Okinawa Institute of Science and Technology School Corporation Rules for Personal Information Protection

Approved by the President
October 1, 2024

Article 1 Purposes

The purpose of these Rules is to set forth the necessary matters concerning the protection of Personal Information at the Okinawa Institute of Science and Technology School Corporation (hereinafter, the "Corporation") so as to ensure proper and seamless administrative and business operations of the Corporation, while protecting the rights and interests of an individual, based on the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter, the "Act") and Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013; hereinafter, "Number Act").

Article 2 Ground Policies

1. The Corporation shall handle all Personal Information held by the Corporation in an appropriate manner, in light of the fact that the information should be handled with care under the principle of respect for the autonomy of an individual.
2. The Corporation's officers and employees (including indirect employees; the same applies hereinafter), students and visitors (hereinafter collectively, "Officers and Employees") shall recognize the importance of protection of Personal Information and shall follow these Rules to handle Personal Information.

Article 3 Definitions

These Rules use terms as defined in Article 2, Article 16 and Article 60 of the Act, and Article 2 of the Number Act.

Article 4 Chief Executive Officer

The Chief Executive Officer (hereinafter, the "CEO"), as the head of the Corporation, shall act in compliance with the provisions of the Act, make final decisions on the matters pertaining to the management of the Personal or Other Related Information, and submit reports and applications to the Prime Minister and other competent ministers or to the national Personal Information Protection Commission and other administrative organizations.

Article 5 General Manager for Personal Information Protection

1. A General Manager for Personal Information Protection (hereinafter, the "General Manager") shall be established in the Corporation, as a position to be filled by the Secretary General.
2. The General Manager shall have general responsibility for the management of Personal Information, pseudonymized Personal Information, anonymized Personal Information, information pertaining to individual and other information

which is defined by the Act and is subject to application of the Act and the Number Act (hereinafter, the "Personal or Other Related Information") by the Corporation under the order of the CEO.

3. The General Manager shall develop the Corporation's internal rules and other provisions necessary for the maintenance of these Rules and the implementation of the same.
4. The General Manager shall be responsible for facilitating the internal communication and coordination necessary for the implementation of these Rules and for making decisions on important matters pertaining to the protection of Personal Information.

Article 6 Responsible Officer for Personal Information Protection

1. Each division or other division-level office (hereinafter, simply "Division") shall establish a position of Responsible Officer for Personal Information Protection (hereinafter, the “Responsible Officer”), to be filled by the head of the Division.
2. The Responsible Officer shall provide necessary guidance and supervision regarding the protection of Personal Information in the department under his/her responsibility.
3. The Responsible Officer shall serve concurrently as the Information Asset Manager as defined in PRP Part 17, as a general rule.

Article 7 Personal Information Protection Manager

1. Each section or other section-level office (hereinafter simply "Section") shall establish a position of Personal Information Protection Manager (hereinafter, the “Manager”), to be filled by the head of the Section.
2. The Manager shall provide general administration over the affairs pertaining to the management of the Personal or Other Related Information in the Section and shall be responsible for ensuring appropriate management thereof in the Section.
3. When the Manager has appointed a staff member to be in charge of the affairs pertaining to the Personal or Other Related Information in the Section in accordance with paragraph 1 of the following Article, the Manager shall make a report thereof to the Responsible Officer and shall submit a notification of the designated staff member to the General Manager.

Article 8 Personal Information Protection Administrator

1. Each Section shall establish a position of Personal Information Protection Administrator (hereinafter, the “Administrator”), to be appointed by the Manager of the Section from among Record Management Administrators as set forth in the Rules for Corporate Records Management and University Archive.
2. The Administrator shall assist the Manager and shall be in charge of the affairs pertaining to the management of the Personal or Other Related Information in the Section.

Article 9 Chief Information Officer

1. The Chief Information Officer (hereinafter, the “CIO”) of the Corporation shall be

responsible for the management of the Corporation's information system and cybersecurity program.

2. The CIO shall, working in cooperation with the General Manager, the Responsible Officer and the Manager, undertake the tasks to ensure appropriate management of the Personal or Other Related Information using the Corporation's information system and the development of appropriate information system.
3. The CIO shall be responsible for taking measures necessary for ensuring appropriate management and protection of electronic or magnetic records containing the Personal or Other Related Information, working in cooperation with the General Manager.

Article 10 Chief Information Security Officer

1. The Chief Information Security Officer (hereinafter, the "CISO") of the Corporation shall undertake the duties for establishing information security policies, procedures and management technology in the Corporation and overseeing the effectiveness of information security management measures by means of risk assessment and the like.
2. The CISO shall be responsible for maintaining information security, working in corporation with the General Manager and the CIO.

Article 11 Personal Information Protection Consultative Committee

1. The General Manager may establish a Personal Information Protection Consultative Committee (hereafter, the "Committee") for making decisions on important matters pertaining to the management of the Personal or Other Related Information and for facilitating communication, coordination or the like, and convene a meeting periodically or as necessary.
2. The Committee shall be chaired by the Secretary General and consist of members who are deemed necessary by the chairperson for each agenda from among the following persons:
   (1) CIO;
   (2) CISO;
   (3) General Counsel;
   (4) Dean of the Graduate School;
   (5) Dean of Faculty Affairs
   (6) Vice President for Human Resource;
   (7) Vice President for Communication and Public Relations; and
   (8) Any Responsible Officers, Managers or other Officers and Employees who are concerned with the matter to discuss.
3. Matters necessary for the operation of the Committee shall be set forth by the General Manager.

Article 12 Audit Manager

1. The Corporation shall establish a position of Personal Information Protection Audit Manager (hereafter referred to as the "Audit Manager"), to be filled by the Chief Internal Audit Officer.

2. The Audit Manager shall, periodically or as necessary, conduct audit of the status of the management of the Personal or Other Related Information of the Corporation.

