King’s Town Bank Personal Data Breach Emergency Response Guideline

Formulated 05-31-2013
Amended on 03-10-2014
Amended 07-15-2015
Amended 02-19-2016
Amended 11-21-2018
Amended 11-05-2020
Amended 01-13-2022
Amended 06-07-2022

Article 1 Purpose

The purpose of this document is to establish the principles and procedures for handling personal data breaches at the Bank. The goal is to ensure that problems can be resolved quickly and effectively when they occur and that damage can be minimized.

Article 2 Definitions and Scope

I. Personal data breach: An incident that results in a security breach or threat to the personal data held by the Bank due to intentional or unintentional human error or force majeure. For example: Personal data is stolen, disclosed, altered, or otherwise infringed upon. This is further divided into:
   (I) Personal data breaches involving cyber security: personal data breaches involving information processing documents or data containing personal data in the Bank’s confidential and sensitive information assets.
   (II) personal data breaches not involving cyber security: personal data breaches that do not involve cyber security.

II. Major personal data breach: An incident where the theft, alteration, damage, destruction, or disclosure of personal data will endanger the normal operation of the Bank or the rights and interests of a large number of data owners.

III. When a personal data breach occurs, the provisions of this Guideline shall apply. However, personal data breaches caused by “disasters” as defined in the Bank’s “Emergency Response Guideline” shall be handled according to the Bank’s “Emergency Response Guideline” and shall not be subject to the provisions of this Guideline.

IV. The term "disaster" in the preceding Paragraph refers to a regional or local disaster (including fire, wind, water, earthquake, other destruction, and major epidemics) that causes damage or loss of important files (data) in units (including management and business departments) located in the disaster area, resulting in the inability to maintain normal business operations and the necessity for external support.

V. This Guideline specifies the general principles for handling personal data incidents. However, the procedures may be adjusted according to the actual situation for personal data incidents involving cyber security.

Article 3 Responsibilities

I. General Manager

Coordinate matters related to the implementation of emergency response measures by the Personal Data Protection Management Executive Committee (hereinafter "Personal Data Committee") and the business units when a personal data breach occurs.

II. Personal Data Committee

(I) Supervise the reporting and response of personal data breaches.

(II) Responsible for the coordination of personal data protection resources and process improvement.

(III) Responsible for supervising the implementation of corrective measures for personal data breaches and verifying the effectiveness of preventive measures.

(IV) Coordinate the contact for personal data breaches in each business unit.

(V) Designate the affiliated administrative unit as the contact for the Personal Data Committee according to the Bank's "Personal Data File Security Maintenance Regulation."

(VI) Evaluate external matters after a personal data breach occurs. Determine whether it is a "major accidental event," a "major personal data breach," or other related legal liabilities.

III. Personal Data Committee Administrative Unit

(I) Act as the contact for the Personal Data Committee, notify the business unit when a personal data breach is reported, and make a preliminary judgment on the nature of the incident jointly with the relevant personnel.

(II) Track the results of the subsequent emergency response measures.

IV. Business Units of the Head Office

(I) The person responsible for the security of personal data files in each business unit shall act as the contact for personal data breaches in the unit.

(II) When it becomes known that a suspected personal data breach has occurred, the unit shall collect evidence from the relevant personnel, assist in clarifying the facts, and collect relevant evidence.

(III) Handle the identification (understanding the cause, scope of impact, etc.), containment (reducing losses), elimination (problems), and recovery of personal data breaches.

(IV) Respond to emergency response matters and handling results.

V. Unit Where the Personal Data Breach Occurs

(I) Report the personal data breach that occurred in the unit, and the supervisor or deputy supervisor of the operation shall act as the contact and report to the supervisor of the unit.

(II) Assist in handling the identification, containment, elimination and recovery of personal data breaches.

VI. All Colleagues of the Bank

(I) Assist and cooperate in the reporting and handling of personal data breaches.

