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

Approved by the President
August 1, 2023

Article 1 Purpose

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 referred to as the "Corporation") so as to protect the rights and interests of the individual, based on the Act on the Protection of Personal Information (Act No. 57 of 2003. Hereafter referred to as the "Act").

Article 2 Ground Policy

1. The corporation must handle all Retained Personal Information in an appropriate manner, in light of the fact that the information should be handled with care under the principle of respect for the individual.
2. The Corporation's officers and employees (including temporary staff. Hereinafter the same.) and students must recognize the importance of protection of Personal Information and shall take appropriate measures in accordance with these Rules.
3. The Corporation will acquire, use or retain Personal Information only when necessary to carry out its businesses and to achieve its missions.
4. No officers, employees or students of Corporation shall acquire or use Personal Information in a manner that would encourage or induce illegal or unjust acts.
5. Further rules may be imposed locally by the Corporation, these Rules may only increase the level of restrictions but shall not decrease the level of restrictions.

Article 3 Definitions

The terms used in these Rules shall be construed in accordance with Article 2 of the Act.

Article 4 Chief Executive Officer

The Chief Executive Officer (hereinafter referred to as the "CEO"), as the head of the corporation of the Corporation, in accordance with the provisions of the laws, shall make final decisions on the reports and applications to the Prime Minister and other relevant ministers or to the national Personal Information Protection Commission and other government agencies.

Article 5 General Manager for Personal Information Protection

1. The Secretary General shall be appointed as the General Manager for Personal Information Protection (hereinafter referred to as the "General Manager") of the Corporation.
2. The General Manager shall have general responsibility for the management of Personal Information retained by the Corporation under the order of the CEO.

3. The General Manager shall maintain these Rules and develop the necessary guidelines to implement these Rules.
4. The General Manager facilitating the internal communication and coordination necessary to implement these Rules and to determine important matters related to the protection of Personal Information.

Article 6 Responsible Officer for Personal Information Protection

1. Each division shall appoint the Responsible Officer for Personal Information Protection (hereinafter referred to as the "Officer"), a position to be filled by the head of the division.
2. The Officer shall provide necessary guidance and supervision regarding the protection of Personal Information within the department under their jurisdiction.
3. The Officer shall normally be the Information Asset Manager role as defined in PRP Part 17.

Article 7 Personal Information Protection Manager

1. Each section shall appoint the Personal Information Protection Manager (hereinafter referred to as the "Manager"), a position to be filled by the head of the section.
2. The Manager shall have general responsibility for the management of Personal Information retained by the section and shall be responsible for ensuring appropriate management of Retained Personal Information.
3. When the Manager designates a staff member in charge of handling Retained Personal Information within each department in accordance with Paragraph 1 of the following article, the Manager shall report to the Officer to the effect and shall notify the General Manager regarding the designated staff member.

Article 8 Personal Information Protection Administrator

1. Each section shall appoint the Personal Information Protection Administrator (hereinafter referred to as the "Administrator"), who shall be appointed from among the Record Management Administrators by the Manager of each section, etc., 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 day-to- day operations relevant to the management of the Personal Information retained in the section.

Article 9 Chief Information Officer

1. The Chief Information Officer (hereinafter referred to as the "CIO") of the Corporation shall be responsible for the Corporation's management of information systems and cybersecurity program.
2. The CIO shall work with the General Manager, the Officer and the Manager for ensuring appropriate Personal Information protection management by the Corporation's information system and for facilitating appropriate information system.

3. The CIO is responsible for taking necessary actions, in cooperation with the General Manager, to ensure that electronic records containing Personal Information are appropriately managed and protected.

Article 10 Chief Information Security Officer

1. The Chief Information Security Officer (hereinafter referred to as the "CISO") of the Corporation is responsible for establishing information security policies, procedures, and management technology within the Corporation and overseeing the effectiveness of information security management measures through risk assessments and other means.
2. The CISO shall be responsible for maintaining information security in corporation with the General Manager and CIO.

Article 11 Personal Information Protection Consultative Committee

1. If the General Manager finds it necessary, the General Manager shall establish a Personal Information Protection Consultative Committee (hereafter referred to as the "Committee") to determine important matters related to the management of Retained Personal Information and to provide relevant communication and coordination, etc. and hold the meeting periodically or as necessary.
2. The Committee shall be chaired by the Secretary General and consist of the following members, as deemed necessary by the chairperson for each agenda item;
   (1) CIO;
   (2) CISO;
   (3) General Counsel;
   (4) Dean of the Graduate School;
   (5) Vice President for Human Resource;
   (6) Vice President for Communication and Public Relations; and
   (7) Any other persons in charge, officers or employees related to the matter to discuss.