Article 13 Trainings for Officers and Employees

1. The General Manager shall provide trainings necessary for the Corporation's Officers and Employees who are engaged in the handling of the Personal or Other Related Information, to build in-depth understanding of and increase awareness towards the protection of the Personal or Other Related Information.
2. The General Manager shall, working in cooperation with the CIO, provide trainings on the management, operation and security measures of the information system which are necessary for the Corporation's Officers and Employees who are engaged in the affairs pertaining to the management of the information system for handling the Personal or Other Related Information, to facilitate proper management of the Personal or Other Related Information.
3. The General Manager shall implement education and trainings provided onsite for the Managers and the Administrators to ensure appropriate management of the Personal or Other Related Information in the section under their responsibility.
4. The Manager shall take necessary measures for the Officers and Employees to ensure that they will appropriately manage the Personal or Other Related Information, such as by providing them with opportunities to participate in education and trainings conducted by the General Manager.

Article 14 Responsibilities of Officers and Employees

The Officers and Employees shall handle the Personal or Other Related Information in accordance with instructions of the General Manager, the Responsible Officer, the Manager and the Administrator, while in conformity with the purport of the Act and in compliance with all pertinent laws and regulations as well as regulatory provisions.

Article 15 Specifying the Purpose of Use

1. Handling of Personal Information shall be limited to the extent that is necessary for the Corporation to perform the affairs pertaining to the handling thereof, and the Corporation shall specify as much as possible the purpose for which it uses that information (hereinafter, the "Purpose of Use").
2. When altering the Purpose of Use, the Corporation shall not alter it beyond the extent that can be appreciably linked to what it was before the alteration.

Article 16 Restriction Due to Purpose of Use

1. The Corporation shall not handle Personal Information beyond the scope necessary for achieving the Purpose of Use specified pursuant to the provisions of the preceding Article, except for the following cases.
   (1) cases based on laws and regulations;
   (2) cases in which there is a need to protect the life, wellbeing, or property of an individual, and it is difficult to obtain the consent of the identifiable person;
   (3) cases in which there is a special need to improve public wellbeing or promote

healthy child development, and it is difficult to obtain the consent of the identifiable person;

(4) cases in which there is a need to cooperate with a national government organ, local government, or person entrusted thereby with performing the functions prescribed by laws and regulations, and obtaining the consent of the identifiable person is likely to interfere with the performance of those functions;

(5) cases in which the Corporation needs to handle the Personal Information for the purpose of using it in academic research (hereinafter, "Academic Research Purposes") (including cases in which a part of the purpose of handling the Personal Information is for Academic Research Purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests); and

(6) cases in which Personal Information is provided to an academic research institution or the equivalent which needs to handle the Personal Information for Academic Research Purposes (including cases in which a part of the purpose of handling the Personal Data is for Academic Research Purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests).

2. When handling Personal Information beyond the scope of the Purpose of Use specified in the preceding Article, the Corporation shall obtain the identifiable person's consent to do so in advance, except for the cases listed in the preceding paragraph.

Article 17 Prohibition of Inappropriate Use

The Corporation shall not utilize Personal Information in a way that there is a possibility of fomenting or inducing unlawful or unjust act.

Article 18 Proper Acquisition

1. The Corporation shall not acquire Personal Information by deception or other wrongful means.
2. The Corporation shall not acquire Sensitive Personal Information without obtaining the identifiable person's consent in advance, except for the following cases:

(1) cases based on laws and regulations;

(2) cases in which there is a need to protect the life, wellbeing, or property of an individual, and it is difficult to obtain the consent of the identifiable person;

(3) cases in which there is a special need to improve public wellbeing or promote healthy child development, and it is difficult to obtain the consent of the identifiable person;

(4) cases in which there is a need to cooperate with a national government organ, local government, or person entrusted thereby with performing the functions prescribed by laws and regulations, and the consent of the identifiable person is likely to interfere with the performance of those functions;

(5) cases in which the Corporation needs to handle the Sensitive Personal

Information for Academic Research Purposes (including cases in which a part of the purpose of handling the Sensitive Personal Information is for Academic Research Purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests);

(6) cases of acquiring the Sensitive Personal Information from an academic research institution or the equivalent and it is necessary to acquire that information for Academic Research Purposes (including cases in which a part of the purpose of acquiring the Sensitive Personal Information is for Academic Research Purposes, excluding cases in which there is a risk of unjustly infringing on individual rights and interests) (limited to cases in which the Corporation and the academic research institution or the equivalent jointly conduct academic research);

(7) cases in which the Sensitive Personal Information is open to the public by a person identifiable by that information, a national government organ, a local government, an academic research institution or the equivalent, a person set forth in each item of Article 57, paragraph 1, or other person prescribed in Article 6 of the Enforcement Regulations for the Act on the Protection of Personal Information (Personal Information Protection Commission Regulation No. 3 of 2016; hereinafter, "Enforcement Rules"); and

(8) other cases prescribed in Article 9 of the Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003; hereinafter, the "Enforcement Order") as equivalent to the cases set forth above.

Article 19 Notification of a Purpose of Use when Acquiring Personal Information

1. Unless the Purpose of Use has already been disclosed to the public, the Corporation shall promptly notify the identifiable person of that Purpose of Use or disclose this to the public once it has acquired Personal Information.
2. Notwithstanding the provisions of the preceding paragraph, the Corporation shall explicitly specify the Purpose of Use to the identifiable person, before acquiring their Personal Information which appears in a written agreement or other document (this includes an electronic or magnetic record; hereinafter the same applies in this paragraph) as a result of concluding an agreement with the person; or acquiring their Personal Information which appears in a document, directly from the person in question; provided, however, that this does not apply if there is an urgent necessity to dispense with this requirement in order to protect the life, wellbeing, or property of an individual.
3. If the Corporation alters the Purpose of Use, it shall notify identifiable persons of the altered Purpose of Use or disclose this to the public.
4. The provisions of the preceding three paragraphs do not apply to the following cases:
   (1) notifying the identifiable person of the Purpose of Use or disclosing this to the public is likely to harm the life, wellbeing, property, or other rights or interests of the identifiable person or a third party;

(2) notifying the identifiable person of the Purpose of Use or disclosing this to the public is likely to harm the rights or legitimate interests of the Corporation;
(3) it is necessary for the business to cooperate with a national government organ or a local government in performing the functions prescribed by laws and regulations, and notifying the identifiable person of the Purpose of Use or disclosing this to the public is likely to interfere with the performance of those functions;
(4) the Purpose of Use is considered to be obvious, in light of the circumstances in which the Personal Information is acquired.

