Confidential Information Management Manual for Industry-Academia-Government Collaboration

To strengthen trust between the University and its partners in industry-academia-government collaboration, Kanazawa University (“KU” or the “University”) is required to properly control confidential information accessed by KU members in the course of their collaborative activities with others to prevent leaks of Confidential Information.

This Manual describes the procedures that KU faculty and staff are required to carry out to properly control and effectively use Confidential Information.

1. Scope of Confidential Information; Information Controlling Policy

- Scope of information and tangible items
  - Information and tangible items which the University is obligated to keep confidential under an agreement with a partner in industry-academia-government collaboration (excluding Confidential Information containing personal information pertaining to clinical research)

E.g.:
- Information and tangible items designated as being confidential by a partner in a Collaborative Project
- Agreements concluded by the University for Collaborative Projects and designated as being confidential
- Outcomes and related tangible items produced in a Collaborative Project which remain undisclosed and which cannot be publicly disclosed before giving notice to the project partners
- Know-how designated as being confidential based on consultation with a project partner

- Scope of persons assuming the confidentiality obligations
  - Academic staff, other staff and researchers hired by the University and those who participate in a Collaborative Project as a research collaborator (including students who have attained the age of majority)

- Information controlling policy
  - Confidential Information is classified into External Confidential Information and Sensitive External Confidential Information and controlled under the rules specified in the lists on pages 5 to 7.

2. Criteria for Designating Confidential Information

External Confidential Information

External Confidential Information refers to Confidential Information and related tangible items which are not identified as Sensitive External Confidential Information.

Sensitive External Confidential Information

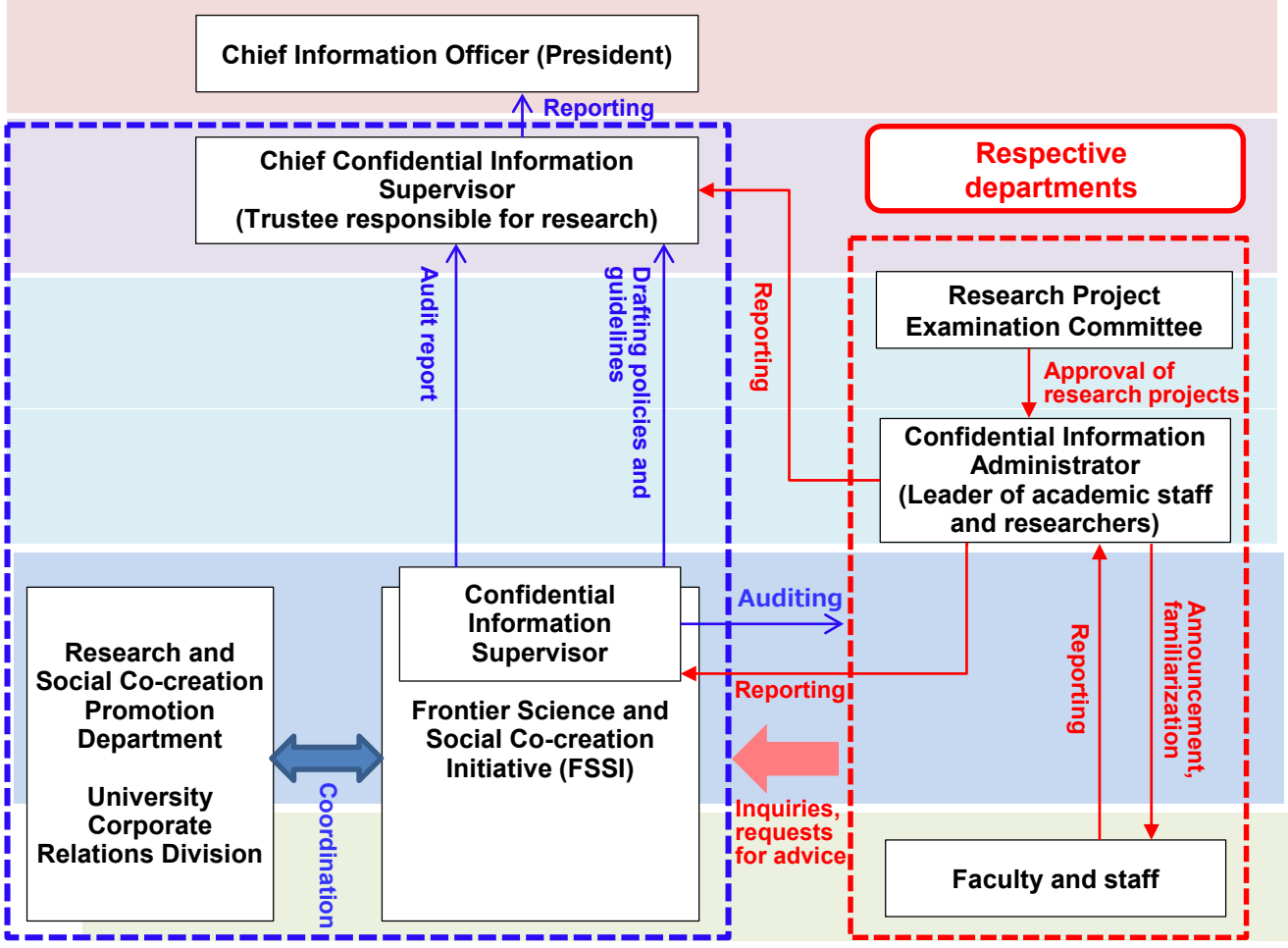
Sensitive External Confidential Information refers to Confidential Information and related tangible items that are subject to advanced control as required by a project partner at the start of a Collaborative Project or thereafter and accepted by the University on condition that the project partner has agreed to bear expenses necessary for such advanced control.