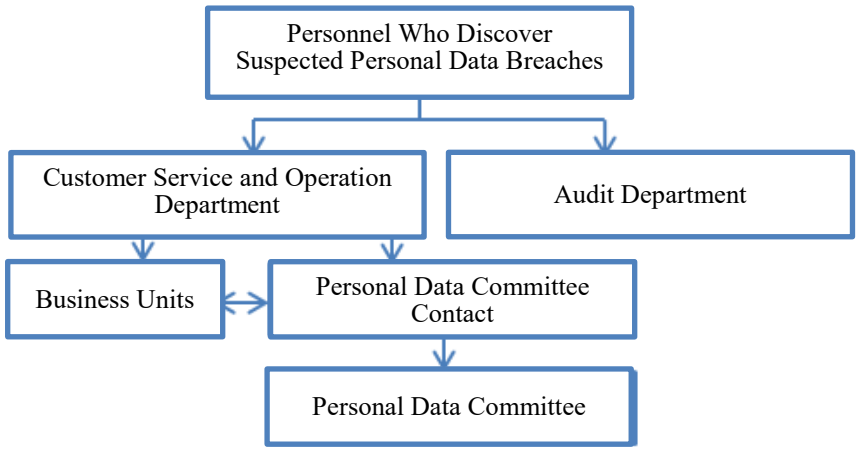
(II) Understand the personal data breach reporting process and assist in reporting to the business unit.

VII. Outsourced Vendors and Personnel

Comply with laws and regulations and the Bank’s relevant personal data protection management provisions.

Article 4 Personal Data Breach Reporting and Acceptance

I. Personal Data Breach Reporting and Acceptance Flowchart



II. Personal Data Breach Reporting and Acceptance Process

(I) Reporting Principles

1. When a personal data breach occurs, it shall be reported according to the flowchart in the previous Paragraph.
2. When personnel at any level cannot be reported according to the previous process, the personnel responsible for reporting should directly report to the next level to ensure the timeliness of the reporting procedure.

(II) Explanation of the Reporting and Acceptance Process

1. When each unit discovers a suspected personal data breach, it shall first report it to the Customer Service and Operation Department and notify the Audit Department. Then, the Customer Service and Operation Department shall notify the Personal Data Committee Contact and the business unit. If a customer reacts to a suspected personal data breach, the customer's name and contact information must also be kept for subsequent contact.
2. After receiving the notification, the Personal Data Committee Contact shall contact the personal data file security maintenance personnel of the relevant business unit. The business unit shall assist in understanding the facts of the reported incident and collecting relevant evidence (the cause of the incident, estimated impact range, etc.) to facilitate the Personal Data Committee Contact to record the matter in the Bank's "Personal Data Breach Handling Notification and Record Form" (hereinafter the "record form").

3. Judgment of Personal Data Breach:
   (1) The Personal Data Committee Contact shall invite personnel from the Risk Management Department and the business unit, and the Audit Department shall be asked to attend. Based on the record form and relevant information, it shall be judged whether the reported case involves a personal data breach. However, if the reported case is clearly identifiable, the Personal Data Committee Contact may make a direct judgment and notify the aforementioned units by email.
   (2) If it is determined that it is not a "personal data breach" (i.e., the exercise of rights or complaint cases under Article 11 of the Personal Data Protection Act), it shall be transferred to the business unit or complaint channel for handling and filed for closing. If it is a "personal data breach," the Personal Data Committee convener shall be notified.
4. The notification and acceptance of personal data breaches shall be completed within one day after receiving the notification but may be extended depending on the complexity of the reported incident.

Article 5 Emergency Response Measures for Personal Data Incidents

I. Convening the Personal Data Committee Meeting
   (I) After confirming the "personal data breach," the Personal Data Committee Contact shall submit the record form and relevant information to the convener. The convener shall assess whether to convene a "Personal Data Committee Meeting" based on the circumstances of the breach.
   (II) There is no need to convene a "Personal Data Committee Meeting" under any of the following circumstances:
      1. Personal data breaches involving cyber security shall be convened by the Bank's information security promotion unit to assess whether to convene an "Emergency Response Team Meeting" (the meeting content includes personal data breach issues).
      2. The circumstances of the incident are minor and do not affect the Bank's operations or only affect the rights of a few data subjects.
   (III) If the Personal Data Committee Meeting is not convened due to the minor circumstances of the breach (i.e., the second type of the previous item), the convener shall directly instruct the business unit to handle the emergency response measures.
   (IV) Emergency response measures for personal data breaches must include the following contents: methods to control the damage to the data subjects involved, appropriate methods to notify the data subjects involved after the breach is found out, the facts of the breach, the response measures taken, and the consultation service hotline.

(V) If the personal data breach is reviewed by the Personal Data Committee or the emergency response team and deemed to be a "major personal data breach" due to Type 1 in Item 2 of this Subparagraph, the Compliance Department shall notify the competent authority within 72 hours after the discovery of the personal data breach (including holidays in the deadline calculation) according to the "Regulations Governing Security Measures of the Personal Information File for Non-government Agencies Designated by Financial Supervisory Commission." If it also meets the definition of a "major accidental event," the Audit Department shall notify the competent authority according to the "Financial Institution Reporting Procedures for Major Incidents and Other Compliance Matters" and the "King's Town Bank Major Incident Handling Mechanism."