Article 20 Maintaining the Accuracy of Data

1. The Officers and Employees shall endeavor to keep the contents of Personal Data accurate and up to date, within the scope necessary for achieving the Purpose of Use, and delete the Personal Data without delay if they no longer require it.
2. The Officers and Employees shall make corrections in accordance with instructions of the Manager if they discover an error, etc., in the contents of Personal Data
3. When Personal Data or media (including those built into terminals and servers) on which Personal Data are recorded are no longer needed, the Officers and Employees shall delete said Personal Data or dispose of said media in a manner that makes said Personal Data unrecoverable or indecipherable, in accordance with instructions of the Manager.

Article 21 Measures for Managing the Security of Personal Data

1. The General Manager shall take the necessary and appropriate measures for managing the security of Personal Data including preventing the leakage, loss or damage of the Personal Data they handle, and ensure that the Employees comply with such measures.

Article 22 Operations Outsourcing, etc.

1. When outsourcing operations pertaining to the handling of Personal Data, the Manager shall take the necessary measures, such as verifying the management capability of the Personal Data at the time of selection.
2. The Manager shall draft documents of contract for outsourcing operations pertaining to the handling of Personal Data in accordance with guidelines separately stipulated by the CISO, in addition to these Rules.
3. When executing a contract for outsourcing operations as set forth in the preceding paragraph with a selected third party, the Manager shall explicitly recite the following matters in the contract and shall confirm in writing the necessary matters, such as the management and implementation systems to be carried out by the supervisor and the workers of the outsourced party and matters concerning inspection of the status of the management of Personal Information.
   (1) taking measures equivalent to the security control measures to be taken by the Corporation;
   (2) obligations such as maintaining confidentiality of Personal Data and

prohibition of use of Personal Data for a purpose other than the Purpose of Use;

(3) matters concerning conditions pertaining to subcontracting, such as restrictions on subcontracting or prior approval, including the cases where the sub-contractor is a subsidiary (which means a subsidiary as defined in Article 2, item 3 of the Companies Act (Act No. 86 of 2005)) of the outsourced party.

(4) matters concerning restrictions on reproduction, etc., of Personal Data;

(5) matters concerning measures to be taken in response to the event of leakage, etc., of Personal Data (including, but not limited to, reporting by the outsourced party to the Manager of the occurrence of the leakage, etc.);

(6) matters concerning deletion of Personal Data and return of media at the end of outsourcing;

(7) termination of contract, liability for damages, and other necessary matters in the event of a breach; and

(8) in addition to the matters prescribed in the preceding items, matters necessary due to the nature of the handling of Personal Data to be outsourced.

4. The Manager shall, when outsourcing operations pertaining to the handling of Personal Data, confirm the management and implementation systems and the status of Personal Information management in the outsourced party at least once a year, in principle, by on-site inspection, suitably for the contents and the volume of the Personal Data pertaining to the outsourced works, such as confidentiality thereof.
5. In cases where operations pertaining to the handling of Personal Data are subcontracted by the outsourced party, the Manager shall have the outsourced party take the measures of paragraphs 1 and 3, and shall implement the measures in the preceding paragraph through the outsourced party or by the outsourced party itself, suitably for the contents of Personal Data pertaining to the operations to be subcontracted, such as confidentiality thereof. The same applies to any subsequent subcontract to be performed by any subsequent subcontractor with respect to the operations pertaining to the handling of Personal Data.
6. The Manager shall, when having an indirect employee handle Personal Data, explicitly recite in an indirect employment contract with the indirect employee matters concerning the handling of Personal Data such as the confidentiality obligation.

Article 23 Access Restriction

1. The Manager shall, working in cooperation with the CIO, restrict the extent of the Officers and Employees who are authorized to access Personal Data and the contents of the authorization to the extent that is just necessary to the operations to be performed by said Officers and Employees, suitable for the contents of the Personal Data such as confidentiality (including easiness of individual identification according to anonymity levels, presence or absence of Sensitive Personal Information, the nature and the degree of damage that may have been caused by leakage or the like; the same applies hereinafter).
2. Unauthorized Officers and Employees shall not access Personal Data.

3. Even the Officers and Employees who are authorized to access may not access Personal Data for a purpose other than carrying out the operations.

Article 24 Limitations to Reproduction, etc.

1. Even when the Officers and Employees handle Personal Data for a purpose other than carrying out the operations, the Manager shall limit the cases where the following acts can be performed, according to the contents of the retained Personal Information such as confidentiality:
   (1) reproduction of Personal Data;
   (2) transmission of Personal Data;
   (3) external delivery or taking out of media recording Personal Data; and
   (4) other acts which may cause impediments in appropriate management of Personal Data.
1. The Officers and Employees shall, when performing any of the acts listed in the preceding paragraph, obtain permission from the Manager.

Article 25 Management of Media

The officers and Employees shall store media recording Personal Data in a place designated by the Manager and in accordance with instructions of the Manager and, when finding it necessary, store them in a fireproof safe or take measures such as lock the cabinet.

Article 26 Restrictions on Provision of Personal Data to Third Parties

1. The Corporation shall not provide Personal Data to a third party without obtaining the identifiable person's consent in advance, except for the following cases:
   (1) cases based on laws and regulations;
   (2) cases in which there is a need to protect the life, wellbeing, or property of an individual, and it is difficult to obtain the consent of the identifiable person;
   (3) cases in which there is a special need to improve public wellbeing or promote healthy child development, and it is difficult to obtain the consent of the identifiable person;
   (4) cases in which there is a need to cooperate with a national government organ, local government, or person entrusted thereby with performing the functions prescribed by laws and regulations, and obtaining the consent of the identifiable person is likely to interfere with the performance of those functions;
   (5) cases in which to provide the Personal Data for the purpose of publication of academic research results or teaching is unavoidable (excluding cases in which there is a risk of unjustly infringing on individual rights and interests);
   (6) cases in which the Corporation needs to provide the Personal Data for the Academic Research Purposes (including cases in which a part of the purpose of handling the Personal Data is for Academic Research Purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests) (limited to cases in which the Corporation and the third party jointly conduct academic research);

(7) cases in which the third party is an academic research institution or the equivalent, and the third party needs to handle the Personal Data for Academic Research Purposes (including cases in which a part of the purpose of handling the Personal Data is for Academic Research Purposes, and excluding cases in which there is a risk of unjustly infringing on individual rights and interests).

