

Regulations on the Handling of Specific Personal Information

Chapter 1 General Provisions	
(Purpose)	
Article 1	These Regulations set down security measures and the points to be noted at each stage of “acquisition/input,” “use/processing,” “storage/preservation,” “transfer/transmission,” and “deletion/disposal” of Specific Personal Information, etc. handled by Branches in Japan of State Bank of India (hereinafter referred to as the “Bank”) in order to ensure the appropriate handling of Specific Personal Information, etc. in accordance with the “Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures” (hereinafter referred to as the “Numbers Act”) and relevant laws and regulations, and internal regulations. These Regulations shall apply to Specific Personal Information, etc. in preference to other regulations concerning the protection of personal information of the Bank, and other regulations shall apply to matters not stipulated in these Regulations.
(Definitions)	
Article 2	Terms appearing in these Regulations are defined as follows. Unless otherwise specified, the terms used in these Regulations shall have the same meaning as those defined in the Act on the Protection of Personal Information (hereinafter referred to as the “APPI”), the Numbers Act, and other relevant laws and regulations.
(i)	The term “Personal Information” shall mean information relating to a living individual which falls under any of the following. a. those containing a name, date of birth, or other descriptions etc. whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual) b. those containing an individual identification code
(ii)	The term “Individual Identification Code” shall mean any character, number, symbol or other codes falling under any of the following and specified by Article 1 of the Cabinet Order to Enforce the Act on the Protection of Personal Information (hereinafter referred to as the “Cabinet Order of the APPI”). a. those character, number, symbol or other codes which are able to identify a specific individual and into which a bodily partial feature of the specific individual has been converted for their usage on computers b. those character, number, symbol or other codes which are assigned in regard to the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated or electromagnetically recorded in a card or other documents issued to an individual in order to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or, stated or recoded for the said user or purchaser, or recipient of issuance
(iii)	The term “Individual Number(s)” shall mean a number obtained by converting a resident record code pursuant to the provisions of the Numbers Act, which is designated for identifying the person to whom the resident record code is assigned (including a number, symbol, or other code that corresponds to the Individual Number and is used in lieu of said Individual Number, excluding the resident record code), and includes not only the number of a living individual but also of a deceased individual.
(iv)	The term “Specific Personal Information” shall mean Personal Information containing the Individual Number as its contents.

- (v) The term “Specific Personal Information, etc.” shall mean the Individual Number and Specific Personal Information.
- (vi) The term “Personal Information File” shall mean a personal information file as set forth in Article 60, Paragraph 2 of the APPI, which is held by an administrative authority, etc. (meaning an administrative authority, etc. as set forth in Article 2, Paragraph (11) of the APPI) or a Personal Information Database, etc. as set forth in Article 16, Paragraph (1) of the APPI, which is held by a person other than an administrative authority, etc.
- (vii) The term “Specific Personal Information File” shall mean a Personal Information File containing the Individual Number as its contents.
- (viii) The term “Personal Data” shall mean personal information constituting a personal information database, etc.
- (ix) The term “Retained personal data” shall mean personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, other than those set down in Article 5 of the Cabinet Order of the APPI as harmful to the public or other interests if their presence or absence is made known.
- (x) The term “Process Using an Individual Number” shall mean a process where administrative authorities, local governments, incorporated administrative agencies, etc., and other persons handling administrative processes handle Individual Numbers to the extent necessary for efficiently searching and managing Personal Information in the Specific Personal Information File that is being held pursuant to the provisions of Article 9, Paragraphs (1) through (3) of the Numbers Act.
- (xi) The term “Process Related to an Individual Number” shall mean a process where another person's Individual Number is used, to the extent necessary, in Processes Using Individual Numbers that are performed pursuant to the provisions of Article 9, Paragraph (4) of the Numbers Act.
- (xii) The term “Person in Charge of a Process Using an Individual Number” shall mean a person who handles Processes Using Individual Numbers and a person who is entrusted with all or part of Processes Using Individual Numbers.
- (xiii) The term “Person in Charge of a Process Related to an Individual Number” shall mean a person who handles Process Related to the Individual Numbers and a person who is entrusted with all or part of Process Related to the Individual Numbers.
- (xiv) The term “Employee” shall mean a person who is directly or indirectly under the direction and supervision of the Bank and is engaged in the business of the Bank. The term “Employee” shall include not only an employee who is in an employment relationship with the Bank (a full-time employee, contract employee, temporary employee, part-time employee, etc.), but also a person who is not in an employment relationship with the Bank (a director, executive officer, council member, auditor, inspector, dispatched employee, etc.).
- (xv) The term “Specific Personal Information Protection Administrator” shall mean a person who is appointed by the Branch Manager within the bank and has responsibility and authority for the implementation and operation of various regulations, etc. related to the protection of Specific Personal Information, etc.
- (xvi) The term “Specific Personal Information Protection Division Manager” shall mean a person appointed by the Specific Personal Information Protection Administrator who has responsibility and authority for the implementation and operation of various regulations, etc. related to the protection of Specific Personal Information, etc. (together with xv above) in each division.
- (xvii) The term “Handling Person of a Process Related to an Individual Number” shall mean an employee who engages in a process handling Individual Numbers within the Bank.
- (xviii) The term “Chief Audit Officer” shall mean a person appointed by the Country Head & CEO (“CH&CEO”) (CEO at Osaka Branch) in the Bank, who has authority for implementing audits

