## **Confidential Information Management Rules**

- Follow the management rules of confidential / strictly confidential information below.
- For each section, check one or multiple appropriate boxes based upon the prior agreement between the companies and Kanazawa University.

Section	Confidential Information	Strictly Confidential Information	
Chief manager	<ul> <li>The faculty or staff member who obtained the confidential information.</li> </ul>	<ul> <li>The faculty or staff member who obtained the strictly confidential information.</li> <li>The faculty member who is the leader of the research team (hereinafter referred to as the "SCI-manager").</li> </ul>	
Labeling	□The confidential information shall be labelled as "Confidential." □Others * ( )	□The strictly confidential information shall be labelled as "Strictly Confidential." □Others * ( )	
	* The labels shall be determined based on the prior agreement between the companies and Kanazawa University.		
Managing the original register	_	<ul> <li>The management is not required.</li> <li>The management by the SCI-manager is required.</li> <li>Making a report to the trustee for research is required.</li> </ul>	
Restriction of entering the storage	<ul> <li>In principle, entering the room in which the confidential information is stored shall be restricted.</li> </ul>	<ul> <li>Entering the room in which the strictly confidential information is stored is restricted.</li> <li>Entering the building or floor in which the strictly confidential information is stored is restricted.</li> <li>Others())</li> </ul>	
Access restriction	•Only faculty members, staff members, collaborative researchers, or collaborative research students are permitted to access the confidential information.	<ul> <li>Only faculty members, staff members, or collaborative researchers are permitted to access the strictly confidential information.</li> <li>Only faculty members, staff members, collaborative researchers, or collaborative research students are permitted to access the strictly confidential information.</li> </ul>	
	•The faculty or staff members who are responsible for managing the confidential information shall designate authorized personnel.	<ul> <li>The faculty or staff members who are responsible for managing the strictly confidential information shall designate authorized personnel.</li> <li>The SCI-manager shall designate authorized personnel.</li> </ul>	
Viewing	<ul> <li>Only the authorized personnel is permitted to view the confidential information.</li> <li>The confidential information must not be viewed by unauthorized personnel.</li> </ul>	<ul> <li>Only the authorized personnel is permitted to view the strictly confidential information.</li> <li>The strictly confidential information must not be viewed by unauthorized personnel.</li> <li>Recording on the management table is required.</li> <li>Making a report to the trustee for research is required.</li> <li>Others())</li> </ul>	

Section		Confidential Information	Strictly Confidential Information
Copying Printing Picture Taking	Authorized personnel	<ul> <li>The faculty or staff members who are responsible for managing the confidential information.</li> <li>Personnel who obtained a permission from the authorized faculty or staff members.</li> </ul>	<ul> <li>The faculty or staff members who are responsible for managing the strictly confidential information.</li> <li>Personnel who obtained a permission from the authorized faculty or staff members</li> <li>The SCI-manager</li> <li>Personnel who obtained a permission from the SCI-manager.</li> </ul>
	Recording Reporting	_	<ul> <li>☐Recording on the management table is required.</li> <li>☐Making a report to the trustee for research is required.</li> </ul>
	Paper documents	•Copies of the paper documents must not be left in the copy machine.	<ul> <li>Copies of the paper documents must not be left in the copy machine.</li> <li>Copying/printing/picture taking shall be recorded using user IDs.</li> <li>Copying/printing/picture taking is prohibited.</li> <li>Others ( )</li> </ul>
	Digitized information	Copies of the digitalized information must not be left in the printer/digital camera/cell phone etc.	<ul> <li>Copies of the digitalized information must not be left in the printer/digital camera/cell phone etc.</li> <li>Printers shall be installed in access controlled rooms.</li> <li>Printers shall be installed in the offices of the faculty or staff members who are responsible for managing the strictly confidential information.</li> <li>Being present in front of the printer while printing is required.</li> <li>Copying/printing/picture taking shall be recorded using user IDs.</li> <li>Copying/printing/picture taking is prohibited.</li> <li>Others ( )</li> </ul>