2. In the following cases, a person receiving the Personal Data shall be excluded from the scope of the third party in the context of provision of Personal Data according to the preceding paragraph:
   2. cases where Personal Data are provided when the Corporation outsources all or part of the handling of the Personal Data within the extent necessary for achieving the Purpose of Use;
   3. cases where Personal Data to be used jointly with a specific party are provided to said specific party, when matters, including indication of such joint use and items of Personal Data which are subjected to the joint use, the extent of persons who use jointly and the Purpose of Use by the persons who use the Personal Data, and name and address of the person who is responsible for the management of the Personal Data, and, if the person is a judicial person, name of the representative thereof, have already been notified to the identifiable person pertaining to the Personal Data or have been placed in a state that can be readily known to the identifiable person in advance.
3. The Corporation shall, when any of name and address of the person who is responsible for the management of the Personal Data, and, if the person is a judicial person, name of the representative thereof as set forth in the preceding paragraph has been changed, promptly notify the identifiable person pertaining to the Personal Data or place in a state that can be readily known to the identifiable person, or, when the Purpose of Use by the persons who use the Personal Data or the person who is responsible for the management of the Personal Data as set forth in the same paragraph is to be changed, notify the identifiable person pertaining to the Personal Data or place in a state that can be readily known to the identifiable person in advance.

Article 27 Restrictions on the Provision of Personal Data to Third Parties in Foreign Countries

1. Notwithstanding the preceding Article, when the Corporation provides Personal Data to a third party in a foreign country (meaning a country or region located outside the territory of Japan), the Corporation shall obtain an identifiable person's prior consent to the effect that the person approves the provision to the third party in a foreign country, except for the following cases:
   (1) cases falling under any of the items of paragraph 1 of the preceding Article;
   (2) cases when Personal Data is provided to a third party located in a country prescribed in Article 15 of the Enforcement Rules as a foreign country that has a system for the protection of Personal Data that is recognized to be of a level comparable to that of Japan in protecting the rights and interests of individual;
   (3) cases when Personal Data is provided to a person who has established a system that conforms to the standards prescribed in Article 16 of the Enforcement

Rules as those being necessary for continuously taking measures equivalent to the measures to be taken by business operators handling Personal Information with respect to the handling of Personal Data;

2. When intending to obtain the identifiable person's consent pursuant to the provisions of the preceding paragraph, the Corporation shall provide the person with information on the national system on the Personal Information protection in the foreign country, the measures that the third party takes for the protection of Personal Information, and other information that is to serve as a reference to the person, pursuant to Article 17 of the Enforcement Rules, in advance of the consent.
3. When having provided Personal Data to a third party (limited to a person establishing a system prescribed in paragraph 1) in a foreign country, the Corporation shall take necessary measures to ensure continuous implementation of the equivalent measures by the third party, and provide information on necessary measures to the person at the request of said person, pursuant to Article 18 of the Enforcement Rules.

Article 28 Preparing of Records on Provision of Personal Data to Third Parties

1. When the Corporation has provided Personal Data to a third party, the Manager shall prepare a record pursuant to Article 19 of the Enforcement Rules on the date of the provision of the Personal Data, the name of the third party, and other matters prescribed in Article 20 of the Enforcement Rules; provided, however, that this does not apply to cases in which the provision of Personal Data falls under any of the items of Article 26, paragraph 1 or paragraph 2 (or any of the items of Article 26, paragraph 1, in cases of a provision of Personal Data under paragraph 1 of the preceding Article).
2. The Manager shall maintain the record of the preceding paragraph for at least a period of 3 years (in cases prescribed in Article 21, paragraph 1 or paragraph 2 of the Enforcement Rules, for a period as specified in the paragraph) from the day on which the record was prepared.

Article 29 Confirmation on Receiving Personal Data from a Third Party

1. When the Corporation receives Personal Data from a third party, the Manager shall confirm matters set forth in the following pursuant to Article 21 of the Enforcement Rules.; provided, however, that this does not apply to cases in which the provision of Personal Data falls under any of the items of Article 26, paragraph 1 or paragraph 2:
   (1) the name and address of the third party and, if the third party is a corporation, the name of its representative;
   (2) background of the acquisition of the Personal Data by the third party.
2. When the Manager conducts confirmation under the preceding paragraph, the third party of the preceding paragraph shall not falsify against the Corporation any matters pertaining to the confirmation.
3. When having given confirmation of the preceding paragraph, the Manager shall prepare a record pursuant to Article 23 of the Enforcement Rules on the date of

receipt of the Personal Data, matters pertaining to the confirmation, and other matters prescribed in Article 24 of the Enforcement Rules.

4. The Manager shall keep the record of the preceding paragraph, as a basic rule, for a period of at least 3 years (in the case of Article 25, item 1 or item 2 of the Enforcement Rules, for the period specified therein) from the day on which the record was prepared.