and for reporting from a fair and objective position. (xix) The term “Specific Personal Information Management Area” shall mean the area where the information system that handles the Specific Personal Information File is managed. (xx) The term “Specific Personal Information Handling Area” shall mean the area where the process handling Specific Personal Information, etc. is implemented	(Scope of processes for which the Bank handles Individual Numbers) Article 3 The scope of processes for which the Bank handles Individual Numbers shall be as follows: 1. Processes Related to Individual Numbers pertaining to Customers (i) Processes for application and notification for opening an account related to financial instruments transactions (including application and notification procedures for the use of the Nippon Individual Savings Account) (ii) Processes for preparation and provision of legal documents related to financial instruments transactions (including preparation and provision of written response related to tax examinations by a national tax authority) (iii) Processes for provision to book-entry institutions, etc. information related to financial instruments transactions 2. Processes Related to Individual Numbers pertaining to Employees and their Dependents (i) Processes for preparation of withholding receipts for employment income and retirement income (ii) Processes for notification of employment insurance (iii) Processes for notification of health insurance and employees’ pension insurance 3. Processes Related to the Individual Number pertaining to the Spouse of an Employee (i) Processes for notification of the Spouse falling within Third grade under the National Pension System 4. Processes Related to Individual Numbers pertaining to individuals other than those listed above (i) Processes for preparation of payment records of remuneration and fees, etc. (ii) Processes for preparation of payment records of dividends, distribution of surplus, and interest on funds (iii) Processes for preparing payment records of royalty, etc. for real estate (iv) Processes for preparing payment records of consideration for receiving the transfer of real estate, etc.
(Scope of Specific Personal Information, etc. handled by the Bank) Article 4 The scope of Specific Personal Information, etc. handled by the Bank shall be Individual Numbers used in Processes Related to Individual Numbers conducted by the Bank under the preceding article and Personal Information listed in the following items that is managed in association with Individual Numbers: (i) Identification documents (Individual Number Cards, Identification Documents, etc.), and copies thereof, that have been presented by customers who are individuals or employees of the Bank when implementing measures for verifying their identity pursuant to Article 16 of the Numbers Act. (ii) A statutory record prepared by the Bank for submission to an administrative authority, etc. such as a tax office, and a voucher prepared for submission to a book-entry institution, etc., and a copy thereof (iii) Tax returns, etc. containing the Individual Numbers to be received from customers who are individuals or employees of the Bank in the preparation of statutory record by the Bank	

- (iv) Inquiry documents, etc., received by the Bank for tax examination from a national tax authority, containing the customer's Individual Numbers
- (v) Other information that is stored in association with the Individual Number within the scope of the processes listed in the preceding Article.

Chapter 2 SECURITY MEASURES

Section 1 Organizational and Human Security Measures

(Organizational Structure)

Article 5 The organizational structure pertaining to Processes Related to an Individual Number to be implemented by the Bank shall be as set forth in the following items:

- (i) CH&CEO (CEO at Osaka Branch) shall appoint Compliance Officer (Manager, Compliance at Osaka Branch) as Specific Personal Information Protection Administrator and have him/her perform his/her duties.
- (ii) CH&CEO (CEO at Osaka Branch) shall designate a Risk Department in charge of supervising the inspection and improvement, etc. of the handling of Specific Personal Information, etc.
- (iii) The Specific Personal Information Protection Administrator shall designate the Remittance Section in charge of the Process Related to an Individual Number pertaining to Customers as set forth in Article 3, Paragraph (1) and the General Affairs Section in charge of the Process Related to an Individual Number pertaining to Employees etc. as set forth in Article 3, Paragraphs (2) to (4).
- (iv) The Specific Personal Information Protection Administrator shall appoint AVP (Remittance) and Chief Operating Officer (VP II at Osaka Branch) as the Specific Personal Information Protection Division Manager for the department in charge of the Process Related to an Individual Number as set forth in the preceding item.
- (v) The Specific Personal Information Protection Division Manager of the department handling the Process related to an Individual Number as provided in Item (iii) shall appoint staff of the Remittance Section as appropriate person from the relevant department as the Handling Person of a Process Related to an Individual Number.
- (vi) The Specific Personal Information Protection Administrator may, if necessary, request the Specific Personal Information Protection Division Manager to submit the record pertaining to the Handling Person of a Process Related to an Individual Number.

(Responsibility of the Specific Personal Information Protection Administrator)

Article 6 The Specific Personal Information Protection Administrator shall, under the instruction by CH&CEO (CEO at Osaka Branch) and in accordance with the provision of these Rules, be responsible for establishing internal rules for the protection of Specific Personal Information, implementing security measures, and formulating action plans to promote education and training, etc. and implementing measures such as familiarizing employees with such information.