Article 12 Auditor

1. The Chief Internal Audit Officer of the Corporation shall be appointed as the Personal Information Protection Audit Manager (hereafter referred to as the "Audit Manager").
2. The Audit Manager shall be responsible for auditing the status of management for Retained Personal Information.

Article 13 Responsibilities of Officers and Employees

The Corporation's officers and employees must adhere to the letter and intent of all relevant laws, ordinances, and guidelines, etc., and follow the instructions of the General Manager, the Officer, and the Manager for handling of the Retained Personal Information.

Article 14 Handover

When leaving a position at the Corporation, Manager and Administrator must transfer

all Retained Personal Information that they store to their successor or immediate supervisor.

Article 15 Acquisition of Personal Information

1. The Corporation must specifically explain or notify any proposed or intended use of Personal Information to the person at the time of acquisition.
2. If the Personal Information to be acquired falls under the category of Special Care-required personal information, the consent of the individual to the purpose of use shall be obtained.
3. If the Personal Information to be acquire falls under the category of Specified Personal Information, it shall be acquired in accordance with the Corporation's Rules on Handling Individual Numbers and Specific Personal Information.

Article 16 Personal Information Files

1. When the Personal Information is acquired in accordance with the preceding article, the Manager shall create a Personal Information File concerning such Retained Personal Information.
2. When a Personal Information File is created in accordance with the preceding paragraph, the Manager shall register it on the Corporation's Personal Information File Registration List (hereafter referred to as the "PIPL) provided by the CISO.
3. 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.
4. When the Corporation retains a Personal Information File, the General Manager shall notify the Personal Information Protection Commission of the Government regarding the following matters in advance. The same shall apply when the notified matters are to be changed.
   (1) Name of the Personal Information File;
   (2) Name of the said Incorporated Administrative Agencies and the name of the organizational section in charge of the affairs pertaining to the Personal Information;
   (3) Purpose of Use of the Personal Information File;
   (4) Matters recorded in the Personal Information File (hereinafter referred to as the "Recorded Matters" in this article) and the scope of individuals that are recorded in the Personal Information File as Individuals Concerned (limited to those who can be identified through a search without other description about the individual including the name and date of birth) (such scope shall be hereinafter referred to as the "Scope of Record" in this article);
   (5) Method of collecting the Personal Information recorded in the Personal Information File (hereinafter referred to as the "Recorded Information" in this article);
   (6) When Special Care-required Personal Information is included in the Recorded Information, a description to that effect;
   (7) Where the Recorded Information is routinely provided to a party outside the

said Incorporated Administrative Agencies, the name of such party;

(8) When a part of the Recorded Matters or the matters listed in item 5 or the preceding item is to be omitted from the Personal Information File Register, or when a Personal Information File is to be omitted from the Personal Information File Register, a statement to that effect;

(9) Name and address of the organizational section that accepts the request prescribed in Article 67, paragraph 1 of the Act, Article 90, paragraph 1 of the Act, or Article 98, paragraph 1 of the Act;

(10) Where the proviso of Article 90, paragraph 1 of the Act or the proviso of Article 98, paragraph 1 of the Act applies, a description to that effect; and

(11) Other matters designated by a Cabinet Order.

Article 17 Management of Personal Information File Registry

1. The Corporation must prepare and publish a Personal Information File Registry describing the matters listed in Paragraph 4 of the preceding article for each Personal Information Files held by the Corporation.
2. The Rules and Compliance Section shall create, store, and publish the Personal Information File Registry. However, the Personal Information File listed in the following items shall not be listed in the Personal Information File Registry.
   (1) Personal Information Files recording matters of vital interest to Japan, such as national security and diplomatic secrets;
   (2) Personal Information Files created for the purpose of investigating crimes and tax-related offenses;
   (3) Personal Information Files containing records of personnel, salary and other matters relating to employees;
   (4) Pilot Personal Information Files;
   (5) Copy files of Personal Information Files that have already been published in a Personal Information File Registry;
   (6) Personal Information Files containing only Personal Information that will be deleted within one year;
   (7) Personal Information Files used only for the purpose of sending goods and money and for business communication;
   (8) Personal Information Files created, obtained and used exclusively for academic research purposes; and
   (9) Personal Information Files containing fewer than 1,000 individuals.
3. The Manager must formally request the Rules and Compliance Section when updating the Personal Information File Registry and, whenever necessary, amend matters recorded to the Personal Information File Registry.

