Okinawa Institute of Science and Technology School Corporation
Regulations on Handling Individual Numbers and Specific Personal Information

January 1, 2016
Approved by the CEO/President
[Partial Amendment] February 8, 2016
[Partial Amendment] April 1, 2018

Chapter 1 General Provisions

Article 1. Objective

The objective of these Regulations is to prescribe the necessary measures to ensure the appropriate handling of Individual Numbers and Specific Personal Information (hereinafter, the "Specific Personal Information") at the Okinawa Institute of Science and Technology School Corporation (hereinafter, "the University").

Article 2. Definitions

The definitions of the terms used in these Regulations shall be construed in accordance with each of the following items.

(1) Personal Information
Means the information relating to a living individual that can be used to identify such individual from his or her name, date of birth or other description of such individual, or a mark such as a number or code that is assigned to each individual (this includes information that is insufficient by itself to identify the individual, but can be used to enable a simple check with other information to identify said individual).

(2) Individual Number
Means the number obtained by converting a resident record code pursuant to Article 2 paragraph (5) of the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (hereinafter, the "ID Act") in order to identify the person to whom the resident record where said resident record code is stated pertains.

(3) Specific Personal Information
Means Personal Information that includes the Individual Number.

(4) Personal Information File
Means a set of information that includes Personal Information, that is systematically arranged so that Specific Personal Information can be searched for using a computer, and systematically arranged in such a way that Specific Personal Information can be easily retrieved as pursuant to the provisions of the Order for Enforcement of the Act on the Protection of Personal Information.

(5) Specific Personal Information File

Means the Personal Information File that includes the Personal Information.

(6) Affairs Related to the Individual Number

Means the affairs that are processed in relation to affairs using the Individual Number by using another person's Individual Number to the extent necessary pursuant to the provisions of Article 9, paragraph (3) of the ID Act. (Affairs using the Individual Number means affairs that persons processing administrative affairs, such as Government, local governments, or incorporated administrative agencies or other individuals and organs assuming administrative functions process by using the Individual Number to the extent necessary to search and manage efficiently the Personal Information in the Specific Personal Information File that is kept by said persons pursuant to the provisions of Article 9, paragraph (1) or paragraph (2) of the ID Act.)

(7) Person

Means a specific individual who is or can be identified by an Individual Number.

(8) Worker

Means a person within the organization of the University who is engaged in the business of the University under both the direct and indirect direction and supervision of the University. Specifically, apart from officers and employees of the University, this includes temporary employees, etc.

Chapter 2 Obtaining Specific Personal Information

Article 3. Specifying and Changing Purpose of Use

1. The University shall use Specific Personal Information only for the following purposes (hereinafter, the "Purpose of Use").

(1) Specific Personal Information about officers and employees, students and their spouses and families of the University

・Affairs concerning tax withholding at the source for earned income and retirement income

・Affairs concerning the creation of declaration of tax exemption for salaried employee, notification of insurance premium deduction and notification of special exemptions for the spouse of the income earner

・Affairs concerning mutual aid business (Private School Mutual Aid) in accordance with the Promotion and Mutual Aid Corporation for Private Schools of Japan

・Affairs concerning the notification, application and claim for health insurance and welfare pension insurance

・Affairs concerning the notification, application, claim and creation of certificates for employment insurance

・Affairs concerning the creation of certificates for worker's accident insurance

・Affairs concerning the creation of notification, registration and the application for property accumulation savings, and property accumulation pension savings

・Affairs concerning notification of Category III insured persons for the National Pension

(2) Specific Personal Information concerning individuals other than pursuant to the provisions of the preceding paragraph

・Affairs concerning the creation of payment records for remuneration and fees, etc.