Article 30 Restrictions on the Provision of Information Related to Personal Information to Third Parties

1. Except cases set forth in each item of Article 26, paragraph 1, if it is assumed that a third party acquires information related to Personal Information (limited to those compiled in a database or the equivalent of information related to Personal Information; the same applies hereinafter) as Personal Data, the Corporation shall not provide the information related to Personal Information to the third party without confirming the matters set forth as follows pursuant to Article 26 of the Enforcement Rules:
   (1) the identifiable person's consent to the effect that the person approves of the third party acquiring information related to Personal Information as Personal Data that can identify the person from the Corporation has been obtained;
   (2) for provision to a third party in a foreign country, when the Corporation intends to obtain the identifiable person's consent of the preceding item, information on the national system for Personal Information protection in the foreign country, information on the measures that the third party takes for the protection of Personal Information, and other information that serves as a reference to the person have been provided in advance to the person pursuant to Article 17 of the Enforcement Rules.
2. The provisions of Article 27, paragraph 3 apply mutatis mutandis to cases in which the Corporation provides information related to Personal Information pursuant to the provisions of the preceding paragraph. In this case, the phrase ", and provide information on the necessary measures to the identifiable person at the request of said person," in Article 27, paragraph 3 is replaced with ",".
3. The provisions of paragraphs 2 and 3 of the preceding Article apply mutatis mutandis to cases in which the Corporation conducts confirmation pursuant to the provisions of paragraph 1. In this case, the phrase "received" in paragraph 3 of said Article is replaced with "provided."

Article 31 Responsibilities as an Academic Research Institution or the equivalent

With regard to the handling of Personal Information for Academic Research Purposes, the Corporation shall comply with the provisions of the Act, take necessary measures to ensure the appropriateness of such handling, and endeavor to publicize the details of such measures.

Article 32 Preparation of Pseudonymized Personal Information

1. When preparing pseudonymized Personal Information (limited to those compiled

in a pseudonymized Personal Information database or the equivalent; the same applies hereinafter), the Corporation shall process Personal Information in accordance with standards prescribed in Article 31 of the Enforcement Rules as those necessary to make it impossible to identify a specific individual unless collated with other information.

2. When having prepared pseudonymized Personal Information or having acquired pseudonymized Personal Information and deleted or other related information (meaning information related to identifiers or their equivalent and individual identification codes that were deleted from Personal Information used to prepare the pseudonymized Personal Information, and the means of processing carried out pursuant to the provisions of the preceding paragraph) related to the pseudonymized information, the Corporation shall take measures for the management of the security of deleted or other related information in accordance with standards prescribed in Article 32 of the Enforcement Rules as those necessary to prevent leakage of deleted or other related information.
3. Notwithstanding the provision of Article 16 and except cases based on laws and regulations, the Corporation shall not handle pseudonymized Personal Information (limited to Personal Information; hereinafter the same applies in this Article) beyond the necessary scope to achieve the Purpose of Use specified in Article 15, paragraph 1.
4. To apply the provisions of Article 19 to the pseudonymized Personal Information, the phrase "notify the identifiable person of that Purpose of Use or disclose this to the public" in paragraphs 1 and 3 of that Article is replaced with "disclose that Purpose of Use"; the phrase "notifying the identifiable person of the Purpose of Use or disclosing this to the public" in the provisions of items (1) through (3) of paragraph 4 of that Article is replaced with "disclosing the Purpose of Use".
5. The Corporation shall endeavor to erase Personal Data that constitutes pseudonymized Personal Information and deleted or other related information without delay when utilization of the Personal Data and the deleted or other related information has become unnecessary. In this case, the provisions of Article 20 do not apply.
6. Notwithstanding the provisions of Article 26, paragraph 1 and Article 27, and except cases based on laws and regulations, the Corporation shall not provide a third party with Personal Data that constitutes pseudonymized Personal Information. In this case, the term "each preceding paragraph" in Article 26, paragraph 2 is replaced with "Article 32, paragraph 6"; the phrase "notifies the person, or makes the information readily accessible to the person " in item (2) of that paragraph is replaced with "disclose "; the phrase "notify the person or make this readily accessible to the person " in paragraph 3 is replaced with "disclose this "; the phrase "any of the items of Article 26, paragraph 1 or paragraph 2 (or any of the items of Article 26, paragraph 1, in cases of a provision of Personal Data under paragraph 1 of the preceding Article)" in the proviso of Article 28, paragraph 1) and the term "any of the items of Article 26, paragraph 1 or paragraph 2" in the proviso of Article 29, paragraph 1 are replaced with "cases based on laws and regulations or any of the items of Article 26, paragraph 2".

7. The Corporation, in handling that information, shall not collate the pseudonymized Personal Information with other information in order to identify a person identifiable by Personal Information that was used to prepare the pseudonymized Personal Information.
8. The Corporation, in handling that information, shall not use contact addresses and other information contained in the pseudonymized Personal Information to make a call, send by post, transmit by using electronic or magnetic means or other methods as prescribed in Article 41, paragraph 8 of the Act, or visit a residence.
9. The provisions of Article 15, paragraph 2, Article 56 and Articles 58 do not apply to pseudonymized Personal Information, Personal Data that constitutes pseudonymized Personal Information, and Personal Data that constitutes pseudonymized Personal Information
10. The provisions of the preceding paragraphs shall apply mutatis mutandis to the case where a person who has been outsourced with the handling of pseudonymized processed information (including outsourcing with at least one level of subcontractors) by the Corporation performs the outsourced work.

Article 33 Restrictions on Provision of Pseudonymized Personal Information to Third Parties

1. Except in cases based on laws and regulations, the Corporation shall not provide pseudonymized Personal Information (excluding those that constitute Personal Information; the same applies hereinafter in this Article) to a third party.
2. The provisions of Article 26, paragraph 2 apply mutatis mutandis to a person receiving pseudonymized Personal Information. In this case, the phrase "when notifies the person, or makes the foregoing information readily accessible to the person " in item (2) of the paragraph is replaced with "when discloses ", and the phrase "unless notifies the person or makes this readily accessible to the person " in item (3) is replaced with "discloses this ".
3. The provisions of Articles 21 through 25 and the preceding Article, paragraph 7 and paragraph 8 apply mutatis mutandis to the handling of pseudonymized Personal Information. In this case, the phrase "leakage, etc." in Article 21 is replaced with "leakage"; and the term "not" in preceding Article, paragraph 7 is replaced with "neither acquire deleted or other related information, nor".

Article 34 Handling of Specific Personal Information

The handling for the Specific Personal Information shall be stipulated by the Corporation’s Rules on Handling Individual Numbers and Specific Personal Information.