Article 18 Access Restriction

1. The Manager shall work with the CIO to restrict staff with access to Personal Information and the details of that access to the minimum scope required for those staff members to implement their work, as warranted by the confidentiality and nature of the Retained Personal Information. In considering the details of the access, the Manager must consider the ease of personal identification such as

anonymity level, the presence or absence of Special Care-required Personal Information, the nature and the extent of the damage caused by leakage of the Personal Information, and so on.

2. Unauthorized officers and employees shall not access Personal Information.
3. Even executives and employees with access privileges shall not access Personal Information for non-operational purposes.

Article 19 Access Control

1. The Manager shall work with the CIO to take necessary measures when handling Retained Personal Information in information systems, as warranted by the confidentiality and nature of Personal Information, to control access by establishing security measures (passwords, smart cards, biometrics) to verify authorization (hereinafter referred to as the "Authentication Functions").
2. When taking security measures described in the preceding paragraph, the Manager shall work with the CIO to initiate any rules for the management of passwords, etc. (including regular and as-necessary reviews) and take any required security measures in order to prevent the theft of passwords, etc.

Article 20 Access Records

1. The Manager shall, as warranted by the confidentiality and nature of Retained Personal Information, work with the CIO to enact such measures as may be necessary to record access to Personal Information and retain records (hereafter referred to as the "Access Record") for a predetermined regular audit of the Access Records.
2. The Manager shall work with the CIO to take any necessary measures to prevent the unauthorized modification, theft, or unauthorized destruction of the Access Records.

Article 21 Monitoring of Access

In order to monitor inappropriate access to Personal Information, the Manager shall, as warranted by the confidentiality and nature of such information, work with the CIO to take measures necessary to check at regular intervals.

Article 22 Settings of Administrative Authority

The Manager shall, as warranted by the confidentiality and nature of Retained Personal Information, take necessary measures such as acquiring a sign in document to acknowledge that they will be subject to disciplinary action by the Corporation if they conduct improper manipulation, in order to minimize harm in the event of theft of system administrative authority and prevent internal improper manipulation of such information, etc.

Article 23 Prevention of Unauthorized External Access

The Manager shall, as warranted by the confidentiality and nature of Retained Personal Information, work with the CIO to take such measures as may be necessary to prevent unauthorized external access to IT systems handling the Retained Personal

Information (e.g. firewall establishment to control access pathways).

Article 24 Prevention of Disclosure Incidents by Fraud

The Manager shall work with the CIO to take necessary measures to eliminate vulnerabilities exposed in software and prevent the infection of IT system by malware that has grasped such vulnerabilities (including maintaining introduced software in its most up to date state at all times), in order to prevent the unauthorized disclosure, loss, or damage of the Retained Personal Information due to malware.

Article 25 Limitations to Duplication, etc.

1. Even when officers or employees handle the Retained Personal Information for operational purposes, the Manager must limit the cases in which the actions listed below can be carried out as warranted by the confidentiality and nature of the Retained Personal Information in question.
   (1) Copying of the Retained Personal Information;
   (2) Distribution of the Retained Personal Information;
   (3) Distribution to outside parties or distribution of media containing the Retained Personal Information; and
   (4) Other inappropriate management of the Retained Personal Information.
2. The Corporation's officers and employees shall obtain permission from the Manager when performing any of the items listed in the preceding paragraph.

Article 26 Error Correction, etc.

The Corporation's officers and employees must, as instructed by the Manager, promptly correct the Retained Personal Information errors, etc.

Article 27 Management of Media

The Corporation's officers and employees shall store the Retained Personal Information media in a designated location as instructed by the Manager, and when deemed necessary, store said media under lock and key in a fireproof safe.

Article 28 Deletion and Disposal

In the event that the Retained Personal Information, media (including storage, terminals, and servers) is no longer needed, the Corporation's officers and employees must, as instructed by the Manager, delete relevant information and/or destroy relevant media in a manner that renders it impossible to recover or decipher the Retained Personal Information.