The methods and procedures to be used for controlling Sensitive External Confidential Information will be determined through consultation between the University and each project partner based on the lists on pages 5 to 7.

3. Organizational Framework

- The **Chief Information Officer** is authorized to make final decisions in relation to important issues in the control of Confidential Information. The President is assigned to this position.
- The **Chief Confidential Information Supervisor** is responsible for supervising operations for controlling Confidential Information. The Trustee responsible for research is assigned to this position.
- The **Confidential Information Supervisor** is responsible for familiarizing faculty and staff with the Chief Confidential Information Supervisor's instructions and responds to inquiries or requests for advice from faculty and staff. A person selected from the academic staff attached to the FSSI and appointed by the Chief Confidential Information Supervisor is assigned to this position.
- The position of **Confidential Information Administrator** of each department is assigned to the leader of the faculty in the department who need to access Confidential Information.
- As is conventionally done, External Confidential Information is required to be controlled under the responsibility of each faculty or staff member who has acquired the same from a project partner. (**For controlling methods and procedures, see the lists on pages 5 to 7.**)
- Regarding the workflow for reporting critical incidents, see page 10.

Organizational Framework for Controlling Confidential Information



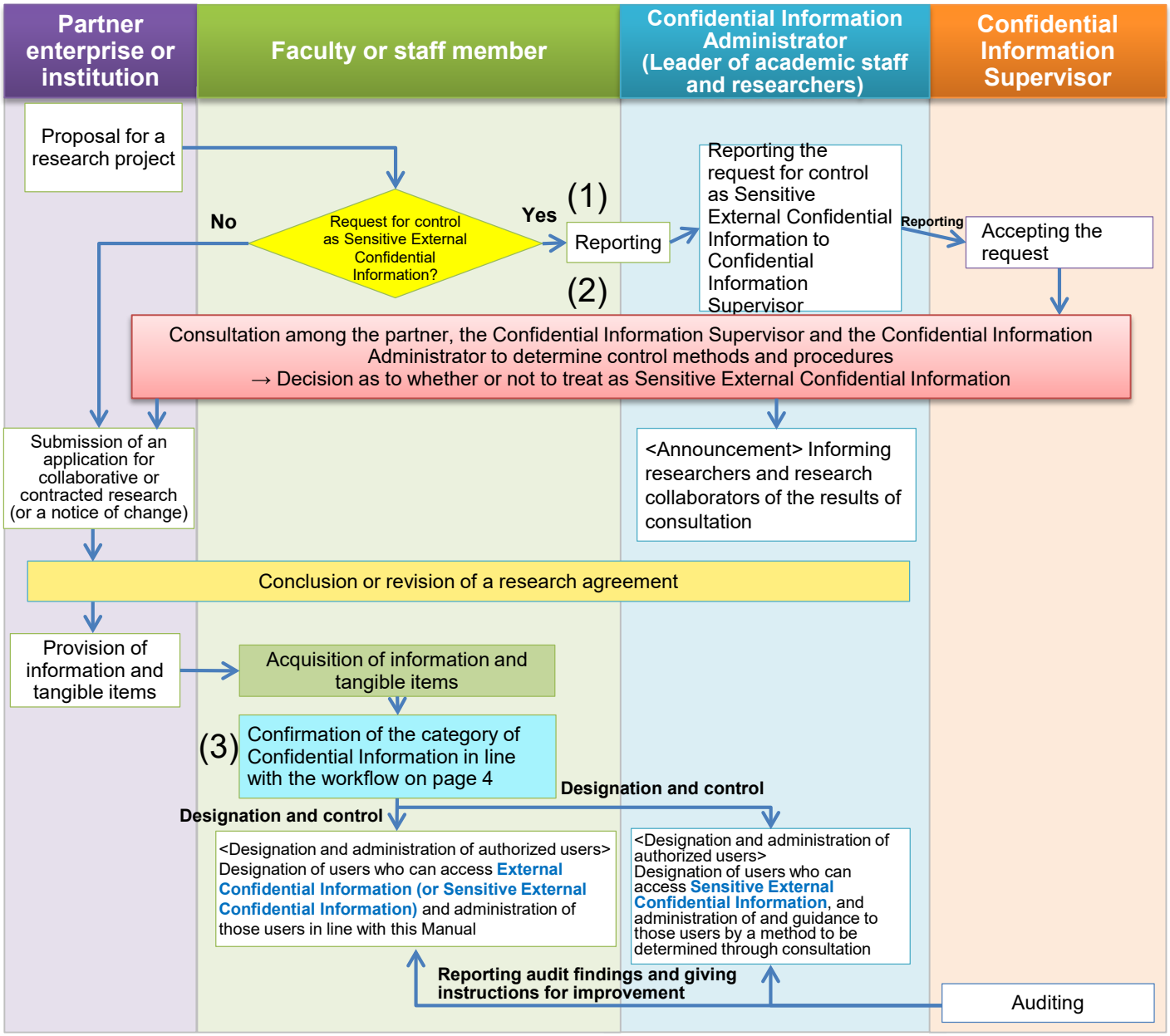
4. Procedural Flow When Collaborative or Contracted Research is Proposed

1) If a faculty or staff member receives a request for control in the form of Sensitive External Confidential Information from a project partner at the start of a Collaborative Project or thereafter, the faculty or staff member must make a report to the relevant Confidential Information Administrator.

2) Upon receipt of a report specified in item (1) above, the Confidential Information Administrator must inform the Confidential Information Supervisor of the request for control in the form of Sensitive External Confidential Information. Then, the Confidential Information Administrator and the Confidential Information Supervisor will consult with the project partner and determine whether or not to control the information in question as Sensitive External Confidential Information.

