Short Version)

When students assigned to a laboratory participate in collaborative research, explanation of informed consent requirements shall be provided as below:



Operational Manual for Confidential Information Management for Industry-Academia Collaborations at Nagoya University

暫定版

Purpose	These detailed operational rules aim to establish the matters necessary to carry out, in a reasonable manner, confidential information level designation as prescribed in Article 5, confidential information management as prescribed in Article 6, and obtainment of informed consent from students as prescribed in Article 7of the Confidential Information Management Guidelines for Industry-Academia Collaboration stipulated separately, and to consequently promote proper management as well as utilization of confidential information during industry-academia collaborations.
Confidential Information Designation	1. Regarding confidential information level designation as prescribed in Article 5 of the Confidential Information Management Guidelines for Industry-Academia Collaboration, the Confidential Information Management Committee, etc. shall prescribe policies and standards to identify the confidential information and designate a level of confidentiality. In accordance with these policies, etc., each department shall establish operational rules by which faculty, etc. shall identify confidential information and also designate its level of confidentiality. 2. Faculty and staff members, etc. shall classify confidential information obtained from companies into appropriate level, based on the Confidential Information Level Designation Flowchart stipulated in Attachment 1.
Confidential Information Management at Each Level	1. For the management of confidential information (Levels 1 to 3) as prescribed in Article 4 of the Confidential Information Management Guidelines for Industry-Academia Collaboration, specific examples of confidential information management set forth in Article 6 of the same Guidelines shall be prescribed in Appended Table 1; specific examples include how to label a level of its confidentiality, restrict access to, store, copy, view, distribute, take out, and dispose of documents with confidential information or digitized information.
Informed Consent When Having Students Participate in Collaborative Research, etc.	When faculty and staff members, etc. have students participate in collaborative research, etc., they shall obtain informed consent from students as prescribed in Article 7 of the Confidential Information Management Guidelines for Industry-Academia Collaboration, respecting students' voluntary intentions. (i) Faculty and staff members, etc. shall explain the requirements of informed consent to students using the flowchart prescribed in Attachment 2 as a reference, and have them participate in collaborative research, etc. only upon receiving their consent.

Operational Manual for Confidential Information Management for Industry-Academia Collaborations at Nagoya University