Article 29 Handling Records of Retained Personal Information

As warranted by the confidentiality and nature of the Retained Personal Information, the Manager must create registers, etc. and record the status of the Retained Personal Information use, storage, and handling.

Article 30 Ensuring Security at Management of Information System, etc.

1. In order to ensure appropriate protection of Personal Information in

electromagnetic records, the Corporation must take necessary measures, depending on the content of the information, to control access to the information system, record access, prevent unauthorized access from outside, prevent leaks, etc. due to computer viruses, limit the terminals where such information is processed, and prevent theft of terminals.

2. The CIO and CISO, in cooperation with the General Manager, is responsible for ensuring the appropriate protection of the Retained Personal Information in electronic records.
3. The CIO must take necessary actions in accordance with the guideline published by the government.
4. The CIO must establish internal guidelines for the management of passwords and take necessary measures to prevent theft of password.
5. The CIO must record the status of access to Personal Information and store such records as warranted by confidentiality and nature of Personal Information in question.
6. The Corporation must take necessary measures to prevent the alternation, theft, or unauthorized deletion of access records.
7. The Corporation must take necessary measures such as route control to prevent unauthorized external access to the system that handles Personal Information, etc.
8. The Corporation must take necessary measures to prevent the unauthorized disclosure and destruction of Personal Information by infection of IT system by computer virus.
9. The Corporation must determine who is authorized to enter the server room that handles Personal Information, etc., and shall take measures such as restricting the use and removal of such information, inspection, etc.
10. CIO shall set forth the details of safely assurance in PRP Part 17.

Article 31 Processing of Retained Personal Information in Information Systems

1. If carrying out an action such as copying the Retained Personal Information temporarily to process it, officers and employees shall limit the Retained Personal Information subject to such action to the minimum necessary and shall promptly delete any information no longer required after processing is complete.
2. The Manager shall, as warranted by the confidentiality and nature of the Retained Personal Information in question, confirm the situation from time to time with a focus on the state of implementation of deletion, etc.

Article 32 Encryption

1. The Manager shall, as warranted by the confidentiality and nature of the Retained Personal Information, work with the CIO to take necessary security measures to encrypt the Retained Personal Information.
2. The Corporation's officers and employees shall, as warranted by the confidentiality and nature of the Retained Personal Information, carry out encryption appropriately (actions such as the selection of appropriate passwords and measures to prevent their unauthorized disclosure are included) on the

Retained Personal Information that they process based on these security measures.

Article 33 Information Verification

The Corporation's officers and employees shall verify input against original copies, as warranted by the importance of the Retained Personal Information handled by information systems, in order to confirm the content of the Retained Personal Information before and after processing, and verify, etc. the integrity of existing Retained Personal Information.

Article 34 Backup

The Manager shall, in cooperation with CIO, as warranted by the importance of the Retained Personal Information, take necessary security measures to create and provide decentralized storage of the Retained Personal Information backups.

Article 35 Management of Information System Design Documents, etc.

The Manager shall take necessary security measures to store, copy, destroy, etc., the information system design documents, schematic diagrams, and other documentation for information systems related to the Retained Personal Information.

Article 36 Limitations for Terminals

The Manager shall, as warranted by the confidentiality and nature of Retained Personal Information, take necessary security measures to restrict terminals at which Retained Personal Information may be accessed.

Article 37 Theft Prevention, etc. for Terminals

1. The Manager shall take necessary security measures to prevent the theft and/or loss of terminals.
2. The Corporation's officers and employees shall not remove terminals from the Corporation premises or bring in terminals from outside except when deemed necessary by the Manager.

Article 38 Viewing Prevention against Third Party

The Corporation's officers and employees shall take necessary security measures to prevent the viewing of the Retained Personal Information by third parties when terminals are used (guidelines for logging off information systems).

Article 39 Restrictions on Connection of Devices and Media with Recording Functions

1. The Manager must, as warranted by the confidentiality and nature of the Retained Personal Information, work with the CIO to take necessary measures to restrict connection of smartphones, USB flash drives, and other devices and media with recording functions to information system terminals (including upgrade of such devices) in order to prevent unauthorized disclosure, loss, or damage of the Retained Personal Information.
2. The Manager shall further ensure that the system terminals are prevented from

accessing inappropriate cloud or other online services to the maximum reasonable extent possible.