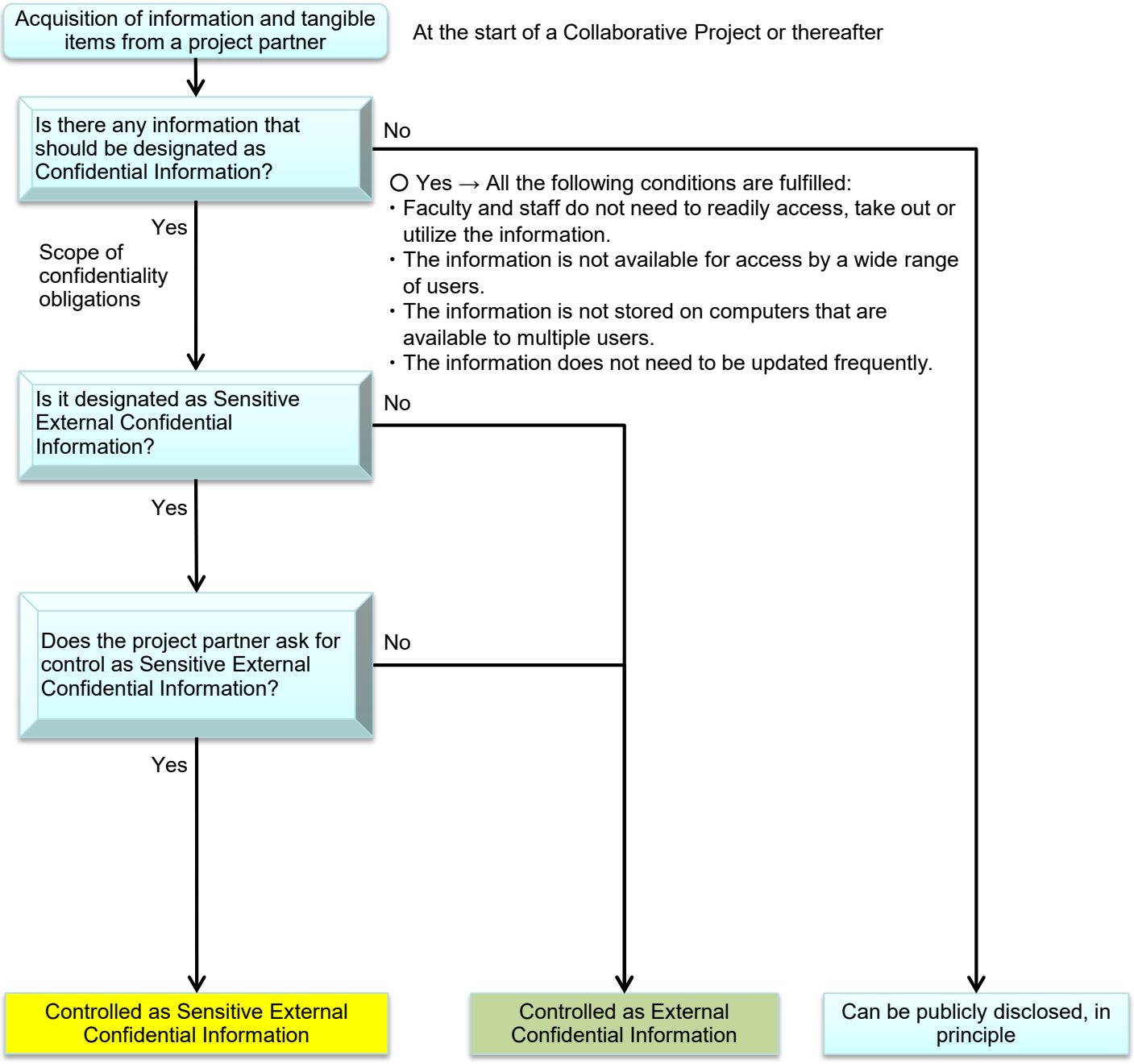
(The contact information of the Confidential Information Supervisor is shown on page 11.)

3) When a faculty or staff member receives certain information or a certain tangible item under an obligation of confidentiality from a project partner, the faculty or staff member must confirm its category of Confidential Information in accordance with the workflow shown on page 4.



5. Workflow for Confirming the Category of Confidential Information

- When a faculty or staff member receives certain information or a certain tangible item under an obligation of confidentiality from a project partner, the faculty or staff member must confirm its category in line with the following workflow and control the Confidential Information based on the lists on pages 5 to 7.



6. Methods of Controlling Confidential Information

- Confidential Information must be handled in line with the following rules.
- For the items with a box (☐), one applicable item must be selected based on consultation with the project partner.
- Red-letter items for Sensitive External Confidential Information describe a requirement stricter than that for External Confidential Information.
- The formats of administration tools (charts, sheets, etc.) can be downloaded at the URL shown on page 11.