Attachment 1

暫定版

Section	Level 3	Level 2	Level 1
Criteria for Designation	● Confidential Information that its leakage may result in extremely serious losses or advantages for a company, etc. e.g.) Confidential Information that affects company's stock prices, M&A, LBO, etc.	● Confidential Information that its leakage may result in serious losses or advantages for a company, etc. e.g.) Confidential information regarding research, etc. received from companies during collaborative research, etc., on which restrictions have been imposed by the other party. e.g.) Know-how generated through collaborative research, etc., including the confidential information obtained from companies, and for which its contents and attribution are designated, and on which restrictions have been imposed by the other party.	● Information, etc. on which a normal obligation of ma confidentiality is imposed between the University and company, etc. e.g.) Confidential information regarding research etc. received from companies, etc. during collaborative research, etc. e.g.) Contract documents such as collaborative research agreements, etc. e.g.)Know-how generated during collaborative research, etc., in which confidential information obtained from companies, etc. is included, and its contents and attribution are designated. ● In principle, a level of confidential information which students may access is Level 1 only.
Level Designation	● Confidential Information Supervising Director shall determine and designate a level of the notified confidential information based on the Designation Flowchart. ● For confidential information determined and designated as Level 3 confidentiality, the original data shall be managed.	● Confidential Information Managing Director shall determine and designate a level of the notified confidential information based on the Designation Flowchart. ● For confidential information determined and designated as Level 2 confidentiality, the original data shall be managed. ● Confidential information designated as Level 3 confidentiality shall be reported to the Confidential Information Supervising Director	● Confidential Information designated Faculty and staff members in charge of the management of obtained confidential information shall determine and designate its level based on the Designation Flowchart, then report the result to the Confidential Information Managing Director. ● Confidential Information designated as Level 2 confidentiality or higher must be reported to the Confidential Information Managing Director.
Authorized Personnel	● The Confidential Information Supervising Director will designate authorized personnel. Faculty and staff members, etc. and collaborative researchers	● The Confidential Information Managing Director will designate authorized personnel. Faculty and staff members, etc. and collaborative researchers	● Faculty and staff members in charge of the management of obtained confidential information will designate authorized personnel Faculty and staff members, etc., collaborative researchers, and students
Labeling	● Confidential information labeled by companies as "Top Secret" or other such words, shall be labeled as Level 3 confidential information.	● Confidential information labeled by companies as "Secret" or other such words, shall be labeled as Level 2 confidential information.	● Confidential information labeled by companies as "Confidential" or other such words, is desired to be labeled as Level 1 confidential information.
Entrance and Exit Restriction	● Entering and leaving the buildings or floors where documents with confidential information or digitized information is stored must be restricted.	● Entering and leaving the rooms where documents with confidential information or digitized information is stored must be restricted.	● Entering and leaving the rooms where documents with confidential information or digitized information is stored are desired to be restricted.
Storage	● Confidential information data (such as documents in paper form) must be stored in a locked dedicated storage cabinet, etc. Keys must be managed by the Confidential Information Supervising Director, or faculty and staff members, etc. and collaborative researchers designated by the Confidential Information Supervising Director.	● Confidential information data (such as documents in paper form) must be separated from other data and stored in a locked dedicated storage cabinet, etc. ● Keys must be managed by the Confidential Information Managing Director	● Confidential information data (such as documents in paper form) must be stored in a locked storage cabinet. ● Keys must be managed by the faculty and staff members in charge of the management of obtained confidential information.
	● When storing digitized information on information device (such as PC), make sure to take measures such as encryption, then store the information on a dedicated information device not connected to any network and install the information device in the access controlled area. The information device must be authenticated by password.	● When storing digitized information on information device (such as in a PC), make sure to take measures such as encryption, and install the information device in the access controlled area. The information device must be authenticated by password.	● When storing digitized information on information device (such as in a PC), install the information device in the access controlled area as a general rule. In the case it cannot be installed in the access controlled area, take measures such as encryption, then store it on information device, or setup an authentication by password on the device.
	● Digitized information must not be stored on digital media (such as a USB).	● When storing digitized information on digital media (such as a USB), take measures such as encryption, then setup an authentication by password on the digital media. Store the digital media in a locked storage cabinet, etc. ● Keys must be managed by the Confidential Information Managing Director	● When storing digitized information on digital media (such as a USB), the digital media must be stored in a locked storage cabinet, etc., separating from other digital medias. ● Keys must be managed by the faculty and staff members in charge of the management of obtained confidential information.

Operational Manual for Confidential Information Management for Industry-Academia Collaborations at Nagoya University