Article 40 Access Control

1. The Manager shall work with the CIO to authorize persons to enter the core server room and other areas in which equipment handling the Retained Personal Information is located (hereinafter referred to as the "Server Room, etc.") and take necessary security measures to confirm the purpose of entry, log room access, identify outsiders, ensure that staff members are present when outsiders are granted access or that such outsiders are monitored by monitoring systems, and restrict or inspect the bringing in, use, and taking out of external electromagnetic media. If other media storage contains the Retained Personal Information, similar measures shall be taken when deemed necessary.
2. The Manager shall, when deemed necessary, work with the CIO to simplify the management of server room access by identifying the Server Room, etc. entrances and exits and restricting location signs.
3. The Manager shall work with the CIO to enact security measures to manage access to the Server Room, etc. and storage facilities, if deemed necessary, installing access Authentication Functions and formulating rules for the management of passwords, etc. (including regular and as-necessary reviews) and take such measures as to prevent the theft of passwords, etc.

Article 41 Management of Server Room, etc.

1 The Manager shall work with the CIO to take security measures as may be necessary to prevent unauthorized intrusions providing locks, alarms, and monitoring equipment for the Server Room, etc.

2 The Manager shall work with the CIO to take preventative measures against natural disasters, etc., by providing the Server Room, etc. with anti-seismic, fireproofing, smoke proofing, and waterproofing equipment, ensuring reserve power supplies for servers/other equipment and preventing damage to wiring.

Article 42 Provisions of Retained Personal Information

1. When providing the Retained Personal Information to outside parties other than the Administrative Agencies, etc. pursuant to Article 69, Paragraph 2, Item 2 and 4 of the Act, the Manager shall document the party receiving information by specifying the purpose of use, the legal rationale for the work in which used, the scope and content of usage records, and the form of use, etc.
2. In the case of the preceding paragraph, the Manager shall require the enactment of security measures and shall, when deemed necessary, perform on-site inspections prior to provision and periodically thereafter to confirm the status of measures, record findings, and seek improvements, etc.
3. When providing the Retained Personal Information to the Administrative Agencies, etc. pursuant to Article 69, Paragraph 2, Item 3 of the Act, the Manager shall, when deemed necessary, take the measures as set forth in the preceding two paragraphs.

4. When providing the Retained Personal Information to the Administrative Agencies, etc. pursuant to Article 69, Paragraph 2, Item 3 and 4 of the Act, the Manager shall anonymize Retained Personal Information as needed through considering the purpose of use by outside parties, the contents of the works by outside parties, and the level of secrecy of the Retained Personal Information to reduce the risk of the occurrence of damage caused by the leakage of the Retained Personal Information.
5. When the Retained Personal Information is disclosed to a third party located in a foreign country, the Manager must, in principle, obtain the prior consent of the individual to the effect that the provision of the Retained Personal Information to the third party located in the foreign country is permitted.
6. When the consent of the individual is to be obtained pursuant to the provision of the preceding paragraph, the Manager must, pursuant to the Rules of the Personal Information Protection Commission, provide the individual in advance with information that may be helpful to the individual, such as the system concerning the protection of the Retained Personal Information in the foreign country concerned, measures taken by the third party to protect the Retained Personal Information, and other information that may be helpful to the individual.
7. When the Corporation provided the Retained Personal Information to a third party located in a foreign country (limited to those who have established the system stipulated in Paragraph 1.), the Corporation must take necessary measures to ensure the continuous implementation of the corresponding measures by the third party in accordance with the Rules of the Personal Information Protection Commission and shall provide information on such necessary measures to the individual concerned at the individual's request.
8. When a third party is expected to obtain the Personal Related Information (limited to that which constitutes a database of personal related information, etc.) as Personal Information, the Corporation must not provide the Personal Related Information to a third party without first confirming the following matters in accordance with the rules of the Personal Information Protection Commission.
   (1) The consent the individual concerned has been obtained to allow the third party to receive the Personal Related Information from the business operator handling the Personal Related Information and to acquire the information as Personal Data that identifies the individual concerned;
   (2) In the event of provision to a third party in a foreign country, when the consent of the individual is to be obtained as set forth in the preceding item, the system concerning the protection of Personal Information in the foreign country, the measures taken by the third party to protect Personal Information, and other information that should be of reference to the individual concerned are provided to the individual concerned in advance, in accordance with the Rules of the Personal Information Protection Commission.
9. In the event of providing the Retained Personal Information to a third party in a foreign country for a purpose other than the purpose of use, the Corporation must obtain the prior consent of the individual that allows the provision to the third party in the foreign country, except in any of the following cases.