Category of rules		External Confidential Information	Sensitive External Confidential Information
Who is responsible for the control		・The faculty or staff member who has acquired the Confidential Information	☐The faculty or staff member who has acquired the Confidential Information ☐Confidential Information Administrator
Labeling		☐Must be marked as “Confidential.” ☐Other* ( )	☐Must be marked as “Strictly Confidential.” ☐Other* ( )
		* If the project partner adopts a different labeling practice, a mutually agreeable mark to identify Confidential Information must be determined through consultation.	
Management with administration tools (charts, sheets, etc.)		-	☐ No need to use administration tools ☐ Need to use administration tools Primarily managed by: Confidential Information Administrator ☐ Must be reported to the Chief Confidential Information Supervisor.
Entry and exit control		・Entry control is required, in principle, for the rooms used for storing Confidential Information.	☐ Entry into the rooms used for storing Confidential Information must be restricted. ☐ Entry into the building or floor used for storing Confidential Information must be restricted. ☐ Other ( )
Access control		・Access to the information is limited to faculty and staff, collaborating researchers, and students acting as a research collaborator. ・Access authority is given to the users designated by the faculty or staff member responsible.	☐ Access to the information is limited to faculty and staff and collaborating researchers. ☐ Students acting as a research collaborator may be included in authorized users. ☐ Access authority is given to the users designated by the faculty or staff member responsible. ☐ Access authority is given to the users designated by the Confidential Information Administrator.
Viewing		・Only those who are given access authority ・Must be made unreadable by anyone other than authorized users.	・Only those who are given access authority ・Must be made unreadable by anyone other than authorized users. ☐ Must be recorded in administration tools. ☐ Must be reported to the Chief Confidential Information Supervisor. ☐ Other ( )
Copying, printing, photographing	Authorized users	・The faculty or staff member responsible for the control of the Confidential Information ・Authorized users who have obtained permission from the faculty or staff member responsible	☐ The faculty or staff member responsible for the control of the Confidential Information ☐ Authorized users who have obtained permission from the faculty or staff member responsible ☐ Confidential Information Administrator ☐ Authorized users who have obtained permission from the Confidential Information Administrator
	Recording, reporting	-	☐ Must be recorded in administration tools. ☐ Must be reported to the Chief Confidential Information Supervisor.
	Handling of information in paper form	・Original documents and copies must be immediately collected from the copy machine in each instance.	☐ Original documents and copies must be immediately collected from the copy machine in each instance. ☐ Creation of paper outputs must be controlled based on user IDs. ☐ Copying, printing and photographing are prohibited. ☐ Other ( )
	Handling of electronic information	・Paper outputs must be collected immediately after printing. ・Photographic data on a digital camera, mobile phone, smartphone or other device must be deleted after photographing.	☐ Paper outputs must be collected immediately after printing. ☐ Photographic data on a digital camera, mobile phone, smartphone or other device must be deleted after photographing. ☐ Printers must be located in a room subject to entry and exit control. ☐ Printers must be located in a room exclusively for users authorized to handle the Confidential Information. ☐ Those who use a printer must wait at the printer while paper outputs are being printed. ☐ Creation of paper outputs must be controlled based on user IDs. ☐ Copying, printing and photographing are prohibited. ☐ Other ( )