2. The Specific Personal Information Protection Administrator shall comply with the provisions set forth in these Regulations and shall ensure that they are understood and complied with by the Specific Personal Information Protection Division Manager and the Handling Person of a Process Related to an Individual Number who handles Specific Personal Information, etc. through “acquisition/input,” “use/processing,” “storage/preservation,” “transfer/transmission,” “deletion/disposal,” or “outsourced processing of Specific Personal Information”, etc.
3. The Specific Personal Information Protection Administrator shall be responsible for the businesses listed in the following items:
 - (i) Establishment, revision, or abolition of these Regulations and the criteria for selecting outsourcees.
 - (ii) Appointment of a department handling Process Related to an Individual Number.

(iii) (iv) (v) 4.	- Advice and guidance to, and collection of reports from the Specific Personal Information Protection Division Manager pertaining to the handling status of the Specific Personal Information, etc. - Planning of education and training on the security management of the Specific Personal Information, etc. - Other matters concerning the security management of the Specific Personal Information, etc. at the Bank as a whole. - The Specific Personal Information Protection Administrator for the purpose of formulating and implementing the compliance program.
	(Responsibility of Specific Personal Information Protection Division Manager) Article 7 The Specific Personal Information Protection Division Manager shall understand and comply with the matters stipulated in these Regulations. In addition, in accordance with the advice and guidance of the Specific Personal Information Protection Administrator, the Specific Personal Information Protection Division Manager shall implement education and training to ensure that the Handling Person of a Process Related to an Individual Number understands and complies with these matters, implement security measures, and implement measures such as familiarizing employees with these matters. 2. The Specific Personal Information Protection Division Manager shall be responsible for the businesses listed in the following items in the department in charge: (i) Familiarizing the Handling Person of a Process Related to an Individual Number with these Regulations and the criteria for selection of outsourcees and conducting necessary instructions for compliance therewith (ii) Nominating and recording the Handling Person of a Process Related to an Individual Number (iii) Establishing and amending authority to handle Specific Personal Information, etc. (iv) Approving applications for the use of Specific Personal Information, etc. and managing records, etc. (v) Implementing education and training on the security management of the Specific Personal Information, etc. (vi) Managing records, etc. concerning the Specific Personal Information, etc. (vii) Managing the establishment and change of Specific Personal Information Management Areas and Specific Personal Information Handling Areas (viii) Understanding the handling status of the Specific Personal Information, etc. (ix) Supervising the handling status of the Specific Personal Information, etc. by outsourcees (x) Reporting to and consulting with the Specific Personal Information Protection Administrator concerning the handling status of the Specific Personal Information, etc. (xi) Response to tax examinations by a national tax authority (xii) Other matters concerning the security management of the Specific Personal Information, etc. in the department in charge. 3. The Specific Personal Information Protection Division Manager shall promptly report to the Specific Personal Information Protection Administrator if he or she finds the fact or sign of violation of the Numbers Act, the APPI, or other relevant laws and regulations, guidelines, these Regulations, or other internal rules and regulations, such as leakage, loss or damage of Specific Personal Information, etc. (hereinafter referred to as the “Leakage, etc.”).
	(Supervision of the Handling Person of a Process Related to an Individual Number) Article 8 The Specific Personal Information Protection Division Manager shall conduct necessary and appropriate supervision of the Handling Person of a Process Related to an Individual Number so that the Specific Personal Information, etc. will be handled appropriately pursuant to these Regulations, and shall regularly report to the Specific Personal Information Protection Administrator the handling status of the Specific Personal

Information, etc.
(Responsibilities of the Handling Person of a Process Related to an Individual Number) Article 9 The Handling Person of a Process Related to an Individual Number shall, when engaging in the business of handling Specific Personal Information, etc., such as “acquisition/input,” “use/processing,” “storage/preservation,” “transfer/transmission,” “deletion/disposal,” or outsourced processing, etc. of the Specific Personal Information, etc., conduct their business with due care to protect the Specific Personal Information, etc., in accordance with the Numbers Act and other relevant laws and regulations, guidelines, these Regulations, and other internal regulations as well as instructions given by the Specific Personal Information Protection Division Manager. 2. When a Handling Person of a Process Related to an Individual Number is aware of a fact or sign of violation of the Numbers Act or the APPI, or other relevant laws and regulations, guidelines, these Regulations, or other internal regulations, such as Leakage, etc. of the Specific Personal Information, etc., he/she shall promptly report to the Specific Personal Information Protection Division Manager or the Specific Personal Information Protection Administrator 3. A Handling Person of a Process Related to an Individual Number who merely receives a document, etc. containing an Individual Number without confirming the contents of such document, etc. shall, upon receipt of said document, immediately circulates said document to a Handling Person of a Process Related to an Individual Number who performs the identification under the Numbers Act in a non-leaking manner, and shall not leave an Individual Number in his/her possession.
(Education and Training) Article 10 The Specific Personal Information Protection Administrator shall be responsible for planning and operating the education and training necessary to ensure that the Handling Person of a Process Related to an Individual Number complies with these Regulations. 2. The Specific Personal Information Protection Division Manager shall implement education and training necessary to ensure that the Handling Person of a Process Related to an Individual Number complies with these Regulations in accordance with the planning and guidance of the Specific Personal Information Protection Administrator. 3. The Handling Person of a Process Related to an Individual Number shall receive education to ensure compliance with these Regulations conducted by the Specific Personal Information Protection Division Manager.
(Administrative Flow Pertaining to Preparation of Statutory Record) Article 11 The administrative flow for preparing statutory record such as withholding receipts and payment records shall be stipulated separately.
(Records of Operation Status Based on these Regulations) Article 12 The Handling Person of a Process Related to an Individual Number shall record the status of use of the Specific Personal Information, etc. with regard to the items listed in the following items in order to confirm the status of operation based on these Regulations: (i) Records of the status of acquisition of the Specific Personal Information, etc. and input into the Specific Personal Information File (ii) Records of the status of use and output of the Specific Personal Information File (iii) Records of the transfer of documents and media, etc. containing the Specific Personal Information, etc. (iv) Records of deletion and disposal of the Specific Personal Information File (v) If deletion or disposal is outsourced, records certifying the deletion or disposal is outsourced and records certifying that the outsourcee has properly deleted or disposed of the Specific Personal Information File.