(1) The third party is located in a country that is stipulated by national regulations as a country with a Personal Information protection system that is recognized as having a level of protection equivalent to that of Japan;
(2) When the said third party has established a system that conforms to the standards established by the rules as necessary to continuously take measures equivalent to those required to be taken by Business Operators Handling Personal Information;
(3) When pursuant to laws;
(4) When providing Retained Personal Information exclusively for the purpose of compiling statistics or academic research;
(5) When it is clearly in the interest of the individual to provide the information to a person other than the individual; and
(6) Where there are other special reasons for providing the Retained Personal Information

10. In the event where the Retained Personal Information is provided to a third party in a foreign country for a purpose other than the purpose of use, the Corporation must take necessary measures to ensure the continuous implementation of the corresponding measures by the third party in accordance with the Rules of the Personal Information Protection Commission, and shall provide information concerning such necessary measures to the individual concerned at the individual's request, except when required by law or in the cases listed in Item 4 of the preceding paragraph of the preceding article.

Article 43 Operations Outsourcing, etc.

1. When outsourcing operations related to the handling of the Retained Personal Information, the Manager must take all necessary security measures avoid selection of parties lacking the capacity to appropriately manage Personal Information.
2. The Manager must make any contracts for outsourcing operations related to the handling of the Retained Personal Information in accordance with these Rules and separately the guideline set forth by the CISO.
3. The Manager must make any contracts for outsourcing operations related to the handling of Specific Personal Information in accordance with the Corporation's Rules on Handling Individual Numbers and Specific Personal Information.
4. When the Manager enters into an outsourcing contract with the selected third party for the operations stipulated in the preceding paragraph, the Manager must specify the following matters in the contract and confirm in writing the necessary matters including the management and operational systems of the person responsible for the services and the person engaged in work at the outsourced party and matters concerning the inspection of the state of management of Personal Information.
   (1) Obligations to protect the confidentiality of Personal Information and prohibit it from being used for any purpose other than that intended;
   (2) Restrictions or Conditions on sub-contracts;
   (3) Restrictions on copying, etc. of Personal Information;

(4) Response to unauthorized disclosure or other incident involving Personal Information;
(5) Destruction of Personal Information and return of digital media at the conclusion of outsourcing; and
(6) Contract cancellation procedures, liability for damages, and other necessary measures in the event of breach of contract.

5. Prohibition of subcontracting including the case of the subcontractor as a subsidiary, defined in Article 2, Paragraph 1, Item 3 of the Companies Act (Act No. 86 of July 26, 2005) of the contractor. In the exceptional case, conditions exist for subcontracting, such as a requirement to seek prior approval. Whether or not the subcontractor is a subsidiary of the contractor, the Contract shall specify that the subcontractor shall comply with the requirements that the Corporation puts forth to the contractor.
6. When outsourcing operations related to the handling of retained personal information, as warranted by the confidentiality, nature, and amount of the relevant Retained Personal Information, the Manager shall check the contractor's personal information management systems, organization, and practices through regular physical inspections conducted at least annually in principle.
7. If a contractor sub-contracts operations involving the handling of the Retained Personal Information, the Manager shall require the contractor to take the measures described in Paragraph 1 and 4, and, as warranted by the confidentiality and nature of the relevant Retained Personal Information, the measures described in Paragraph 6 shall be taken either via the contractor or directly by the party outsourcing the operations. The same requirements shall apply if operations involving the handling of the Retained Personal Information are further sub-contracted.
8. When temporary staff handle the Retained Personal Information, the Manager must contain explicit provisions regarding the confidentiality obligations and other aspects of the handling of Personal Information in the temporary staff referral contacts.
9. When outsourcing the handling of Personal Information to the contractor, the Manager must anonymize Personal Information as needed in the manner prescribed in Paragraph 4 of the preceding Article.