Attachment 1

暫定版

Section	Level 3	Level 2	Level 1
Copy	● Copying, printing, and taking pictures are not allowed.	● Only the Confidential Information Managing Director or those who have received permission from the Confidential Information Managing Director are allowed to copy, print, or take pictures. ● When printing out digitized information, as a general rule, use printers installed in an access controlled area, or a private room, etc. where only the authorized handlers of such digitized information have occupied, and be careful that the information is not be read by anyone without authority to access such digitized information. If using the printers installed in the place other than above, make sure to wait in front of the printer during printing, and collect all papers once printing is complete.	● Only faculty and staff members in charge of the management of obtained confidential information, or those who have received authority to access from faculty and staff members in charge of the management of obtained confidential information, may copy, print, or take pictures. ● When copying or printing, make sure to collect all data or papers once copying or printing is complete, in order to prevent anyone without authority to access from reading the printed or copied information.
Viewing	● Anyone without authority to access the information shall not be allowed to view it.	● Anyone without authority to access the information shall not be allowed to view it. ● When showing digitized information on the screen, be aware of your surroundings so that anyone without authority to access the information cannot read it.	● Anyone without authority to access the information shall not be allowed to view it. ● When showing digitized information on the screen, be aware of your surroundings so that anyone without authority to access the information cannot read it.
Distribution	● Distribution and sending are not allowed.	● Documents shall be labeled as “Secret” or other such words to indicate its Level 2 confidentiality, and other necessary measures such as providing an explanation of the methods of handling such information shall also be taken in order to prevent the leakage of information to anyone without authority to access the information. ● In the case where the document, etc. is distributed during a meeting, etc., consecutive numbers shall be attached to each copy, and all copies shall be collected once the meeting is finished. ● When sending documents, etc. via postal mail, the envelope shall be sealed and sent as a confidential letter depending on the situation. ● When sending digitized information via e-mail to those with authority to access the information, the information shall be encrypted before being sent. ● When sending via FAX, request a recipient of the fax data to wait in front of the FAX machine to receive the data as soon as it arrives.	● It is desirable that documents, etc. are labeled as “Confidential” or other such words to indicate its Level 1 confidentiality, and other necessary measures such as providing an explanation of the methods of handling such information or collecting documents, shall also be taken in order to prevent the leakage of information. ● When sending digitized information via e-mail to those with authority to access the information, the information shall be encrypted or password shall be set to digital media before being sent.
Taking out	● The information shall not be taken outside the storage area.	● If taking the information outside the storage area, permission from the Confidential Information Managing Director shall be obtained in advance. ● If taking the information outside campus, the assigned handler themselves must carry the information and store it in a storage cabinet at the destination. ● If taking out digital media on which digitized information is stored outside the storage area, appropriate measures such as encryption of data, etc. shall be taken. ● If sending digitized information via e-mail or other means, appropriate measures such as encryption of data, etc. shall be taken.	● If taking the information outside the storage area, persons with authority to access themselves must carry the information and store it in a storage cabinet at the destination. ● If taking out digital media on which digitized information is stored outside the storage area, appropriate measures such as encryption of data, etc. shall be taken. ● If sending digitized information via e-mail or other means, appropriate measures such as encryption of data, etc. shall be taken.
Disposal	● Permission from the Confidential Information Supervising Director shall be obtained in advance. ● Under the direction and responsibility of the Confidential Information Supervising Director, remaining information shall be disposed of so that it is not viewed by any third party.	● Permission from the Confidential Information Managing Director shall be obtained in advance. ● Under the direction and responsibility of the Confidential Information Managing Director, remaining information shall be disposed of so that it is not viewed by any third party.	● Under the direction and responsibility of the faculty and staff members in charge of the management of obtained confidential information, remaining information shall be disposed of so that it is not viewed by any third party.

Trial Phase of the Confidential Information Management Policy, etc.

The formulated Confidential Information Management Policy, etc. and its format are being tested as follows:

1. Institute of Innovation for Future Society (COI)

COI, at which academic-industrial collaborative courses with various institutions are conducted, has referred to the Confidential Information Management Policy, etc. in carrying out sufficient management methods for confidential information: COI has obliged retirees and students to submit confidentiality consent forms, thus complying with the Confidential Information Management Rules.