Article 35 Handling of Anonymously Processed Information held by Administrative Agencies, etc.

The handling of the Anonymously Processed Information Held by Administrative Agencies, etc. shall be stipulated by the Corporation’s Rules on Provision, etc. of Anonymously Processed Information Held by Administrative Agencies, etc.

Article 36 Personal Information Files

1. Upon possession of Personal Information file, the Manager shall register it to the Personal Information File Registration List (hereafter, the “PIPL) of the Corporation.
2. The Manager shall promptly update the registration information in the PIPL when there is a change in the contents of the Personal Information File registered in the PIPL.

Article 37 Preparation and Publication of Personal Information File Registers

1. The Corporation shall prepare and make public a register on Personal Information Files, with descriptions of the following matters on each of the Personal Information Files.
   (1) the name of the Personal Information File;
   (2) the name of the organ and the name of the organizational section in charge of the affairs in which the Personal Information File will be used;
   (3) the Purpose of Use of the Personal Information File;
   (4) particulars recorded in the Personal Information File (hereinafter, the "Recorded Particulars") and the scope of individuals (hereinafter, the "Scope of Record") that are recorded in the Personal Information File as an identifiable person (limited to those who can be identified through a search without another individual's name, date of birth, or other identifiers or their equivalent; the same applies hereinafter);
   (5) the means of acquiring the Personal Information recorded in the Personal Information File (hereinafter, the "Recorded Information");
   (6) if the Recorded Information contains Sensitive Personal Information, an indication as such;
   (7) if the Recorded Information is routinely provided to a party external to the Corporation, the name of that party;
   (8) the name and address of the organization that officially receives requests for disclosure, correction, or suspension of use of the Retained Personal Information;
   (9) if any special procedure is prescribed by law for a request pertaining to the correction or suspension of use of the retained Personal Information, an indication as such;
   (10) other matters prescribed in Article 21, paragraph 6 of the Enforcement Order.
2. The Rules and Compliance Section shall develop, maintain, and make public the Personal Information File Register. However, a Personal Information File falling under any of the following items shall not be listed in the Personal Information File Register.
   (1) a Personal Information File recording information concerning personnel affairs, wages, welfare benefits, or any equivalent matters of the Officers and Employees (including a Personal Information file concerning an employee recruitment examination conducted by the Corporation);
   (2) a Personal Information File exclusively used for the purpose of experimental

computer processing;

(3) a Personal Information File which contains all or a part of the Recorded Information contained in another Personal Information file subject to the publication prescribed in the preceding paragraph, if its Purpose of Use, Recorded Particulars, and Scope of Record are within the scope of those subject to that publication;

(4) a Personal Information File that only contains Personal Information to be erased within 1 year;

(5) a Personal Information File that is used for sending materials or any goods or money or for making communications necessary for business operations, which only contain the names, addresses and other necessary details of the recipients of the sending or the communication;

(6) a Personal Information File that any of the Officers and Employees prepares or acquires based on his/her own initiative for Academic Research Purposes, in which the Recorded Information is used exclusively for the Academic Research Purposes;

(7) a Personal Information File with the number of identifiable persons recorded therein is less than 1000;

(8) other Personal Information Files as prescribed in Article 20, paragraph 3 and Article 21, paragraph 7 of the Enforcement Order.

3. The Manager shall inform the Rules and Compliance Section to update the Personal Information File Register when a Personal Information File to be registered in the Personal Information File Register is newly received or when it is necessary to change any matters registered therein.

Article 38 Access Control

1. The Manager shall, in cooperation with the CIO, take necessary measures for access control, such as setting up a function to identify authorization using the Personal or Other Related Information (limited to those handled by information systems, the same applies hereinafter up to Article 52 (excluding Article 50)) (hereinafter, "Authentication Function"), such as passwords, etc. (passwords, IC cards, biometric information, etc.; the same applies hereinafter), in accordance with confidentiality and other contents of such information.
2. When taking the measures of the preceding paragraph, the Manager shall, in cooperation with the CIO, develop any rules for the management of passwords, etc. (including regular and as-necessary reviews) and take any required security measures in order to prevent skimming or other means of stealing passwords, etc.

Article 39 Access Records

1. The Manager shall, in cooperation with the CIO, take necessary measures to record the status of access to the said Personal or Other Related Information suitably for the confidentiality and other contents of such information, and maintain the records (hereinafter, "Access Records") for a certain period of time and to analyze the Access Records on a regular basis and on an as-needed basis.
2. The Manager shall, in cooperation with the CIO, take any necessary measures to

prevent modification, theft, or unauthorized deletion of the Access Records.

Article 40 Monitoring of Access

The Manager shall, in cooperation with the CIO, take necessary measures to monitor inappropriate access to the Personal or Other Related Information, which are suitable for the confidentiality, contents, and volume of such information, such as setting a function to display a warning when a certain amount of information which contains or is likely to contain the Personal or Other Related Information is downloaded from the information system, and periodically checking such settings.

Article 41 Settings of Administrative Authority

The Manager shall take necessary measures suitable for the confidentiality and other contents of the Personal or Other Related Information, such as minimizing the extent of privileges of the information system administrator in order to minimize damage in the event of unjustifiable theft of the privileges and to prevent unauthorized manipulation from inside the Corporation.

Article 42 Prevention of Unauthorized External Access

The Manager shall, in cooperation with the CIO, take necessary measures, such as route control by setting up a firewall, to prevent unauthorized access from outside to information systems that handle the Personal and Other Related Information.

Article 43 Prevention of Leakage by Malware

The Manager shall, in cooperation with the CIO, take necessary measures (including keeping the installed software up to date) to eliminate publicly-known vulnerabilities of software and to prevent infection by recognized malware, in order to prevent leakage of the Personal or Other Related Information due to malware.