Article 44 Creation, Handling and Limitation of Pseudonymized Information

1. When the Corporation creates Pseudonymized Information (limited to that which constitutes the database of pseudonymized information, etc.), the Corporation must process Personal Information in accordance with the standards prescribed by the Rules of the Personal Information Protection Commission as necessary to make it impossible to identify a specific individual unless it is cross-checked with other information.
2. When Pseudonymized Information is created, or when Pseudonymized Information and the deleted information, etc. (meaning descriptions, etc. and personal identification codes deleted from Personal Information used to create

Pseudonymized Information, as well as information on the processing method used in accordance with the preceding paragraph) pertaining to the said Pseudonymized Information is obtained, the Corporation must take measures for secure management of the deleted information, etc. in accordance with the standards prescribed by the Rules of the Personal Information Protection Commission as those necessary to prevent leakage of the deleted information, etc.

3. Notwithstanding the provisions of Article 18 of the Act, the Corporation must not, except as otherwise required by laws and regulations, use any Pseudonymized Information (limited to that which is Personal Information. The same shall apply hereinafter in this Article).
4. When the Corporation creates Pseudonymized Information, the Corporation shall publicly announce the purpose of use specified or notified at the time of acquisition of said Personal Information.
5. When there is no longer a need to use Personal Data and Deleted information, etc., that is Pseudonymized, the Corporation must endeavor to delete such Personal Data and deleted information, etc., without delay. In this case, the provisions of Article 22 of the Act shall not apply.
6. The Corporation must not disclose Pseudonymized Information (excluding information that is Personal Information) to any third party (excluding those who are entrusted with the handling of said Pseudonymized Information) in principle.
7. In handling Pseudonymized Information, the Corporation must not obtain deleted information, etc., or check said Processed Pseudonymized Information against other information in order to identify the individual whose Personal Information was used to create said Pseudonymized Information.
8. In handling the Pseudonymized Information, the Corporation must not use the contact information or other information contained in the said Pseudonymized Information to make a telephone call, send a letter by postal mail, or by a general or specified letter service operator stipulated in the Act on the Service of Letters by Private Business Operators, send a telegram, send a facsimile device or electromagnetic method, or visit a residence.
9. The provisions of Paragraph 2 of Article 17, Article 26, and Articles 32 through 39 of the Act shall not apply to Pseudonymized Information, Personal Data that is the Pseudonymized Information, and the retained Personal Data that is the Pseudonymized Information.
10. The provision of the preceding paragraphs shall apply mutatis mutandis to the case where a person who has been entrusted with the handling of the Pseudonymized Information (including entrustment over two or more stages) by the Corporation.

Article 45 Handling of Specific Personal Information

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

Article 46 Handling of Anonymously Processed Information held by

Administrative Agencies, etc.

The procedures of handling for 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 47 Report of Incidents

1. The Corporation's officers and employees who are aware of unauthorized disclosure of Personal Information or other security problems related to Personal Information must immediately report to the department's Manager and the CISO.
2. Upon receiving a report under the preceding paragraph, the Manager must immediately report it to the responsible person. They must also confirm that the report has been notified to the General Manager.
3. Upon receiving a report under Paragraph 1, the Manager, in cooperation with the CISO, must immediately take necessary measures to prevent the spread of damage, such as unplugging the LAN cables of terminals suspected of illegal access from outside or infection by illegal programs(including having officers and employees take the necessary measures to prevent the spread of damage) and shall investigate the circumstances under which the incident occurred and submit a report to the General Manager. This does not preclude additional reports on matters that come to light after the report has been submitted.
4. The General Manager shall instruct the Manager to notify the all affected individuals based on the report described in the preceding paragraph.
5. Based on the instruction described in the preceding paragraph, the Manager must promptly notify the all affected individuals of the outline of the situation, the items of 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 all affected individuals. However, this shall not apply in cases where it is difficult to notify the individual concerned and alternative measures necessary to protect the rights and interests of the individual concerned are taken. Such notification shall also be made to the persons concerned or organizations to which the individual belongs, as necessary.
6. Upon receiving a report under Paragraph 1, the General Manager, in cooperation with the CISO, shall determine whether the case is minor or not, after confirming the details of the case and the damage.
7. When a case is judged to be minor in the preceding paragraph, the General Manager shall alert the Officer responsible for the management of the case, including prevention of recurrence of such a case.
8. In the event of an incident that is not deemed minor under paragraph 5, the General Manager must promptly report to the President that such an incident has occurred.

Article 48 Preliminary Report to the Government

1. In the event of a case under Paragraph 8 of the preceding Article, the General

Manager must immediately report to the National Personal Information Protection Commission, the Okinawa Promotion Bureau of the Cabinet Office, and other relevant ministries and agencies, a preliminary report regarding the content of the case, the circumstances surrounding the case, and the state of damage.