・Affairs concerning tax withholding at the source for remuneration (including gratuities and allowances) paid by the University

(3) Specific Personal Information relating to real estate or other transaction

・Affairs concerning the creation of payment records for real estate rents or for other transaction

・Affairs concerning the creation of payment records for consideration paid for acquisition of real estate or for other transaction

2. If the University proposes to change the Purpose of Use, this shall be done within the scope of what is considered to be reasonably equivalent to the Purpose of Use prior to the change.
3. If the University changes the Purpose of Use, the changed Purpose of Use shall be notified to the Person or publicly announced.

Article 4. Notice or Announcement of the Purpose of Use at the Time of Acquisition

1. If the University acquires Specific Personal Information, it shall notify the Person of the Purpose of Use or publicly announce it beforehand.
2. The provisions of the preceding paragraph shall not apply to the following cases.

(1) Cases in which it is necessary to cooperate with Government, local government, incorporated administrative agencies or other individuals and organs assuming administrative functions in executing the affairs pursuant to the provisions of laws and regulations and when notifying the Person of the Purpose of Use or publicly announcing it risks impeding the execution of the affairs

(2) Cases in which it is considered that the Purpose of Use is clear in consideration of the circumstances of the acquisition.

Article 5. Restrictions on Acquisition

The University shall not collect another person's Specific Personal Information, except in cases that fall under any of the items in Article 19 of the ID Act.

Article 6. Restrictions on Request of Provision of Individual Number

The University shall not request another person to provide an Individual Number, except in cases where the person falls under any of the items of Article 19 of the ID Act and may receive provision of Specific Personal Information.

Article 7. Personal Identification

When the University receives provision of an Individual Number from the Person or that Person's agent, the Person shall be identified in accordance with the provisions of Article 16 of the ID Act, using the

following method.

(1) Cases where the person has an Individual Number Card, by presentation of the Individual Number card or the copy.

(2) Cases where the person does not have an Individual Number Card, by presentation of each of the following documents or the copy. However, in the case that the University finds that such person is the Person based on consideration of the employment relation with that person or other circumstances, there shall be no requirement to receive provision of the documents to verify the identity.

- Either the Notification Card or resident record with Individual Number attached
- Any document (limited to currently valid documents) such as a driver's license, passport or other document that verifies identity.

Article 8. Security Control Measures

When acquiring Specific Personal Information, the University shall undertake the security control measures as pursuant to the provisions of Article 21 (Record of Handling Specific Personal Information), Article 22 (Record of Management Status Based on these Regulations), Article 25 (Supervision and Training of Officers and Employees), Article 26 (Supervision of Entrustees), and Article 31 (Technical Security Control Measures).

Chapter 3 Use of Specific Personal Information

Article 9. Restrictions on Use other than the Purpose of Use

1. The University shall not handle Specific Personal Information beyond the scope necessary for achievement of the Purpose of Use specified by the provisions of Article 3.
2. Notwithstanding the provisions of the preceding paragraph, in cases that fall under any of the following items, the University may handle Specific Personal Information beyond the scope of the Purpose of Use specified pursuant to the provisions of Article 3.

(1) When there is a disaster of extreme severity (however, restricted to affairs to the extent necessary for the payment of money such as mutual aid money based on a contract that has been concluded in advance)

(2) In cases where it is necessary for protecting the life, body or property of humans, when the consent of the Person is obtained or when it is difficult to obtain the consent of the Person.

Article 10. Restrictions on Generation of Specific Personal Information Files

The University shall not generate a Specific Personal Information File beyond the extend necessary for processing Affairs Related to the Individual Numbers except in cases where he or she falls under any of Article 19, items (xi) through (xiv) of the ID Act and can provide or receive provision of Specific Personal Information.

Article 11. Security Control Measures

When using Specific Personal Information, the University shall undertake the security control measures as pursuant to the provisions of Article 21 (Record of Handling Specific Personal Information), Article 22 (Record of Management Status Based on these Regulations), Article 25 (Supervision and Training of Officers and Employees), Article 26 (Supervision of Entrustees), Article 27 (Control of Areas Handling Specific Personal Information), Article 28 (Prevention of Theft or Loss), Article 29 (Prevention of Leaks when Taken Outside) and Article 31 (Technical Security Control Measures).