II. Implementation of Emergency Response Measures

(I) The business unit shall implement emergency response measures as instructed and report the handling status to the unit supervisor at any time to adjust the response measures as appropriate.

(II) After the preliminary determination of the breach is eliminated, the business unit supervisor shall still closely monitor the relevant operations and conduct necessary investigations to prevent potential breach from recurring.

(III) The business unit shall eliminate the problem within 3 days from the date of the breach, but this may be extended depending on the complexity of the breach.

(IV) After the problem is eliminated, the business unit shall record the handling result (including the handling status and actual impact range) in the "Record Form", report it to the unit supervisor, and then forward it to the Personal Data Committee Contact for feedback to the convener and Personal Data Committee member.

III. Post-Processing and Review and Improvement

(I) After the personal data breach is confirmed to be completed, the business unit shall formulate corrective and preventive measures and record them in the "Personal Data Breach Correction and Prevention Handling Form." The convener may convene another Personal Data Committee meeting to review the cause of the breach and the completeness of the existing security control measures if necessary and review the performance of the corrective and preventive measures proposed by the business unit to avoid similar breaches from recurring.

(II) If it is a "major personal data breach," the corrective and preventive measures it has researched shall be conducted by a fair, independent, and qualified expert with relevant recognized qualifications for overall diagnosis and review.

(III) If any compensation is involved, the Personal Data Committee shall discuss the content of the compensation and instruct the relevant units to notify the data subjects involved.

(IV) If the Personal Data Committee meeting is not convened after the review, the business unit shall still fill in the “Personal Data Breach Correction and Prevention Handling Form” and send it to the Personal Data Committee Contact for the Personal Data Committee members to review.

Article 6 Additional Provisions

I. Regular personal data breach drills and tests shall be conducted annually to improve the efficiency and response capabilities of handling personal data incidents.

II. All relevant documents related to the personal data breach response and handling process (including drill records) shall be kept for at least 5 years for inspection.

III. Matters not covered by this Guideline shall be handled according to the relevant provisions of each business unit.

IV. This Guideline shall be implemented after approval by the General Manager, and the same shall apply to its amendments.

Attachment 1. King's Town Bank Personal Data Breach Handling Notification and Record Form

I. Basic Information of the Reporting Unit ＊ If it is a customer response, fields 1 to 6 must be filled in; if it is not a customer response, only fields 1 and 2 need to be filled in.
1. Report Time: Year Month Day
2. Notifying unit: ○○ Branch/○○ Department/○○ Credit Center
3. Customer name:
4. Customer Telephone:
5. Customer Email:

II. Incident Notification Matters
1. Occurrence Date:_____Year_____Month_____Day_____Hou_____Minute
2. Incident description (briefly describe the cause of the incident, status, possible scope of impact, etc. The reporting unit or business management unit shall cooperate to provide relevant evidence.)

III. Incident Handling and Determination Result

1. Acceptance Time:_____Year_____Month_____Day	Acceptance number:

2. Preliminary Analysis and Determination

☐ Determination by the Personal Data Committee Contact and relevant units;

☐ The Personal Data Committee Contact directly determines that this incident is:

○ A personal data breach. Relevant information shall be forwarded to the convener of the Personal Data Committee (including cases where non-natural personal customer data is stolen, disclosed, or altered).

○ A non-personal data breach, transferred to the Customer Complaint or Right-to-Exercise Acceptance Unit for handling, and closed the case for filing.

Explanation:

Recording Time:_____Year_____Month_____Day

☐ Convened the Personal Data Committee/Emergency Response Team meeting on Year_____Month_____ Day _____ according to the instructions of the convener (major cyber security incident).