2. In the case of the preceding paragraph, the General Manager shall immediately make public the facts and measures to prevent recurrence, etc., according to the content and impact of the case. If, through the investigation and analysis described in Paragraph 3 of the preceding Article, new details, circumstances, and damage, concerning the case come to light after the said public announcement, the General Manager is not precluded from making a public announcement again.

Article 49 Recurrence Prevention Measures

1. The Manager must promptly submit a final report, including measures to prevent recurrence, to the General Manager after the investigation and analysis as stipulated in Article 47, Paragraph 3.
2. The Manager, together with the CISO and other relevant staff, must implement the recurrence prevention measures reported in the preceding paragraph.

Article 50 Reporting to the Government

1. The General Manager must promptly report the case to the Okinawa Development Bureau of the Cabinet Office and the National Personal Information Protection Commission, based on the final report under Paragraph 1 of the preceding Article.
2. When the General Manager makes a public announcement of a case pertaining to a report under Paragraph 1, he/she shall promptly provide the information to the Administrative Management Bureau of the Ministry of Internal Affairs and Communications.
3. When the General Manager makes a report under Paragraph 1, he/she shall report the contents of the report to the Council Committee.
4. When the General Manager has made a report under Paragraph 1, he/she shall submit a final report on the case to the President.

Article 51 Inspection

1. The General Manager may request the Officer to inspect and report at least once a year on the status of use and storage of Retained Personal Information in each division under his/her jurisdiction.
2. When requested as in the preceding paragraph, the Officer must order the Manager of each section under their jurisdiction to inspect and report on the status of use and storage of the Retained Personal Information in their respective section and shall report the results of such inspection and report to the General Manager.
3. Upon receiving the order set forth in the preceding paragraph, the Manager must conduct an inspection of the use and storage status of the Retained Personal Information in each section and report the inspection to the Officer.
4. The Manager shall inspect on a regular and as necessary basis the digital recording media, processing channels, and storage methods, etc. for the Retained Personal

Information in his or her section and shall report findings to the Officers, and if deemed necessary, the results shall be reported to the General Manager through the Officer.

Article 52 Audit

The Audit Manager shall perform regular and as necessary audits (including independent audits by external auditors; hereinafter the same) of the management at the Corporation in question to verify the appropriate management of the Retained Personal Information, and shall report the findings to the General Manager.

Article 53 Evaluation and Review

The General Manager, the Officer, and the Manager shall evaluate measures for the appropriate management of the Retained Personal Information from the perspective of their effectiveness based on the findings of the audit provided in the preceding article or inspection under Article 49 and shall review such measures when deemed necessary.

Article 54 Cooperation with Government Agencies

The Corporation shall carry out appropriate management of the Retained Personal Information in close cooperation with the Okinawa Development and Promotion Bureau of the Cabinet Office in question based on Paragraph 4 of the "Basic Policy on the Protection of Personal Information" (Cabinet Decision, April 2, 2004).

Article 55 Training for Officers and Employees

1. The General Manager shall provide adequate training for the Corporation's officers and employees handling the Retained Personal Information in matters of the Retained Personal Information handling and increase general awareness of protection of Personal Information.
2. The General Manager shall work with the CIO to ensure necessary training for the Corporation's officers and employees involved in the management of information systems handling the Retained Personal Information in the management, operations, and security of information systems to enable appropriate management of the Retained Personal Information.
3. The General Manager shall implement training for the Managers and the Officers for the appropriate management of the Retained Personal Information at the site of each section, etc. under their jurisdiction.

Article 56 Secretariat

The secretariat concerning these Rules shall be conducted by the Information Security Section for operations in the responsibilities of the CIO and CISO, and by the Rules and Compliance Section for operations in the responsibilities of the General Manager.

Article 57 Disciplinary Actions

A Corporation's officer, employee or student in violation of these Rules, by willful act or gross negligence, or those involved in the said violation, shall be subject to disciplinary actions provided in the Corporation's Rules of Employment or University

Rules, etc.

Article 58 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 59 Transition from OIST Promotion Corporation
All Personal Information held by the OIST Promotion Corporation at the time of transition to the Corporation must be transferred to the Corporation and managed in accordance with these Rules.

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.