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

#### Confidential information related to the University’s independent research
- Experiment data and research results (software, biological samples, etc.) prior to patent application
- Papers, laboratory notes, or other information prior to paper publication.

#### Confidential information offered by companies or other universities, etc. that is provided in the course of collaborative research, etc.
- Examples: Research data, research and development plans, source code, etc.

#### Confidential information other than “trade secrets”

#### “Trade secrets”

---

---

### 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.

---

---

Confidential information from companies must be given sufficient attention!!
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.
"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 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.

University, etc
Faculty, etc

Company A

Company B

(Venture Companies)

Person who has already been provided with trade secrets during his or her tenure

Using the trade secret against their duties in managing the trade secrets (applies to No. 5.)

Disclosing the trade secret against their duties in managing the trade secrets (applies to No. 5.)

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).”

### Information that possibly falls into trade secrets

#### Information from companies

<table>
<thead>
<tr>
<th>“Intellectual property constituting the company’s strength”</th>
<th>“Information assets constituting the company’s strength”</th>
</tr>
</thead>
</table>
| **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.) |
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

<table>
<thead>
<tr>
<th>Established, Formulated, and Constructed Items:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Policies and guidelines</td>
</tr>
<tr>
<td>• Process for classifying confidential information into appropriate level</td>
</tr>
<tr>
<td>• Methods for level management according to the level of risk</td>
</tr>
<tr>
<td>• Informed consent requirements for students</td>
</tr>
<tr>
<td>• Process for obtaining informed consent</td>
</tr>
<tr>
<td>• University-wide confidential information management system</td>
</tr>
<tr>
<td>Established</td>
</tr>
<tr>
<td>Formulated</td>
</tr>
<tr>
<td>Established</td>
</tr>
<tr>
<td>Constructed</td>
</tr>
</tbody>
</table>

**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
### 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

- **University President (General Director)**
  - 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.

- **Board of Directors**
  - Chairperson of the Confidential Information Management Committee
  - Members from each department

- **Confidential Information Supervising Director**
  - Drafting of policies and guidelines
  - Proposal of the operation manual

- **Confidential Information Operations Director**
  - Reports from AR&IAGC on the management situation

- **Person in Charge of Confidential Information at AR&IAGC (URA)**
  - Cooperation

- **Department Directors**
  - Confidential Information Managing Director (faculty leading the research)
  - Reports
  - Dissemination

- **Consultation**

- **Faculty and staff members, 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)**

- **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.
### Grades of Secret Information

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 3</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
| **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.) |
| **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. |
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”.)
Determine the level of confidentiality based on the Operation Manual_Attachment 1 (flowchart).

For Level 1 information, designate authorized personnel and manage the information based on the operation manual.

For Level 2 information, designate authorized personnel, and manage the information and give directions based on the operation manual.

For Level 3 information, designate authorized personnel, and manage the information and give directions based on the operation manual.

Notify the Confidential Information Managing Director if information is determined to be of Level 3 confidentiality.

Offer consultation

Hold training sessions

Make final decisions

Responsibility for the inspections (for information of Level 2 and 3 confidentiality)

Assume the greatest responsibility

Carry out inspections (for information of Level 2 and 3 confidentiality)
Flowchart for Confidential Information Level Designation

For level designation, the following five criteria must be considered.

**Criterion-1**
Must the information be designated as confidential information?

- Yes
- No

**Criterion-2**
Has the other party designated a confidential information level?

- Yes
- No

The answer is "NO" for information on which a normal duty of confidentiality has been imposed.

**Criterion-3**
Are entities to which information will be disclosed designated, or is a record of disclosures directed?

- Yes
- No

**Criterion-4**
Will the company bear the cost of managing the information in the event it is managed as Level 2 confidentiality or higher?

- Yes
- No

**Criterion-5**
Is it possible to bear the costs of putting restrictions on a floor and building?

- Yes
- No

Confirm the level of confidentiality (check the value of the confidential information)
Reconfirm the necessity of management as Level 2 confidentiality or higher, determined above at Criterion-4

- Yes
- No

**Level 3**
**Level 2**
**Level 1**
**May be publicly released**
**May not receive the information**
| 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. |
Explain the system for collaborative research so that students understand their position within it.

Presentation of research results at academic conferences or submission of papers may be restricted.

Explain that even if selecting “NO”, students will not suffer consequences in the laboratory.

Employment at other companies in the same industry may be restricted when seeking employment.

Explain the duties of an RA, etc.

Explain the handling of confidential information.

• Explain that research themes are classified by type.
• Inform students of the advantages collaborative research offers them.
• Inform students of the disadvantages collaborative research may bring them.
• Explain the duty of confidentiality for research information.
• Explain the system and rules for carrying out collaborative research, etc.

Explain the rules for collaborative research.
- Explain the system for collaborative research so that students understand their position within it.
- Explain the operation manual for the management of confidential information.
- Explain that they must proceed with their duties by obtaining approval from the person responsible for the research and following their instructions.

Explain educational and awareness activities.

- Explain the contents of the consent form and ask students to submit it with their seals affixed (not mandatory).
- Explain that even if selecting “NO”, students will not suffer consequences in the laboratory.

Are you able to accept the restrictions, duty of confidentiality, and rules for collaborative research?

This question is only for faculty.

Must be addressed with companies at the time of entering into a collaborative research contract.

Do you consent to being hired as an RA, etc., and can you sign and affix your seal to the contract?

Have students sign and affix their seals to the employment contracts for RAs, etc.

Explain the duties of an RA, etc.

• When hired as an RA, etc., the cost of employment will be paid from collaborative research funds.
• When hired as an RA, etc., the student will bear the same duty of confidentiality as faculty and staff members.
• When hired as an RA, etc., the student shall be bound by the contents set forth in the contract.