Article 44 Processing of Personal or Other Related Information in Information Systems

1. When carrying out an action such as reproduction of the Personal or Other Related Information for temporal processing, the Officers and Employees shall limit the Personal or Other Related Information subject to such processing to the extent that is just necessary for the processing and shall promptly delete any information that is no longer needed upon completion of the processing.
2. In the case of the preceding paragraph, the Manager shall confirm the situation as necessary with a focus on the state of implementation of deletion, etc. of the Personal or Other Related Information, suitably for the confidentiality and other contents of such information.

Article 45 Encryption

1. The Manager shall, in cooperation with the CIO, take necessary measures to encrypt the Personal or Other Related Information, suitably for the confidentiality and other contents of such information.
2. The Employees shall carry out encryption appropriately in line with the preceding

paragraph on the Personal or Other Related Information that they process based on these security measures, suitably for the confidentiality and other contents of such information.

Article 46 Restrictions on Connection of Devices and Media with Recording Functions

The Manager shall, in cooperation with the CIO, take necessary measures to prevent leakage, etc. of the Personal or Other Related Information, suitably for the confidentiality and other contents of such information, by restricting connection to smartphones, USB memory sticks, and other devices and media with recording functions to information system terminals, etc. (including measures for updating said devices), etc.

Article 47 Limitations for Terminals

The Manager shall take necessary measures to restrict terminals at which the Personal or Other Related Information may be processed suitably for the confidentiality and other contents of such information.

Article 48 Theft Prevention, etc. for Terminals

1. The Manager shall take necessary measures to prevent theft and/or loss of terminals, such as fixing the terminals and keeping the offices locked.
2. The Officers and Employees shall not remove terminals from the Corporation premises or bring in terminals from outside except when the Manager acknowledges necessity.

Article 49 Viewing Prevention against Third Party

The Officers and Employees shall take necessary measures suitable for the conditions of use, to prevent third parties from viewing the Personal or Other Related Information when using terminals, such as never leaving information systems without logging off.

Article 50 Information Verification

The Officers and Employees shall perform verification in accordance with the level of importance of the Personal or Other Related Information handled by information systems, such as verification of input against original document descriptions, confirmation of the contents of the Personal or Other Related Information before and after processing, verification against the existing Personal or Other Related Information and the like.

Article 51 Backup

The Manager shall, in cooperation with the CIO, take necessary measures to create backups and provide decentralized storage, suitable for the level of importance of the Personal or Other Related Information.

Article 52 Management of Information System Design Documents, etc.

The Manager shall take necessary measures to store, reproduce, dispose of and the like the information system design documents, schematic diagrams, and other documentation for information systems related to the Personal or Other Related Information, in order to maintain confidentiality from external parties.

Article 53 Area Access Control

1. The Manager shall, in cooperation with the CIO, designate authorized persons who are allowed to enter the core server room and other areas in which equipment handling the Personal or Other Related Information is located (hereinafter, the "Server Room, etc. ") and take necessary measures to check the purpose of entry, take room access logs, identify external personnel, monitor external personnel entry by physical on-site presence of the Officers and Employees or through monitoring equipment when external personnel is granted access, and restrict or inspect the bringing in, use, and taking out of external electromagnetic media. If there is a facility designated for the storage of media that contains the Personal or Other Related Information, the Manager shall take similar measures when finding it necessary.
2. The Manager shall, in cooperation with the CIO, take measures to facilitate control of the server room access by designating entrances and exits of the Server Room, etc., and restricting location signs when finding it necessary.
3. The Manager shall, in cooperation with the CIO, when finding it necessary in performing the access control to the Server Room, etc., and storage facilities, set access authentication functions, develop rules for the management of passwords, etc. (including regular and as-necessary reviews) and take necessary measures to ensure prevention of skimming or stealing of passwords, etc.

Article 54 Management of Server Room, etc.

1. The Manager shall, in cooperation with the CIO, take measures in case of unauthorized access from external parties, such as installing locking devices, alarms, and monitoring equipment in the Server Room, etc.
2. The Manager shall, in cooperation with the CIO, take measures against natural disasters, etc., such as providing the Server Room, etc. with anti-seismic, fireproofing, smoke proofing, and waterproofing equipment, ensuring reserve power supplies for servers and other equipment and preventing damage to wiring.

Article 55 Report of Incidents

1. When Officers and Employees recognize the occurrence or signs of an incident of leakage, etc. of any Personal or Other Related Information or a fact or sign that a person in charge has violated the provisions of related laws, regulations, rules, etc., or any other incident that may present a security concern, Employees shall immediately report or consult with the Manager in charge of the relevant Personal or Other Related Information and the General Manager.
2. Upon receiving a report of the preceding paragraph, the Manager shall immediately report it to the Responsible Officer. The Manager shall also confirm that the report has been notified to the General Manager.

3. Upon receiving a report of paragraph 1, the Manager, in cooperation with the CISO, shall immediately take necessary measures to prevent the spread of damage, such as unplugging the LAN cables of terminals suspected of unauthorized access from outside or infection due to malware (including causing the Officers and Employees to do so) and shall investigate the circumstances under which the incident occurred and submit a report to the General Manager. However, this does not preclude submission of additional reports on matters that come to light after the report has been submitted.
4. The General Manager shall instruct the Manager to notify identifiable persons based on the report of the preceding paragraph.
5. Based on the instruction of the preceding paragraph, the Manager shall promptly notify identifiable persons of the summary of the situation, the items of the retained Personal Information, the cause, the existence or non-existence of secondary damage or the threat thereof, and the details thereof, as well as other informative matters, to the extent necessary for the protection of the rights and interests of the identifiable persons. However, this does not apply in cases where it is difficult to notify an identifiable person of that occurrence, and the necessary alternative measures are taken to protect the person's rights and interests. Such notification shall also be made to other persons concerned or organizations to which the identifiable person belongs, as necessary.
6. Upon receiving a report of paragraph 1, the General Manager, in cooperation with the CISO, shall determine whether the incident is minor or not, after confirming the details of the incident and the damage.
7. When an incident has been determined to be minor in the preceding paragraph, the General Manager shall alert the Officer(s) responsible for the management of the case, including prevention of recurrence.
8. If an incident that is not deemed minor in paragraph 5 has been occurred, the General Manager shall promptly report to the CEO of the occurrence of the incident.