☐ The business unit shall handle the emergency response measures on its own according to the instructions of the convener (designated date: _____Year_____Month_____Day _____)

＊ Numbering format: Year (YYY) + Date (MMDD) + 13-digit serial number (1~999), such as 109-08-26-01

<table>
<tr><td colspan="3">IV. Business Unit Handling Status (filled in by the Business Unit)</td></tr>
<tr><td>Briefly Describe the Process Process and Results</td><td colspan="2">I. Handling Status and Results

II. Scope of Impact

Processing completion time: _____Year_____Month_____Day</td></tr>
<tr><td colspan="2">Unit Personal Data File Security Maintenance Specialist</td><td>Unit Supervisor</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

<table>
<tr><td>V. Notes on Closing and Filing</td></tr>
<tr><td>The "Personal Data Breach Correction and Prevention Handling Form" has been issued. No.: □□□-□□-□□-□□□, and was approved by the Personal Data Committee on Year_____Month_____Day (see Attachment).
Case closing date: _____Year_____Month_____Day.</td></tr>
</table>

Attachment 2. Personal Data Breach Correction and Prevention Handling Form

<table>
<tr><td colspan="4">Correction and Prevention Handling Form Number (filled in by the Personal Data Committee Contact):</td></tr>
<tr><td colspan="4">Personal Data Breach Acceptance Number:</td></tr>
<tr><td colspan="2">Occurrence Date:</td><td colspan="2">Business Unit:</td></tr>
<tr><td>Problem Description</td><td colspan="3"></td></tr>
<tr><td>Cause Analysis</td><td colspan="3"></td></tr>
<tr><td rowspan="2">Evaluation of Corrective and Preventive Measures:</td><td colspan="3">Corrective Measures: (Control the escalation of the problem or eliminate the impact of a single event)

Expected Completion Date:</td></tr>
<tr><td colspan="3">Preventive Measures: (Eliminate the root cause of the problem and prevent similar breaches from happening)

Expected Completion Date:</td></tr>
<tr><td>Business Management Unit Supervisor Review/Opinion:</td><td colspan="3"></td></tr>
<tr><td colspan="4">Execution Confirmation</td></tr>
<tr><td>Execution Result</td><td>☐ Completed according to the above measures;
☐ evidence:

☐ Other Instructions:</td><td>Execution Officer</td><td>Date:</td></tr>
<tr><td>Performance Confirmation</td><td>☐ Confirmed that the measures meet the requirements; ☐ Evidence:

☐ Other Instructions:</td><td rowspan="2">Confirmation Officer</td><td rowspan="2">Date:</td></tr>
<tr><td>Improve Further</td><td>☐ No
☐ Yes, open another corrective and preventive handling form number:</td></tr>
<tr><td>Personal Data Committee Review/Opinion:</td><td colspan="3">☐ Approval for Closing: Completed review on Year ____Month ____ Date ____
☐ Other Instructions:</td></tr>
</table>

- Corrective and Preventive Handling Form Number Format: Year (YYY)＋Date (MMDD) ＋ three-digit serial number (1~999), e.g.,: 109-08-26-01.
- Personal Data Breach Acceptance Number: See "King's Town Bank Personal Data Breach Handling Notification and Record Form" for example.
- How to fill in the Corrective and Preventive Handling Form: Except for the corrective and preventive handling form number, the rest shall be filled in by the business unit. After the confirmation officer confirms that the measures meet the requirements, they shall be sent to the Personal Data Committee for review.

Attachment 3. Personal Data Breach Notification and Record Form:

<table>
<tr><td colspan="3">Personal Data Breach Notification and Record Form:</td></tr>
<tr><td>Name of Non-Government Agency:
_____

Reporting Agency
_____</td><td colspan="2">Reporting Time:
Year Month Day Hour Minute
Reporter: Signature (Seal)
Title:
Telephone:
Email：
Address:</td></tr>
<tr><td>Time of Breach</td><td colspan="2"></td></tr>
<tr><td>Type of Breach</td><td>☐ Stolen
☐ Disclosed
☐ Altered
☐ damage
☐ Destroyed
☐ Other Infringement Breaches</td><td>Total Number of Personal Data (approximately):
_____

☐ General personal data: _____ record(s)
☐ Special personal data : _____ record(s)</td></tr>
<tr><td>Cause of Occurrence and Event Summary</td><td colspan="2"></td></tr>
<tr><td>Damage Status</td><td colspan="2"></td></tr>
<tr><td>Possible Results of Personal Data Breach</td><td colspan="2"></td></tr>
<tr><td>Proposed Response Measures</td><td colspan="2"></td></tr>
<tr><td>Proposed Time and Method of Notification to the Data subjects Involved</td><td colspan="2"></td></tr>
<tr><td>Is FSC Notified Within 72 Hours After Discovering the Personal Data Breach</td><td colspan="2">☐ Yes ☐ No, reason</td></tr>
</table>

Note 1: If the information in each column is not yet clear, you can first fill in "unknown" and then report and update it after it is clear.

Note 2: The preceding 72-hour notification to the FSC includes holidays in the deadline calculation.

Figure 1. Personal Data Breach Emergency Response Flowchart