Chapter 4 Preservation, Provision, Deletion and Disposal of Specific Personal Information

Article 12. Keeping Specific Personal Information

The University shall not keep Specific Personal Information, except in cases falling under any of the items of Article 19 of the ID Act.

Article 13. Ensuring Accuracy of the Data

The University shall endeavor to hold accurate and up to date Specific Personal Information to the extent necessary for achievement of the Purpose of Use specified by the provisions of Article 3.

Article 14. Provision of Specific Personal Information

The University shall not provide Specific Personal Information except in cases falling under any of the items of Article 19 of the ID Act.

Article 15. Deletion and Disposal of Specific Personal Information

The University shall as quickly as possible dispose or delete the Individual Number in cases where the need to process Affairs Related to the Individual Number has ceased and the retention period pursuant to the provisions of laws and ordinances has passed. However, retention may continue in the case that it is possible to mask or delete so that such Individual Number portion cannot be reconstructed.

Article 16. Security Control Measures

When retaining, providing, deleting or disposing of Specific Personal Information, the University shall undertake the security control measures as pursuant to the provisions of Article 21 (Record of Handling Specific Personal Information), Article 22 (Record of Management Status Based on these Regulations), Article 25 (Supervision and Training of Officers and Employees), Article 26 (Supervision of Entrustees), Article 27 (Control of Areas Handling Specific Personal Information), Article 28 (Prevention of Theft or Loss), Article 29 (Prevention of Leaks when Taken Outside), Article 30 (Deletion of Individual Number, Disposal of Documents, Devices and Electronic Media) and Article 31 (Technical Security Control Measures).

Chapter 5 Organization and System

Article 17. The Person in Charge of and the Person Responsible for Handling Affairs

1. As prescribed separately, the University shall clarify the extent of affairs for handling Specific Personal Information, and after clarifying the extent of Specific Personal Information to be handled for identified affairs, identify the Worker to be engaged in such affairs (hereinafter, the "Person Responsible for Handling Affairs") and the person in charge of handling such affairs (hereinafter, the "Person in Charge of Handling Affairs"). In addition, the operational procedures when acquiring Individual Numbers shall be prescribed separately.
2. The University may outsource some operational procedures when acquiring Individual Numbers to business operators that provide cloud services. However, even in the case of outsourcing operational procedures to a business operator, the Personal Identification pursuant to the provisions of Article 7 shall in principle be conducted by a University official.

Article 18. Person Responsible for Managing Specific Personal Information

1. The University shall have a Person Responsible for Managing Specific Personal Information for the security control of Specific Personal Information, and the Chief Operating Officer (COO) shall serve in this position.
2. The Person Responsible for Managing Specific Personal Information shall have jurisdiction over the following areas.

(1) Ensure awareness of these Regulations
(2) In cases where revisions to these Regulations are proposed, draft such proposed revisions
(3) Draft, formulate and ensure awareness of regulations concerning the security control of Specific Personal Information, etc. (except these Regulations)
(4) Collect reports from the Person Responsible for Handling Affairs and give advice and guidance
(5) Educate and train the Person in Charge of Handling Affairs concerning the appropriate handling of Specific Personal Information
(6) Matters concerning other security controls for Specific Personal Information

Article 19. Obligations of Officers and Employees

1. No current or former officers or employees of the University shall disclose the details of the Specific Personal Information, etc. that he or she has come to know in the course of business to another person without due cause or use such information for unjust purpose.
2. An officer or employee who understands that there has been or there is indication of leakage, loss or damage of Specific Personal Information shall report to that effect to the Person Responsible for Handling Affairs or the Person Responsible for Managing Specific Personal Information.
3. An officer or employee who understands that there has been or there is indication of a violation of these Regulations, shall report to that effect to the Person Responsible for Handling Affairs or the

Person Responsible for Managing Specific Personal Information.