Article 56 Reporting, etc., of Leaks

1. The General Manager shall, when leakage, loss or damage, or any other situations concerning the security of the Personal Data handled by the Corporation which fall under any of the following items as those that are highly likely to harm the rights and interests of individuals occurs, report the Personal Information Protection Commission thereof, pursuant to Article 8 of the Enforcement Rules. However, this does not apply to cases in which the Corporation was entrusted by another business handling Personal Information or an administrative entity to perform all or part of the handling of the Personal Data, and has notified said business handling Personal Information or administrative entity of the situation pursuant to Article 9 of the Enforcement Rules.
   (1) situations in which leakage, etc. of Personal Data containing Sensitive Personal Information (excluding data for which advanced encryption or other measures necessary to protect the rights and interests of individuals have been taken; the same applies hereinafter in this Article) has occurred or is likely to

have occurred;
(2) situations in which leakage, etc. of Personal Data that may cause property damage by unauthorized use has occurred or is likely to have occurred;
(3) situations in which the leakage, etc. of Personal Data which may have been caused for a wrongful purpose has occurred or is likely to have occurred;
(4) situations in which leakage, etc. of Personal Data with the number of identifiable persons whose Personal Data have been leaked, etc., is more than 1,000 has occurred or is likely to have occurred.

2. When making the reporting of the preceding paragraph, the General Manager shall, immediately after becoming aware of the situation prescribed in each item of the preceding Article, report the following matters concerning the situation (limited to those that have been recognized at the time the report is required) to the national Personal Information Protection Commission.
(1) Summary
(2) items of Personal Data that have been or may have been leaked, etc.
(3) number of individuals whose Personal Data have been or may have been leaked
(4) cause
(5) existence or non-existence of secondary damage or the threat thereof, and the details thereof
(6) status of response to the identifiable person(s)
(7) status of public disclosure
(8) measures taken to prevent recurrence
(9) other items of reference
3. In the case of the preceding paragraph, the General Manager shall report the national Personal Information Protection Commission of the matters stipulated in the items of the preceding paragraph pertaining to the situation within 30 days (within 60 days in the case where the situation is prescribed in paragraph 1, Item (3)) from the date of becoming aware of the situation.

Article 57 Recurrence Prevention Measures

1. The Manager shall analyze the case of the incident and promptly submit a final report including measures to prevent recurrence to the General Manager.
2. The Manager, together with the CISO and other relevant employees, shall implement the recurrence prevention measures reported in the preceding paragraph.

Article 58 Public Announcement, etc.

1. The General Manager shall promptly make public the facts and measures to prevent recurrence, etc., based on the final report of paragraph 1 of the preceding Article.
2. The General Manager shall promptly provide the relevant ministries and agencies and the Personal Information Protection Commission with information on the content, background, damage, etc. of the incident to be made public pursuant to the preceding paragraph.

3. When the General Manager has made a report of paragraph 1, he/she shall report the contents of the report to the Council Committee.
4. When the General Manager has made a report of paragraph 1, he/she shall submit a final report on the incident to the CEO.

Article 59 Audit

The Audit Manager shall perform regular and as-necessary audits (including independent audits by external auditors; the same applies hereinafter) of the operation of the management of the Personal or Other Related Information in the Corporation to verify the appropriate management of such information and report the General Manager of the results.

Article 60 Inspection

1. The General Manager may request the Responsible Officer to inspect and report at least once a year on the recording media, the route of processing, methods of storage and the like of the Personal or Other Related Information in each division under his/her responsibility.
2. The Responsible Officer shall, upon receipt of the request of the preceding paragraph, order the Manager of each Section under his/her responsibility to inspect and report on the recording media, the route of processing, methods of storage and the like of the Personal or Other Related Information in the Section, and report the General Manager of the results.
3. The Manager shall, upon receipt of the order of the preceding paragraph, conduct an inspection of the recording media, the route of processing, methods of storage and the like of the Personal or Other Related Information in the Section and report the Responsible Officer thereof.
4. The Manager shall inspect on a regular and as-necessary basis the recording media, the route of processing, methods of storage and the like of the retained Personal Information in the Section, and report the results to the Responsible Officer, and, when finding it necessary, report the results to the General Manager through the Responsible Officer.

Article 61 Evaluation and Review

The General Manager, the Responsible Officer, the Manager and the like shall evaluate measures for the appropriate management of the Personal or Other Related Information from the perspective of their effectiveness based on the findings of the inspection of the preceding Article or audit of Article 59, and, when finding it necessary, carry out reviewing and the like of such measures.

Article 62 Cooperation with Administrative Entities

The Corporation shall carry out appropriate management of the Personal Information held by the Corporation in close cooperation with the Okinawa Development and Promotion Bureau of the Cabinet Office in line with the “Basic Policy on the Protection of Personal Information” (Cabinet Decision of April 2, 2004).

Article 63 Secretariat

The affairs pertaining to these Rules shall be undertaken by the Information Security Section for the affairs under the responsibilities of the CIO and CISO, and by the Rules and Compliance Section for the affairs under the responsibilities of the General Manager.

Article 64 Disciplinary Actions

If any of the Officers and Employee violates any of the provisions of these rules, the Corporation may take disciplinary action against him/her as stipulated in the Corporation's rules of Employment or the University rules.

Article 65 Miscellaneous Provisions

In Addition to matters stipulated in these Rules, other necessary details regarding administrations of Personal Information protection, requests for disclosure, correction and suspension of use, etc. shall be stipulated separately by the Secretary General.

Article 66 Transition from OIST Promotion Corporation

All Personal Information held by the OIST Promotion Corporation at the time of transition to the Corporation shall be transferred to the Corporation, and these Rules apply to such information.

Supplementary Provisions

These Rules shall come in effect from April 1, 2022.

Supplementary Provisions

These Rules shall come in effect from January 1, 2023.

Supplementary Provisions

These Rules shall come in effect from August 1, 2023.

Supplementary Provisions

These Rules shall come in effect from April 1, 2024

Supplementary Provisions

These Rules shall come in effect from October 1, 2024