(vi) If the Specific Personal Information File is handled by the information system, record the usage of the information system (login results, access logs, etc.) by the Handling Person of a Process Related to an Individual Number.
(Means for Confirming the Handling Status) Article 13 The Handling Person of a Process Related to an Individual Number shall, as a means of confirming the handling status of the Specific Personal Information File, record the matters listed in the following items in addition to the entries in the Customer Record Maintenance Data Base System referred in the item (vi) of the Article 12 above for the Specific Personal Information, etc. (no duplicate items are required): Specific Personal Information, etc. shall not be entered in the management ledger for Specific Personal Information, etc. (i) Type and name of the Specific Personal Information File (ii) Person in charge and the department in charge of handling (iii) Purpose of use (iv) Status of deletion/disposal (v) Persons who have an authority to access (vi) Location of the “Specific Personal Information Management Area” of the information system handling the Specific Personal Information File (vii) Location of the “Specific Personal Information Handling Area” where processes handling the Specific Personal Information, etc. are to be conducted 2. The Specific Personal Information Protection Division Manager shall manage and supervise the Handling Person of a Process Related to an Individual Number to properly perform the records set forth in each item of the preceding paragraph.
(Response to Leakage, etc. Incident of Specific Personal Information, etc.) Article 14 The Specific Personal Information Protection Administrator shall, in the event of an incident involving the Leakage, etc. of the Individual Numbers or the Specific Personal Information, etc. or risks thereof (hereinafter referred to as the “Leakage, etc. Incident”), we will respond appropriately, such as by submitting a report to relevant competent authorities, or notifying the customer thereof, in accordance with the provisions of Laws and Regulations and following measures. (i) Promptly submit necessary reports to the Financial Services Agency and the Personal Information Protection Commission. (ii) From the viewpoint of preventing secondary damage and avoiding the occurrence of similar cases, the facts of leakage, etc. and measures to prevent recurrence shall be publicly announced in a prompt manner. (iii) Promptly notify the information subject who was the subject of the Leakage, etc. Incident of Specific Personal Information, etc. of the facts of the incident, etc.
(Response to Complaints) Article 15 When the Handling Person of a Process Related to an Individual Number receives a complaint from the information subject with regard to the Number Act, the APPI, the guidelines for the protection of the Specific Personal Information, etc. or these Regulations, such person shall report it to the Specific Personal Information Protection Division Manager. The Specific Personal Information Protection Division Manager who receives the report shall report to the Specific Personal Information Protection Administrator and respond appropriately.
(Audit) Article 16. CH&CEO (CEO at Osaka Branch) shall appoint VP Risk as Chief Audit Officer and shall have such person to conduct audits regularly to audit the fact that the Bank’s internal specific personal information management is being implemented appropriately in