Category of rules		External Confidential Information	Sensitive External Confidential Information
Distribution	Authorized users	・The faculty or staff member responsible for the control of the Confidential Information ・Authorized users who have obtained permission from the faculty or staff member responsible	☐ The faculty or staff member responsible for the control of the Confidential Information ☐ Authorized users who have obtained permission from the faculty or staff member responsible ☐ Confidential Information Administrator ☐ Authorized users who have obtained permission from the Confidential Information Administrator
	Recording, reporting	-	☐ Must be recorded in administration tools. ☐ Must be reported to the Chief Confidential Information Supervisor.
	Handling of information in paper form	・Must be marked as “Confidential,” with an explanation of how to handle it. ・Handouts must be collected where applicable. ・If sending by postal mail, seal the envelope and mark “Private and Confidential” where needed. ・If sending by fax, use a machine with a function for preventing erroneous transmissions.	☐ Must be marked as “Confidential,” with an explanation of how to handle it. ☐ Handouts must be collected where applicable. ☐ All handouts must be serially numbered and collected after the meeting is finished. ☐ If sending by postal mail, seal the envelope and mark “Private and Confidential” where needed. ☐ If sending by fax, use a machine with a function for preventing erroneous transmissions. ☐ If sending by fax, ask the recipient to wait at the fax machine to immediately pick up the documents. ☐ Delivery by hand (no other method allowed) ☐ Distribution prohibited ☐ Other ( )
	Handling of electronic information	・If sending by e-mail, encryptions, password settings or the like are required. ・If sending by e-mail, an attached file and its password must be sent by separate mails.	☐ If sending by e-mail, encryptions, password settings or the like are required. ☐ If sending by e-mail, an attached file and its password must be sent by separate mails. ☐ Distribution prohibited ☐ Other ( )
Storage	Handling of information in paper form	・Must be stored in a locked cabinet. ・The faculty or staff member responsible keeps cabinet keys.	☐ Must be stored in a locked cabinet. ☐ Must be segregated from other documents and stored in a locked cabinet. ☐ Must be stored in a locked dedicated cabinet. ☐ The faculty or staff member responsible keeps cabinet keys. ☐ The Confidential Information Administrator keeps cabinet keys. ☐ Other ( )
	Handling of electronic information	・Logins to information devices (e.g., computers) must be authenticated by passwords. ・Files, folders, etc. must be encrypted, in principle. ・Authority settings for network access are required. ・When storing data on an electronic device (e.g., USB flash drive), the device must be protected by passwords.	・Logins to information devices (e.g., computers) must be authenticated by passwords. ・Files, folders, etc. must be encrypted. ☐ Information devices must be located in a room subject to entry and exit control. ☐ Information devices must be located on a floor and in a building that are both subject to entry and exit control. ☐ Must be stored on a dedicated information device that is disconnected from the network. ☐ When storing data on an electronic device (e.g., USB flash drive), the device must be protected by passwords. ☐ Storing digitized information on an electronic device is prohibited. ☐ Other ( )

Category of rules		External Confidential Information	Sensitive External Confidential Information
Taking out	Authorized users	・The faculty or staff member responsible for the control of the Confidential Information ・Authorized users who have obtained permission from the faculty or staff member responsible	☐ The faculty or staff member responsible for the control of the Confidential Information ☐ Authorized users who have obtained permission from the faculty or staff member responsible ☐ Confidential Information Administrator ☐ Authorized users who have obtained permission from the Confidential Information Administrator
	Recording, reporting	-	☐ Must be recorded in administration tools. ☐ Must be reported to the Chief Confidential Information Supervisor.
	Handling of information in paper form	・When information media need to be taken out of their storage area, only authorized users are allowed to do so.	☐ When information media need to be taken out of their storage area, only authorized users are allowed to do so. ☐ Taking out information media is prohibited. ☐ Other ( )
	Handling of electronic information	・If taking information media out of their storage area, electronic information must be encrypted or protected by passwords.	☐ If taking information media out of their storage area, electronic information must be encrypted or protected by passwords. ☐ Taking out information media is prohibited. ☐ Other ( )
Return, discarding		・Must be returned to a project partner or discarded pursuant to an applicable agreement. ・Make residual data unreadable and discard the information media under the responsibility of the faculty or staff member responsible.	・Must be returned to a project partner or discarded pursuant to an applicable agreement. ☐ Make residual data unreadable and discard the information media under the responsibility of the faculty or staff member responsible. ☐ Make residual data unreadable and discard the information media under the responsibility of the Confidential Information Administrator.
Auditing		・Audits may be conducted as and when necessary. Audit leader: Confidential Information Supervisor	・Audits must be conducted every year. Audit leader: Confidential Information Supervisor
Burden of expenses for special measures		-	・Expenses necessary for special control measures are, in principle, paid and borne by project partners.