4. On receiving a report as set forth in the preceding two paragraphs, the Person Responsible for Handling Affairs shall immediately report such matter to the Person Responsible for Managing Specific Personal Information.
5. The Person Responsible for Managing Specific Personal Information shall examine the details of the reports as set forth in the preceding three paragraphs, and in the case that it is ascertained that these Regulations were in fact violated, report without delay to the CEO/President, while instructing the relevant departments to take the appropriate measures.

Chapter 6 Security Control Measures

Article 20. Security Control for Specific Personal Information

The University shall take the measures pursuant to the provisions from Article 21 to Article 24 and Article 31 to prevent leakage, loss or damage of Specific Personal Information, and other security control of Specific Personal Information.

Article 21. Record of Handling Specific Personal Information

1. The University shall record the following using the separately prescribed format Management Register for Specific Personal Information.

(1) Type and name of Specific Personal Information File
(2) Person responsible, handling division
(3) Purpose of use
(4) Status of deletion and disposal
(5) Persons with access rights

2. Specific Personal Information must not be recorded in the Management Register for Specific Personal Information.

Article 22. Record of Management Status Based on these Regulations

The University shall record the following items as the system log or using one of the separately prescribed formats: "Management Register for Specific Personal Information" or " Record for Taking Out Specific Personal Information" to verify the status of management based on these Regulations.

(1) Record the use and output of the Specific Personal Information File
(2) Record documents and media taken outside
(3) Record deletion and disposal of Specific Personal Information File
(4) Record the proof in the case that deletion or disposal is externally outsourced from the University
(5) Record the usage (such as login history or access log) of the information system for the Person Responsible for Handling Affairs or the Person in Charge of Handling Affairs in the case that Specific Personal Information File is handled in the information system.

Article 23. Responding to Events such as Information Leaks

1. A Worker who understands that there has been or there is indication of an event such as an information leak shall promptly report to the Person Responsible for Managing Specific Personal Information or a person designated by such person.
2. When a report is received as set forth in the preceding paragraph, the Person Responsible for Managing Specific Personal Information shall promptly convene a meeting of the Specific Personal Information Incident Investigation Committee.
3. The Specific Personal Information Incident Investigation Committee shall comprise members from the following list as deemed necessary for each matter by the Committee chair, with the Chief Operating Officer (COO) serving as the Committee chair.

(1) Dean of Faculty Affairs
(2) Vice-President for Gender Equality and Human Resource Development
(3) Vice President for Financial Management
(4) Vice President for Communication and Public Relations
(5) University General Counsel
(6) Chief Information Officer (CIO)
(7) Other persons that the Person Responsible for Managing Specific Personal Information considers to be necessary

4. The Specific Personal Information Incident Investigation Committee shall appropriately and promptly deal with the following matters as required.

(1) Examine the facts and determine the cause
(2) Notify persons who could be impacted
(3) Notify the Specific Personal Information Protection Commission and the competent cabinet minister
(4) Investigate and set measures to prevent reoccurrence
(5) Publicly announce the facts and measures to prevent reoccurrence.

Article 24. Understanding of the Status of Handling and Revision of the Security Control Measures

1. The University shall appoint auditors who understands the status of handling Specific Personal Information to be involved in evaluating, revising and improving the security control measures.
2. The auditors shall inspect the status of handling Specific Personal Information while giving advice concerning revisions to the security control measures.
3. The Auditors of the University shall serve as the auditors.

Article 25. Supervision and Training of Officers and Employees

The University shall provide the necessary and appropriate supervision and training of officers and employees for security control of Specific Personal Information.