accordance with the various provisions, etc. relating to the specific personal information protection. However, an external person who has been separately appointed on the order of the Branch Manager may be added when it is necessary to do so for operational purposes. 2. The Chief Audit Officer shall prepare and implement an audit program in accordance with the internal audit regulations. 3. The Chief Audit Officer shall put together an audit report and submit it to CH&CEO (CEO at Osaka Branch). If there has been a breach of law, the Branch Manager shall provide directions for the required improvements to the Specific Personal Information Protection Administrator and other persons concerned. 4. In addition to promptly implementing measures for making the required improvements, the person who has received directions for improvement shall report the contents to the Chief Audit Officer. 5. The Chief Audit Officer shall evaluate the improvement contents and shall report such evaluations to CH&CEO (CEO at Osaka Branch) and the Specific Personal Information Protection Administrator.
(Review) Article 17. CH&CEO (CEO at Osaka Branch) shall instruct the Specific Personal Information Protection Administrator to regularly review the various regulations, etc. on specific personal information protection to maintain appropriate specific personal information protection in light of audit reports and other business environments, etc.
Section 2 Physical Security Measures (Management of Areas where Specific Personal Information is dealt with) Article 18 The Specific Personal Information Protection Division Manager shall clarify the Specific Personal Information Management Area and the Specific Personal Information Handling Area of the Bank (hereinafter in this article, Articles 19 and 20 referred to simply as the “Management Area” and the “Handling Area”) and shall take the measures specified in the following items for each area, according to the respective areas listed in the respective items. (i) Management Area Refer to the IT Policy and Standards 6.0 of the Branches in Japan for the management of entrance and exit and restrictions on equipment and electronic media to be brought into the Management Area shall be implemented. (ii) Handling Area In addition to security measures for the protection of personal information, a measures as allocating seats to places where there is scarce human for the Handling Person of a Process Related to an Individual Number shall be implemented.
(Prevention of Theft, etc. of Equipment and Electronic Media, etc.) Article 19 The Specific Personal Information Protection Division Manager shall take the measures listed in the following items in order to prevent theft or loss of equipment, electronic media, documents, etc. handling Specific Personal Information, etc. in the Management Area and the Handling Area: (i) Equipment, electronic media, documents, etc. handling Specific Personal Information, etc. shall be stored in lockable cabinets, archives, etc. (ii) When the information system handling the Specific Personal Information File is operated only by the equipment, it shall be fixed using security wires, etc.
(Prevention of Leakage, etc. in the Case of Transfer of Electronic Media, etc.) Article 20 The transfer of electronic media or documents, etc. on which Specific Personal

Information, etc. is recorded (which means the transfer of Specific Personal Information, etc. outside the Management Area or the Handling Area or the transfer of Specific Personal Information, etc. from outside the said area to the said area, including the transfer, etc. within the offices) shall be prohibited except in the following cases: (i) Cases where data is provided to an outsourcee pertaining to Processes Related to an Individual Number within the scope deemed necessary for the implementation of the processes to be entrusted (ii) Cases where data or documents are provided to the Person in Charge of a Process Using an Individual Number with regard to the Process Related to an Individual Number to be implemented by the Bank, such as submission of a statutory record to an administrative authority, etc. (iii) Cases where transferring from the Handling Area to another Handling Area, temporarily passing through a common floor, etc. (limited to the case of passing through a route predetermined by the administrative flow) (iv) Cases where a national tax authority visits as tax examination and present the inquiry documents, etc. containing the Individual Numbers and the Bank transfers such inquiry documents, etc. to the Management Area. (v) Other cases where a transfer request is made to and approved by the Specific Personal Information Protection Division Manager. 2. When transferring electronic media or documents, etc. on which Specific Personal Information, etc. is recorded pursuant to the preceding paragraph, one or more of the security measures prescribed in the following items shall be taken in accordance with the method of safe transfer of the transport media listed in the respective items. Provided, however, that when submitting a statutory record, etc. to an administrative authority, etc. in the form of data, the method of submission designated by the administrative authority, etc. shall be followed. (i) Method of safely transporting electronic media on which Specific Personal Information, etc. is recorded a. Encryption of transport data b. Password protection of transport data c. Use of transport containers that can be locked d. Use of traceable transport means (ii) Method of safely transferring documents, etc. containing Specific Personal Information, etc. (including the case of transferring documents, etc. containing Specific Personal Information, etc. from a Handling Person of a Process Related to an Individual Number in each department to a Handling Person of a Process Related to an Individual Number in another department) a. Seal b. Attachment of blindfold sticker c. Transfer by special case or bag	(Physical Security Measures at the Disposal/ Deletion Stages) Article 21 The management of recording media, etc. at the stage of disposal or deletion of Specific Personal Information, etc. shall be as listed in the following items: (i) When disposing of documents containing Specific Personal Information, etc., the Bank shall use non-recoverable means such as shredding of such records by shredder, etc., masking the Individual Number portion to the extent that it is impossible to restore it, and incineration/dissolution at the Company's own or an external incinerator. (ii) When the Bank disposes of equipment and electronic media containing Specific Personal Information, etc., the Bank shall use non-recoverable means by using the special data deletion software or by physical destruction, etc.
--	---