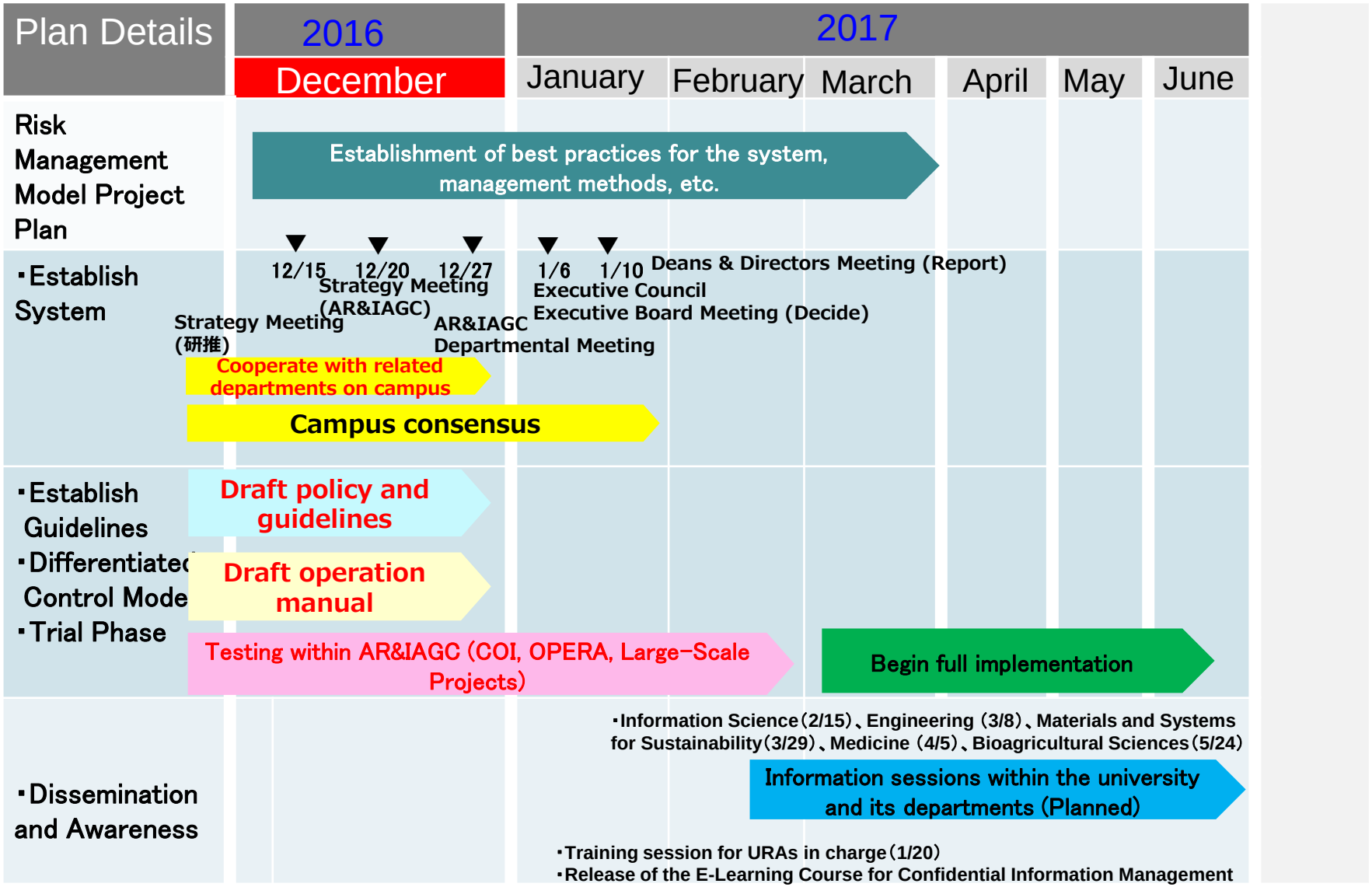
2. Open Innovation Platform for Enterprises, Research Institutes, and Academia (OPERA)

A structure for conducting full-scale collaborative research projects in addition to hiring doctoral students is required for the OPERA platform. For this structure, a system in compliance with the Rules has been implemented, with the soon to be operated "Check Sheet for Hiring Students (for students / academic advisors)," which incorporates informed consent as prescribed in the Confidential Information Management Guidelines for Industry-Academia Collaboration, and other rules and regulations.

3. Large-Scale Collaborative Research Projects Being Conducted with the Support of the Regional Collaboration & Communication Group

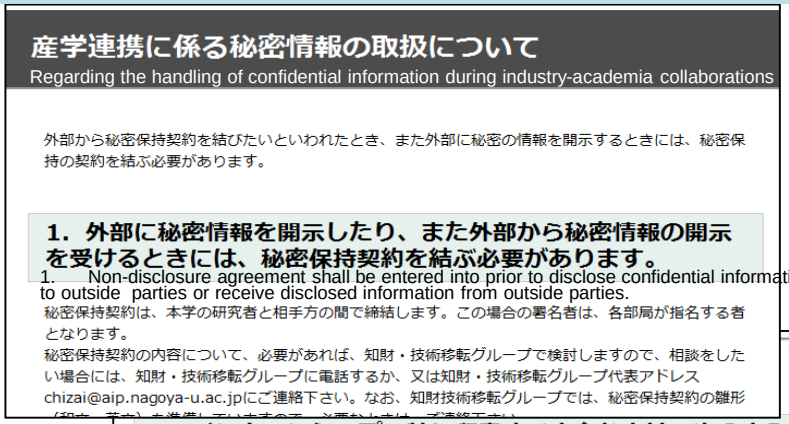
As a precondition for entering the several large-scale collaborative research project agreements that the Regional Collaboration & Communication Group is currently coordinating, confidential information management on the part of the University is being requested by companies, etc. Confidential Information Management Rules are under consideration for use by referring to the Confidential Information Management Policy, and other rules and regulations.

Future Schedule



One-stop Consultation Counter for Confidential Information Management

Feel free to consult with us if you have any concerns about the handling of confidential information or other matters.



【相談窓口】【Contact】

学術研究・産学官連携推進本部

052-747 -6702

Academic Research and Industry-Academia-Government Collaboration Administration Office (AR&IAGC)