Article 26. Supervision of Entrustees

1. When outsourcing all or part of the handling of Specific Personal Information, the University shall, as a general rule, clarify the measures that the outsourcer should undertake in relation to the security control of Specific Personal Information in the outsourcing contract after previously verifying whether or not the measures being undertaken at the entrustee are at an equivalent level to the security control measures that the University should be discharging in accordance with the ID Act, and carry out the necessary and appropriate supervision over the outsourcer.
2. The entrustee shall obtain the consent of the University in the case that all or part of the handling of Specific Personal Information has been further outsourced by the entrustee. In addition, in the case of further outsourcing, the University shall supervise to ensure the entrustee carries out the necessary and appropriate supervision over the further outsourcer.

Article 27. Control of Areas Handling Specific Personal Information

The University shall clarify the areas of control for information systems that handle Specific Personal Information File (hereinafter, the "Control Areas") and areas for implementing affairs for handling Specific Personal Information (hereinafter, the "Handling Areas") and undertake each of the following security control measures.

(1) Control Areas
Entry/exit control and restrictions on carrying devices, etc. into Control Areas

(2) Handling Areas
Undertake measures such as placing walls and room dividers, stationing seats in locations with few comings and goings other than the Person in Charge of Handling Affairs, moving seats to locations with a low possibility of being able to peek from behind, and affixing privacy filters to prevent being able to peek at computer displays.

Article 28. Prevention of Theft or Loss

The University shall undertake the following security control measures to prevent theft or loss of devices, electronic media and documents that handle Specific Personal Information in the Control Areas and Handling Areas.

(1) Keep electronic media and documents that handle Specific Personal Information in cabinets and archives that can be locked.
(2) Fix devices that handle Specific Personal Information File with a security wire.

Article 29. Prevention of Leaks when Taken Outside

1. The University shall undertake the following measures in the case of carrying electronic media and documents in which Specific Personal Information is recorded outside Control Areas and Handling Areas.

(1) Protect through encryption or password data that is carried or use lockable transportation containers.

However, when having to submit legal records in the form of data to administrative agencies, follow the method of submission stipulated by the administrative agencies.

(2) Documents in which Specific Personal Information is recorded shall be carried with a seal.

2. As a general rule, electronic media and documents in which Specific Personal Information is recorded shall not be taken outside, except in the cases of the submission to administrative agencies.

Article 30. Deletion of Individual Number, Disposal of Documents, Devices and Electronic Media

1. When deleting or disposing of an Individual Number, the University shall delete or dispose of such using an unrestorable method in accordance with the following.

(1) In the case of disposing of documents in which Specific Personal Information is recorded, incinerate, dissolve, use a shredder that can cut to the extent that reconstruction is impossible or mask to the extent that the Individual Number portion cannot be reconstructed.

(2) In the case of disposing of devices or electronic media in which Specific Personal Information is recorded, use dedicated data deletion software or destroy physically.

(3) In the case of deleting the Individual Number or some Specific Personal Information within a Specific Personal Information File, delete using a method that cannot be reconstructed unless using dedicated software, program or equipment for data reconstruction.

2. In the case where an Individual Number or Specific Personal Information File was deleted or in the case where the documents or the electronic media were disposed of, the University shall retain a record of the deletion or disposal. In addition, in the case that such affairs are outsourced, the University shall verify the definite deletion or disposal by the entrustee with a certificate of proof.

Article 31. Technical Security Control Measures

1. The University shall control appropriate access to limit the person in charge of handling affairs and the scope of Specific Personal Information File handled in such affairs.

2. The University's information system for handing Specific Personal Information shall authenticate that the Person in Charge of Handling Affairs is the person with the correct access rights based on the identified results.

3. The University shall undertake the following measures to protect the information system against unauthorized external access and malware.

(1) Measures such as firewall shall be established at the connection point between the University's information system and external networks to block unauthorized access.

(2) Security software (such as anti-virus software) shall be installed on the information system and devices.

(3) The use of automatic upgrading functions installed as standard on devices will keep software up to date.