(iii) (iv) (v) (vi) 2. 3.	When deleting Individual Numbers or certain Specific Personal Information in a Specific Personal Information File, the Bank shall use measures that deleted Individual Numbers or Specific Personal Information cannot be easily restored. In an information system that handles Specific Personal Information, etc., such information system shall be established so that the Individual Numbers shall be deleted as soon as possible after the statutory retention period of the relevant statutory record has expired. Documents containing the Individual Numbers shall be disposed of as soon as possible after the legal retention period of the relevant statutory record has expired. If an Individual Number is stated in an inquiry document, etc. received from a national tax authority at the tax examination, the relevant Individual Number shall be deleted or destroyed irrespective of whether or not it belongs to an existing customer promptly after the achievement of the purpose of use. In case where the Handling Person of a Process Related to an Individual Number has deleted the Individual Numbers or the Specific Personal Information File, or disposed of the electronic media, etc. handling Specific Personal Information, etc., such Handling Person of a Process Related to an Individual Number shall retain the record of deletion or disposal. The record of deletion or disposal shall include the type and name of the Specific Personal Information File, the person in charge and the handling department, and the status of deletion or disposal, but shall not include the Individual Number itself. The Specific Personal Information Protection Division Manager shall manage and supervise the Handling Person of a Process Related to an Individual Number to properly perform the operations set forth in paragraph 1 and the records set forth in the preceding paragraph.
Section 3 Technical Security Measures (Access Control)	Article 22 Access control to Specific Personal Information shall be as follows. (i) Limit information system terminals, etc. that can handle Specific Personal Information Files. (ii) Limit the Specific Personal information Files that can be accessed in each information system. (iii) Limit the number of persons who can use the information system that handles the Specific Personal Information File by granting access rights to the User ID.
(Identification and Authentication of those who have Access rights)	Article 23 The information system handling Specific Personal Information, etc. shall authenticate that the Handling Person of a Process Related to an Individual Number is a person with legitimate access rights by means of identifying the User ID, password, magnetic and IC cards, etc., based on the results of identification.
(Prevention of Unauthorized Access, etc. from Outside)	Article 24 The Bank shall protect the information system from unauthorized access from outside or unauthorized software by using each of the following methods: (i) A method for blocking unauthorized access by installing a firewall, etc. at a connection point between the information system and an external network. (ii) A method of checking the existence of unauthorized software by introducing security software, etc. (anti-virus software, etc.) into information systems and equipment. (iii) A method of keeping software, etc. updated by utilizing the automatic updating function, etc. provided as standard equipment and software. (iv) A method of detecting unauthorized access, etc. by periodically analyzing logs, etc.
(Prevention of Leakage, etc. of Specific Personal Information, etc.)	Article 25 The Bank shall prevent Leakage, etc. of Specific Personal Information, etc. through communication channels and Leakage, etc. of Specific Personal Information, etc. stored in an information system when Specific Personal Information, etc. is transmitted

externally via the internet, etc. (i) Measures to Prevent Leakage, etc. in Communication Channels Encryption of communication channels (ii) Measures to Prevent Leakage, etc. of Specific Personal Information, etc. Stored in an Information System Protection by data encryption or password
Section 4 Understanding of External Environment (Understanding of External Environment) Article 26 When the Bank handles Specific Personal Information, etc. in a foreign country, the Bank shall take necessary and appropriate measures for the security management of Specific Personal Information, etc. after understanding the foreign country's regulatory regime, etc. concerning the protection of Personal Information in the foreign country.
Chapter 3 Acquisition of Specific Personal Information, etc.
(Purpose of Use of Individual Numbers) Article 27 The purpose of use of the Individual Numbers that the Bank acquires from customers, employees, or third parties shall be within the scope of the processes to handle the Individual Numbers set forth in Article 3.
(Notice, etc. of Purpose of Use upon Acquisition of Individual Numbers) Article 28 The Bank shall post or keep a document at the office for the purpose of use of the Individual Numbers and publish it on its website on the Internet. When acquiring Individual Numbers from the Bank employees, notice on the internal LAN, presentation of documents describing the purpose of use, and clear stipulation in the work rules shall be conducted. 2. In the event of a change in the purpose of use, the Bank shall change the purpose of use to the extent reasonably recognizable that the change is reasonably related to the original purpose of use and notify, publicly announce, or express such change to the information subject.
(Request for Provision of Individual Numbers) Article 29 The Bank shall be entitled to request the information subject or other Person in Charge of a Process Related to an Individual Number or Person in Charge of a Process Using and Individual Number to provide the Individual Numbers only when it is necessary for the administration of the processes set forth in Article 3.
(Timing for Requesting the Provision of Individual Numbers) Article 30 The Bank will request the provision of Individual Numbers when necessary for the processes set forth in Article 3. 2. The Bank shall request customers to provide Individual Numbers in the following cases: (i) Upon receipt of an application for opening a comprehensive trading account (ii) Upon receipt of an application for opening a NISA account (iii) In other cases which may be required.
(Restriction on Request for Provision of Individual Numbers) Article 31 The Bank shall not request an information subject or a third party (including other Persons in Charge of a Process Related to an Individual Number or Persons in Charge of a Process Using an Individual Number) to provide an Individual Number except in the case where any of the items of Article 3 is applicable and the Bank is able to receive the Individual Number.
(Restriction on Collection of Specific Personal Information, etc.)