7. Rules for Enrolling Students in Research Projects

- If a faculty or staff member asks a student to participate in a Collaborative Project as a research collaborator, the faculty or staff member must explain the conditions for handling research outcomes and Confidential Information to the student. Students have a free choice as to whether to participate or not.
- To learn about how to treat research outcomes and Confidential Information, e-learning materials are available from the Kanazawa University Acanthus Portal (as illustrated below).
- To verify whether each student has decided to participate in a Collaborative Project of his/her own free will, the KU Administration Office will ask for submission of a written oath signed by the faculty or staff member and the student on the occasion of concluding an agreement for a Collaborative Project.

Log in to Kanazawa University Acanthus Portal

Sample of Written Oath

誓　約　書（雛型）

国立大学法人金沢大学（以下「金沢大学」という。）と「相手方企業名等」が平成　　年　　月　　日付けで契約した「共同研究／受託研究のいずれかを記入」，研究題目「□□□」（以下「本研究」という。）において，学生が研究協力者として参加するにあたり，研究担当者及び学生は下記内容について確認，承諾し，それぞれの履行義務について遵守することを誓約いたします。

1．研究担当者は，教育上有意義であると判断して，本研究の研究協力者として学生を参加させること。

2．研究担当者は，学生が本研究に参加するにあたり，本研究の契約内容及びその遵守について，十分な説明をするとともに，本研究に学生が参加するか否かの任意性を確保すること。

3．学生は，研究担当者より前項の説明を受け，本研究の契約内容及びその遵守について，十分理解したうえで，自己の自由意思と責任で，本研究の契約書に定める金沢大学の研究協力者として本研究に参加すること。

4．学生は，本研究の契約書で秘密を保持する旨が規定された秘密情報，ノウハウを，秘密保持有効期間内において適切に管理し，第三者へ漏洩しないこと。卒業等により身分に変更があった場合も同様とする。

5．学生は，本研究の研究成果として発明等を創出し，金沢大学が当該発明等に係る知的財産権を承継することを決定した場合，当該知的財産権を金沢大学に譲渡すること。また，学生は，当該譲渡について，金沢大学から知的財産権に関連する規程に関して十分な説明を受け，自己の自由意思と責任で決定すること。なお，金沢大学は，金沢大学学生等発明取扱規程第６条に基づく補償金を支払うこと。