(4) Regular analysis of logs, to detect unauthorized access.

4. In the case that Specific Personal Information is transmitted externally through the Internet, the

University shall endeavor to have an encrypted communication channel.

Article 32. Disclosure of Specific Personal Information

1. When there is a request from the Person in writing or orally to disclose the retained personal data that relates to Specific Personal Information, that may lead to identification of such Person (including notifying the Person that the University has not such retained personal data that relates to Specific Personal Information that may lead to identification of such Person. The same shall apply hereinafter), the University shall disclose such retained personal data after verifying the identity of person through identification papers. However, the University may keep all or part of the retained personal data undisclosed when falling under any of the following items.

(1) In cases where there is risk of harm to the life, body, property or other rights or interests of the Person or a third party

(2) In cases where there is risk of serious impediment to the proper execution of the University's business

(3) In cases that would violate other laws and regulations

2. Disclosure shall be in writing. However, in cases where there is consent from the person who requested the disclosure, disclosure may be made in a method other than in writing.

3. The notice of the decision to disclose or not disclose retained person data that relates to Specific Personal Information shall be provided to the Person in writing without delay.

Article 33. Corrections of Specific Personal Information

1. When there has been a request from the Person to correct, add or delete the retained personal data that relates to Specific Personal Information on the ground that the retained personal data that relates to such Specific Personal Information that may lead to the identification of such Person is contrary to the fact, the University shall, except in cases in which special procedures are prescribed by any other laws and regulations for such correction, addition or deletion, make a necessary investigation without delay within the scope necessary for the achievement of the Purpose of Use and, on the basis of the results, correct, add or delete the retained personal data that relates to such Specific Personal Information.

2. When the University has corrected, added or deleted the retained personal data that relates to the Specific Personal Information based on the request as set forth in the preceding paragraph, or decided not to make such correction, addition or deletion, the University shall notify the Person of that effect (including the content of the correction, addition or deletion if performed) without delay.

3. When there is another submission from the person who received the notice set forth in the preceding paragraph, the University shall conduct the same process as set forth in the preceding paragraph.

4. In the case of issuing a notice to the effect that all or part of the measures requested by the Person are not taken or in the case of issuing a notice to the effect that different measures have been taken pursuant to the provisions of paragraph 2, the University shall endeavor to explain such reason to the Person.

Article 34. Discontinuance or Erasure of the Use of Specific Personal Information

1. In the case where the University is requested by the Person to discontinue using or to erase the retained personal data that relates to Specific Personal Information as may lead to the identification of the Person on the ground that such retained personal data is being handled in violation of Article 9 or that such retained personal data has been obtained in violation of Article 5, or in the case where the University is requested by the Person to discontinue the provision of the retained personal data that relates to such Specific Personal Information to a third party (hereinafter, "Discontinue the Provision to a Third Party") on the ground that such retained personal data has been provided to a third party in violation of Article 14 and in the case that it is ascertained that there are such grounds, discontinue the use of or erase retained data that relates to such Specific Personal Information or Discontinue the Provision to a Third Party without delay. However, this provision shall not apply to cases in which it costs a large amount or is otherwise difficult to discontinue the use, to erase or discontinue to provide the data to a third party and in which the University takes necessary alternative measures to protect the rights and interest of the Person.
2. When the University has discontinued the use, erase or has decided not to discontinue the use of retained personal data that relates to Specific Personal Information based on the request as set forth in the preceding paragraph or when the University has discontinued the provision to a third party or decided not to discontinue the provision to a third party, the University shall notify the Person of that effect without delay.
3. Paragraphs 3 and 4 of the preceding article shall apply mutatis mutandis to the provision of this article.

Supplementary Provisions

These Regulations shall come into force as from January 1, 2016.

Supplementary Provisions

These Regulations shall come into force as from February 8, 2016.

Supplementary Provisions

These Regulations shall come into force as from April 1, 2018.