Article 32	The Bank shall not collect Specific Personal Information, etc. from an information subject or a third party beyond the scope of the processes set forth in Article 3.
(Identity Verification)	
Article 33	When obtaining an Individual Number from an information subject or its agent, the Bank shall verify the Individual Numbers of customers, employees or third parties and verify the identity of such persons in accordance with the methods stipulated in Article 16 of the Numbers Act and the tax legislations. In addition, with regard to an agent, the Bank shall verify the identity of the agent, the authority of representation, and the Individual Number of the information subject in accordance with the methods set forth in the same article.
(Handling at the Acquisition Stage)	
Article 34	Handling of Specific Personal Information, etc. at the acquisition stage shall be in accordance with the Desk Manual for Remittance.
Chapter 4 Use of Specific Personal Information, etc.	
(Restrictions on the Use of Individual Numbers)	
Article 35	The Bank shall use Individual Numbers only within the scope of the purpose of use set forth in Article 27.
2.	The Bank shall not use Individual Numbers beyond the purpose of use even with the consent of the information subject, except in the cases listed in the following items:
(i)	Cases where money is paid to customers in the event of designation of an extreme disaster, etc.
(ii)	Cases where it is necessary for the protection of the life, body or property of persons
(Restrictions on the Preparation of Specific Personal Information Files)	
Article 36	The Bank shall create a Specific Personal Information File only to the extent necessary to conduct the processes set forth in Article 3 hereof and shall not create a Specific Personal Information File for other cases.
(Handling at the Use Stage)	
Article 37	Handling of Specific Personal Information, etc. at the use stage shall be in accordance with the Notice documents as per Article 28.
Chapter 5 Storage or Preservation of Specific Personal Information, etc.	
(Restrictions on Storage or Preservation of Specific Personal Information, etc.)	
Article 38	The Bank shall not retain or preserve Specific Personal Information, etc. beyond the scope of the processes set forth in Article 3.
2.	Until the expiration of the retention period of the documents containing the Individual Numbers stipulated by the relevant laws and regulations, the Bank may retain such documents not only in hardcopies but also within the system in which such documents are created.
3.	The Bank shall retain or preserve as Specific Personal Information a copy of the identity verification documents (such as the Individual Number Card) presented when implementing measures for identity verification under the Numbers Act, a copy of the statutory record that the Bank submits to an administrative authority, etc., and a return form, etc. containing the Individual Number to be received by the business operator in preparing the statutory record.
(Handling at the Storage or Preservation Stage)	
Article 39	Handling of Specific Personal Information, etc. at the storage or preservation stage shall be in accordance with the Fuban Guidelines.

Chapter 6 Provision of Specific Personal Information, etc.	
(Restriction on Provision of Specific Personal Information, etc.)	
Article 40	Except for the cases listed in the items of Article 19 of the Numbers Act, the Bank shall not provide Specific Personal Information, etc. to a third party (meaning the transfer of Specific Personal Information, etc. that transcends legal personality and does not apply to the transfer of Specific Personal Information, etc. that does not transcend legal personality of the same juridical person) with or without the consent of the Customer.
(Handling at the Provision Stage)	
Article 41	Handling of Specific Personal Information, etc. at the transfer or transmission stage shall be in accordance with the Notice documents as per Article 28.
Chapter 7 Disclosure of Specific Personal Information, etc.	
(Disclosure of Specific Personal Information, etc.)	
Article 42	Where the Bank is requested by an information subject to disclose a Specific Personal Information File in which the information subject is identified, the Bank shall comply with the request to the extent that the information subject has requested disclosure after rigorously verifying that the information subject is the subject of said information in accordance with the procedures and methods prescribed in the Personal Information Protection Rules and Regulations. When sending a copy of the statutory record to the information subject, if a copy of the statutory record contains an Individual Number of other persons, such part shall be masked, etc.
2.	Where the Bank is requested by an information subject to disclose whether or not an Individual Number has been held pursuant to the preceding paragraph, the Bank shall only respond whether or not an Individual Number has been held.
3.	In the event of any of the following items, the Bank may not accept a disclosure request in whole or in part, and in such event the Bank shall explain to the requester to that effect and the reason therefor (indicating the provisions of the APPI which served as the basis for its judgment and the fact which serves as the basis for its judgment):
(i)	Cases where disclosure is likely to harm the life, body, property, or other rights or interests of the information subject or a third party
(ii)	Cases where there is a risk of causing a serious hindrance to the proper performance of the Bank's business.
(iii)	Cases where disclosure violates other laws and regulations
Chapter 8 Deletion or Disposal of Specific Personal Information, etc.	
(Deletion or Disposal of Specific Personal Information, etc.)	
Article 43	The Bank shall continue to collect or retain Specific Personal Information, etc. only to the extent it is necessary for the processes set forth in Article 3. The Individual Numbers stated in the documents, etc. shall be retained for a certain period of time if such documents, etc. are required to be retained for a certain period of time by the relevant laws and regulations. In the event that it is no longer necessary to handle such documents, and the retention period specified by the relevant laws and regulations has expired, the Individual Numbers shall be deleted or disposed of as soon as possible. In addition, if the Individual Number is stated in the inquiry document, etc. received from a national tax authority through the tax examination, the relevant Individual Number shall be deleted or disposed of irrespective of whether or not it belongs to an existing customer immediately after the achievement of the purpose of use.
(Handling at the Elimination or Disposal Stage)	
Article 44	Handling of Specific Personal Information at the deletion or disposal stage shall be in accordance with the Desk Manual for Remittance (Control Register of Personal Data.for