平成　　年　　月　　日

国立大学法人金沢大学
学長　山崎　光悦　殿

研究担当者
所　属：
氏　名（自筆）：　　印

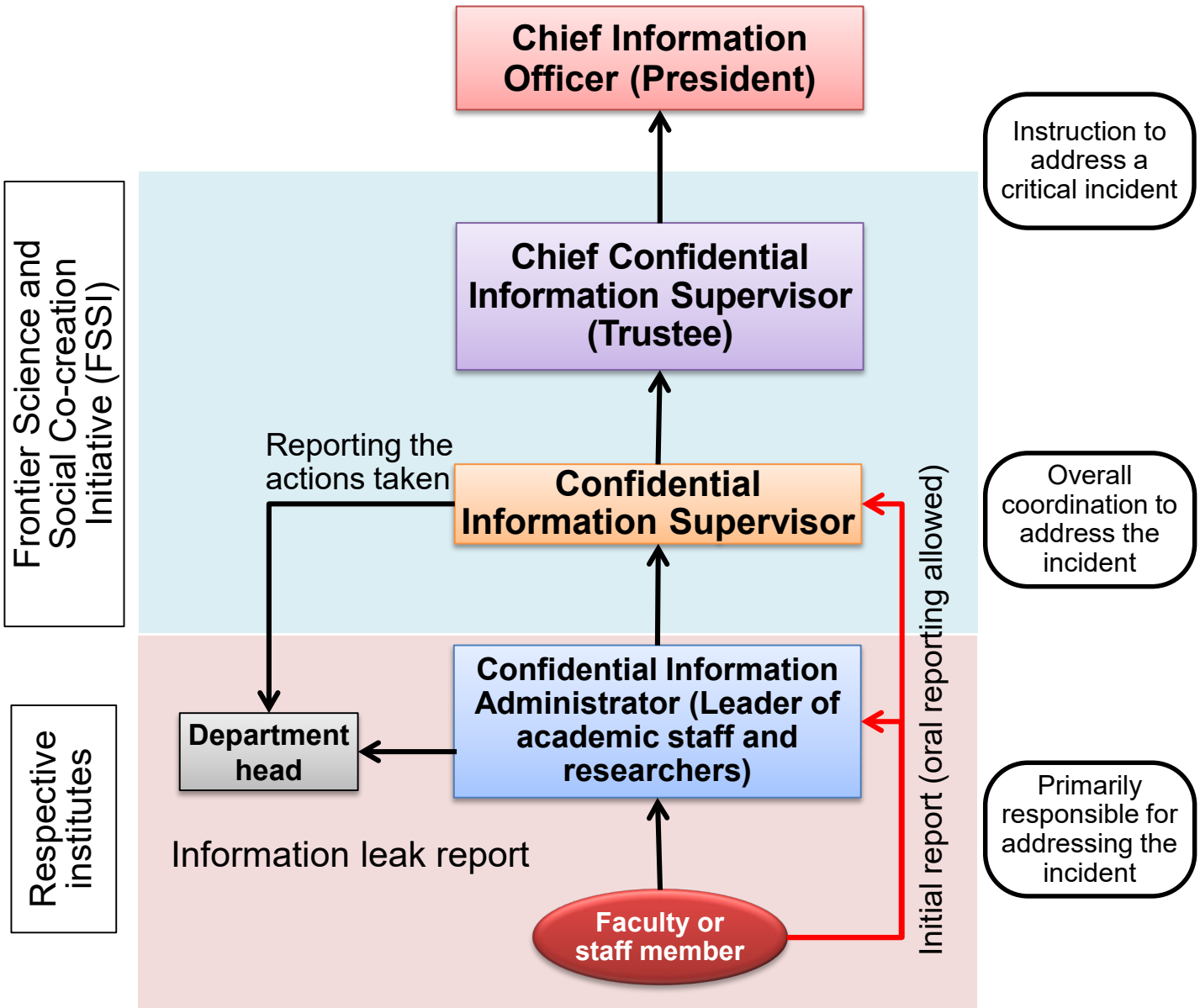
研究協力者（学　生）
所　属：
氏　名（自筆）：　　印

（学　生）
所　属：
氏　名（自筆）：　　印

（※学生が未成年の場合，法定代理人と連名のこと。学生が３名以上の場合，学生欄に準じ本書余白に連記追加すること。）

8. Workflow for Reporting Critical Incidents

- Upon occurrence of a leak of Confidential Information or any other critical incident, faculty and staff must fill out an information leak report and inform the Confidential Information Administrator in line with the following workflow. However, the initial report must be made to the Confidential Information Administrator and the Confidential Information Supervisor as promptly as possible, and may be made orally.
- Based on the information leak report, the Confidential Information Administrator must make a report to his/her boss (the head of the department) and the Confidential Information Supervisor.
- The format of an information leak report is available for download at the URL shown on page 11.



9. Downloads

- Various formatted materials are available for download at the following URL.
  - Confidential Information Register
  - Confidential Information Administration Tools (viewing, copying, printing, photographing, distribution, taking out)
  - Information Leak Report Template

URL: http://o-fsi.w3.kanazawa-u.ac.jp/company/regulation/

10. Inquiries and Information

Confidential Information Supervisor:
Tsuyoshi Mekata, Frontier Science and Social Co-creation Initiative (FSSI)
t-mekata@staff.kanazawa-u.ac.jp

Contact Person:
Kenta Kita, Frontier Science and Social Co-creation Initiative (FSSI)
kenta.kita@staff.kanazawa-u.ac.jp