Section		Confidential Information	Strictly Confidential Information
Distributing	Authorized personnel	<ul> <li>The faculty or staff members who are responsible for managing the confidential information.</li> <li>Personnel who obtained a permission from the authorized faculty or staff members.</li> </ul>	<ul> <li>The faculty or staff members who are responsible for managing the strictly confidential information.</li> <li>Personnel who obtained a permission from the authorized faculty or staff members.</li> <li>The SCI-manager</li> <li>Personnel who obtained a permission from the SCI-manager.</li> </ul>
	Recording Reporting	_	<ul> <li>Recording on the management table is required.</li> <li>Making a report to the trustee for research is required.</li> </ul>
	Paper documents	<ul> <li>The confidential information shall be labelled as "Confidential."</li> <li>An explanation of how to handle the paper documents shall be provided.</li> <li>The paper documents shall be collected back if necessary.</li> <li>The paper documents shall be mailed in a sealed box and marked as "Confidential" if necessary.</li> <li>In principle, some measures for preventing wrong FAX transmissions shall be taken.</li> </ul>	<ul> <li>The strictly confidential information shall be labelled as "Strictly Confidential."</li> <li>An explanation of how to handle the paper documents shall be provided.</li> <li>The paper documents shall be collected back if necessary.</li> <li>The paper documents shall be numbered serially and be collected back after the meeting.</li> <li>The paper documents shall be mailed in a sealed box and marked as "Confidential" if necessary.</li> <li>Some measures for preventing wrong FAX transmissions shall be taken.</li> <li>Being present in front of the FAX machine while faxing is required.</li> <li>Only distributing the paper documents is prohibited.</li> <li>Others ( )</li> </ul>
	Digitized information	<ul> <li>Encrypting or password-protecting is required.</li> <li>The digitalized information and the passwords must be provided in separated emails.</li> </ul>	<ul> <li>Encrypting or password-protecting is required.</li> <li>The digitalized information and the passwords must be provided in separated emails.</li> <li>Distributing the digitalized information is prohibited.</li> <li>Others ( )</li> </ul>

Section		Confidential Information	Strictly Confidential Information
Storing	Paper documents	The paper documents shall be stored in a locked storage.	<ul> <li>The paper documents shall be stored in a locked storage.</li> <li>The paper documents shall be stored in a locked storage separately from any other documents.</li> <li>The paper documents shall be stored in a dedicated locked storage.</li> </ul>
		The faculty or staff members who are responsible for managing the confidential information shall keep the storage key.	<ul> <li>☐ The faculty or staff members who are responsible for managing the strictly confidential information shall keep the storage key.</li> <li>☐ The SCI-manager shall keep the storage key.</li> </ul>
			Others ()
	Digitized information	<ul> <li>Login authentication is required for the information storage device (e.g. PCs)</li> <li>In principle, the confidential information shall be encrypted.</li> </ul>	<ul> <li>Login authentication is required for the information device (e.g. PCs)</li> <li>The strictly confidential information shall be encrypted.</li> <li>Entering the room in which the information storage device is stored is restricted.</li> <li>Entering the building or floor in which the information storage device is stored is restricted.</li> </ul>
		<ul> <li>A permission is necessary to access the network.</li> </ul>	□The strictly confidential information shall be stored on a dedicated information storage device that is not connected to the network.
		•When the confidential information is stored in an information storage device (e.g. USB flash devices), the device shall be password- protected.	<ul> <li>When the strictly confidential information is stored in an information storage device (e.g. USB flash devices), the device shall be password-protected.</li> <li>Storing the strictly confidential information on a electronic device (e.g. a USB flash device) is prohibited.</li> </ul>
			□Others()

Section		Confidential Information	Strictly Confidential Information
Taking the information out from the storage	Authorized personnel	<ul> <li>The faculty or staff members who are responsible for managing the confidential information.</li> <li>Personnel who obtained a permission from the authorized faculty or staff members.</li> </ul>	<ul> <li>The faculty or staff members who are responsible for managing the strictly confidential information.</li> <li>Personnel who obtained a permission from the authorized faculty or staff members.</li> <li>The SCI-manager</li> <li>Personnel who obtained a permission from the SCI-manager.</li> </ul>
	Recording Reporting	_	<ul> <li>□Recording on the management table is required.</li> <li>□Making a report to the trustee for research is required.</li> </ul>
	Paper documents	• The authorized persons, by themselves, shall take the paper documents out from the storage and return in it.	<ul> <li>The authorized persons, by themselves, shall take the paper documents out from the storage and return in it.</li> <li>Taking the paper documents out from the storage is prohibited.</li> <li>Others( )</li> </ul>
	Digitized Information	<ul> <li>When the digitalized information is taken out from the storage, it shall be encrypted or password-protected.</li> </ul>	<ul> <li>□When the digitalized information is taken out from the storage, it shall be encrypted or password-protected.</li> <li>□Taking the digitalized information out from the storage is prohibited.</li> <li>□Others())</li> </ul>
Returning/D	isposing	<ul> <li>The confidential Information shall be returned or disposed of based on the contracts between the companies and Kanazawa University.</li> </ul>	•The strictly confidential Information shall be returned or disposed of based on the contracts between the companies and Kanazawa University.
		• The confidential information shall be disposed of under the direction and responsibility of the faculty or staff members who are responsible for managing the information in such a way that the disposed information can never be accessed by a third party.	☐ The strictly confidential information shall be disposed of under the direction and responsibility of the faculty or staff members who are responsible for managing the information in such a way that the disposed information can never be accessed by a third party.
			☐ The strictly confidential information shall be disposed of under the direction and responsibility of the SCI-manager in such a way that the disposed information can never be accessed by a third party.
Inspection		<ul> <li>The information management officer can conduct an inspection if necessary.</li> </ul>	The information management officer shall conduct an inspection once a year
Cost of special measures		_	<ul> <li>In principle, the cost of special measures for managing the strictly confidential information shall be covered by the companies.</li> </ul>