Osaka Branch) .	
Chapter 9 Handling of Entrustment of Specific Personal Information, etc.	
(Security Measures by Outsourcees)	
Article 45	In the event the Bank entrusts all or part of the Process Related to an Individual Number [or the Process Using an Individual Number, the Bank shall conduct necessary and appropriate supervision to ensure that the outsourcee properly takes measures equivalent to the security measures that the Bank is to implement. In order to conduct such supervision, the Bank shall comply with these Regulations as well as Regulations on Management of Outsourcing.
2.	The “necessary and appropriate supervision” set forth in the preceding paragraph shall include the matters listed in the following items:
(i)	Appropriate selection of outsourcees
(ii)	Conclusion of a contract necessary to have the outsourcee comply with the security measures
(iii)	Understanding of the handling status of Specific Personal Information, etc. at the outsourcee
3.	The “appropriate selection of outsourcees” set forth in item (i) of the preceding paragraph shall be confirmed in advance as to whether the following matters satisfy the level prescribed by the Bank with regard to the protection of Specific Personal Information, etc.
(i)	Equipment
(ii)	Level of technology
(iii)	The status of supervision and education of employees (meaning those who are in the organization of a business operator and are directly or indirectly engaged in the business of the business operator under the direction and supervision of the business operator. Specifically, including directors, auditors, council member, inspectors, dispatched employees, etc. in addition to employees)
(iv)	Management Conditions
(v)	Status of security management of Specific Personal Information, etc. (including, but not limited to, “Clarification of the scope of processes handling Individual Numbers,” “Clarification of the scope of Specific Personal Information, etc.,” “Clarification of the Handling Person of a Process Related to an Individual Number,” and “Deletion of Individual Numbers, Disposal of Equipment and Electronic Media, etc.”)
(vi)	The outsourcee does not fall under any person who is an organized crime group, an organized crime group member, for whom less than five years have passed since it ceased to be an organized crime group member, an associated member of an organized crime group, a corporation related to an organized crime group, a corporate racketeer, etc., a corporate swindler acting in the name of a social movement, or an organized crime group that utilizes specialized knowledge, etc. or any other person equivalent thereto (hereinafter collectively referred to as “Anti-social Forces”) or any of the following (a) through (e)
a.	any person who has a relationship in which Anti-social Forces are deemed to control its management
b.	any person who has a relationship in which Anti-social Forces are deemed to be substantially involved in the management
c.	any person who has a relationship in which it is deemed to wrongly use Anti-social Forces for the purposes of seeking to obtain unfair profit for itself, its company or a third party, or causing damage to a third party, or for other such purposes
d.	any person who has a relationship in which it is deemed to provide funds or benefits to Anti-social Forces
e.	a director or a person substantially involved in the management has a relationship with Anti-social Forces that should be socially condemned

4.	The provisions of the following items shall be included as the contents of the outsourcing contract with regard to the “conclusion of a contract necessary to have the outsourcee comply with the security measures” stipulated in Paragraph (2), Item (ii).
(i)	Provisions relating to the obligation of confidentiality
(ii)	Prohibition of Removal of Specific Personal Information, etc. from the business facilities to outside
(iii)	Prohibition of Use of Specific Personal Information, etc. for other purposes
(iv)	Conditions for re-outsourcing
(v)	Provisions on the responsibilities of the outsourcee in the event of a case of Leakage, etc. Incident
(vi)	Provisions on the return or disposal of Specific Personal Information, etc. after the termination of the outsourcing contract
(vii)	Provisions on supervision and education of employees
(viii)	Provisions concerning the provisions requiring the submission of reports on the status of compliance with the contents of the contract
(ix)	Provisions on the clarification of employees handling Specific Personal Information, etc.
(x)	Provisions that allow the Bank to conduct on-site investigations of entrustment parties
5.	The Bank designates that VP (Compliance) (VP11 at Osaka Branch) shall be responsible for the management of outsourcees.
6.	The Bank shall monitor periodically and where necessary the proper security management of Specific Personal Information, etc. by the outsourcee.
7.	The Bank shall confirm that there is a system that in the event of a Leakage, etc. Incident at the outsourcee, appropriate measures are taken and it will be promptly reported to the Bank.
8.	The outsourcee may re-entrust all or part of the entrusted Processes Related to an Individual Number [or Processes Using an Individual Number] only with the authorization of the Bank. The same shall apply to the further re-outsourcing by the re-outsourcee.
9.	The Bank shall not only judge whether or not the re-outsourcee is appropriate, but also supervise whether or not the outsourcee is conducting necessary and appropriate supervision of the re-outsourcee.
10.	In the event the outsourcee re-entrust the entrusted processes, the Bank shall have the outsourcee include the same provisions as in Paragraph (4) as the content of such re-outsourcing agreement.
Supplementary Provisions	
(Effective Date)	
Article 1	These Regulations shall be effective as of 20/01/2023.
(Alteration or Abolition of Rules)	
Article 2	Amendment or abolishment of these Regulations shall be drafted by the Specific Personal Information Protection Administrator and approved by the Branch Management Committee.