Although students may not be hired as RAs, etc., when faculty judge that they are capable of complying with confidentiality requirements.

Explain the handling of confidential information.

- Explain the specific details of handling confidential information during the collaborative research.
- Explain that students are obliged to attend educational and awareness activities (such as orientations and e-learning) so that they may better understand the rules for managing out confidential information.

When hired as an RA, etc., are you still interested in participating in collaborative research involving confidential information?

Explain educational and awareness activities.

- Explain educational and awareness activities.

C (collaborative research in which companies participate as partners)

B (collaborative research in which companies do not participate as partners)

A (research conducted solely by the laboratory)
<table>
<thead>
<tr>
<th>Purpose</th>
<th>These detailed operational rules aim to establish the matters necessary to carry out, in a reasonable manner, <em>confidential information level designation</em> as prescribed in Article 5, <em>confidential information management</em> as prescribed in Article 6, and <em>obtainment of informed consent from students</em> as prescribed in Article 7 of 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential Information Designation</td>
<td>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.</td>
</tr>
<tr>
<td>Confidential Information Management at Each Level</td>
<td>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.</td>
</tr>
<tr>
<td>Informed Consent When Having Students Participate in Collaborative Research, etc.</td>
<td>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.</td>
</tr>
<tr>
<td>Section</td>
<td>Level 3</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Criteria for Designation</td>
<td>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&amp;A, LBO, etc.</td>
</tr>
<tr>
<td>Level Designation</td>
<td></td>
</tr>
<tr>
<td>Authorized Personnel</td>
<td>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.</td>
</tr>
<tr>
<td>Labeling</td>
<td>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.</td>
</tr>
<tr>
<td>Entrance and Exit Restriction</td>
<td>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.</td>
</tr>
<tr>
<td>Storage</td>
<td>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 dedicated 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 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), 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. 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.</td>
</tr>
<tr>
<td>Digitized information must not be stored on digital media (such as a USB).</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Level 3</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>● Copying, printing, and taking pictures are not allowed.</td>
</tr>
<tr>
<td><strong>Viewing</strong></td>
<td>● Anyone without authority to access the information shall not be allowed to view it.</td>
</tr>
<tr>
<td><strong>Distribution</strong></td>
<td>● Distribution and sending are not allowed.</td>
</tr>
<tr>
<td><strong>Taking out</strong></td>
<td>● The information shall not be taken outside the storage area.</td>
</tr>
<tr>
<td><strong>Disposal</strong></td>
<td>● 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.</td>
</tr>
</tbody>
</table>
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

#### Plan Details

<table>
<thead>
<tr>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>December</strong></td>
<td><strong>January</strong></td>
</tr>
<tr>
<td><strong>Risk Management Model Project Plan</strong></td>
<td></td>
</tr>
<tr>
<td>▪ Establish System</td>
<td>12/15 Strategy Meeting (AR&amp;IAGC)</td>
</tr>
<tr>
<td></td>
<td>12/20 Strategy Meeting (AR&amp;IAGC)</td>
</tr>
<tr>
<td></td>
<td>Cooperate with related departments on campus</td>
</tr>
<tr>
<td></td>
<td>Campus consensus</td>
</tr>
<tr>
<td>▪ Establish Guidelines</td>
<td>Draft policy and guidelines</td>
</tr>
<tr>
<td>▪ Differentiated Control Mode</td>
<td>Draft operation manual</td>
</tr>
<tr>
<td>▪ Trial Phase</td>
<td>Testing within AR&amp;IAGC (COI, OPERA, Large-Scale Projects)</td>
</tr>
<tr>
<td>▪ Dissemination and Awareness</td>
<td></td>
</tr>
</tbody>
</table>

#### 2016

- Establish System
  - Strategy Meeting (AR&IAGC)
  - Cooperate with related departments on campus
  - Campus consensus

#### 2017

- January
  - Executive Council Meeting
- February
  - Executive Board Meeting (Decide)
- March
  - AR&IAGC Departmental Meeting
- April
  - 1/6 Executive Council Meeting
- May
  - 1/10 Executive Board Meeting (Decide)
- June
  - Deans & Directors Meeting (Report)

### Future Schedule Details

- **December 2016**
  - Establishment of best practices for the system, management methods, etc.

- **January 2017**
  - Deans & Directors Meeting (Report)

- **February 2017**
  - Executive Council Meeting

- **March 2017**
  - Executive Board Meeting (Decide)

- **April 2017**
  - AR&IAGC Departmental Meeting

- **May 2017**
  - Deans & Directors Meeting (Decide)

- **June 2017**
  - Deans & Directors Meeting (Report)

### Information Sessions

- Information sessions within the university and its departments (Planned)
- Information Science (2/15), Engineering (3/8), Materials and Systems for Sustainability (3/29), Medicine (4/5), Bioagricultural Sciences (5/24)
- Training session for URAs in charge (1/20)
- Release of the E-Learning Course for Confidential Information Management
Feel free to consult with us if you have any concerns about the handling of confidential information or other matters.

Non-disclosure agreement shall be entered into prior to disclose confidential information to outside parties or receive disclosed information from outside parties. In case of confidentiality, the signatory shall be recorded in the book of records. During your internship, you must pay special attention to certain matters, such as the following important points.

1. During your internship, you must pay special attention to certain matters, such as the following important points.

2. In case of confidentiality, the signatory shall be recorded in the book of records. During your internship, you must pay special attention to certain matters, such as the following important points.

【Contact】
Academic Research and Industry-Academia-Government Collaboration Administration Office (AR&IAGC)
052-747-6702