PremiumTrust Bank

Incident Response Procedure

Classification: Internal

April 2023

Document Number: PTB/ISMS/IRP/A5-24

Date	Document Version	Document Revision History	Document Author/Reviser
April 3, 2023	1.0	Document creation	Information & Cyber Security

Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

Table of Contents

1. Purpose

The aim of this policy is to ensure that PremiumTrust Bank (the “company”) manages appropriately any actual or suspected security incidents relating to information systems and data. This procedure is designed to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up consistently and correctly.
- To help identify and deal with areas for improvement to decrease the risk and impact of future incidents.

2. Scope

2.1. This document applies to all the company's employees, contractual third parties and agents who use its ICT facilities and equipment, or have access to, or custody of, its information.

2.2. All users must understand and adopt this procedure and are responsible for ensuring the safety and security of the company's systems and the information that they use or manipulate. This includes both data stored electronically and in any other form.

2.3. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

3. Definition

3.1. This procedure needs to be applied as soon as information systems or data are suspected to be or are actually affected by an adverse event which is likely to lead to a security incident.

3.2. The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organization's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

3.3. An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information,
- The transfer of data or information to those who are not entitled to receive that information,
- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system,
- Changes to information or data or system hardware, firmware, or software characteristics without the company's knowledge, instruction, or consent,
- Unwanted disruption or denial of service to a system, or
- The unauthorized use of a system for the processing or storage of data by any person.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix 2.

4. Incident Handling Procedure

Events and weaknesses need to be reported at the earliest possible stage, as they need to be assessed by Information and Cyber Security Group. The company shall enable Information & Cyber Security Group to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the company's Information & Cyber Security Group to gain as much information as possible from the business users to identify if an incident has taken place or is occurring.

4.1 Reporting Information Security Events or Weaknesses

The following sections detail how users and Staff must report information security events or weaknesses. *Appendix 1* provides a process flow diagram illustrating the process to be followed when reporting information security events or weaknesses.

4.1.1 Reporting Information Security Events for all Employees

4.1.1.1. Security events, for example a virus infection, could quickly spread and cause data loss across the organization. All users must understand and be able to identify that any unexpected or unusual behavior on the workstation could potentially be a software malfunction. If an event is detected users must:

- Note the symptoms and any error messages on screen. Disconnect the workstation from the network if an infection is suspected (with assistance from INN & S Staff).
- Not use any removable media (for example USB memory sticks) that may also have been infected.

4.1.1.2. All suspected security events must be reported immediately to the Information Security email: infosec@premiumtrustbank.com

4.1.1.3. If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to Senior Management to be assessed.

4.1.1.4. Information & Cyber Security Group will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and contact number of people reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

4.1.2 Reporting Information Security Weaknesses for all Employees

4.1.2.1. Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be misuse.

4.1.2.2. Weaknesses reported to application and service providers by employees must also be reported internally to Information & Cyber Security Group. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by Information & Cyber Security Group.

4.1.3 Reporting Information Security Events and Weaknesses for Support Staff

4.1.3.1. Information security events and weaknesses must be reported to INFORMATION & CYBER SECURITY GROUP who must immediately inform the Business and Customer Services Manager or his representative as quickly as possible and the incident response and escalation procedure must be followed. Security events can include:

- Uncontrolled system changes.
- Access violations – e.g. password sharing.
- Breaches of physical security.
- Non-compliance with policies.
- Systems being hacked or manipulated.

Security weaknesses can include:

- Inadequate firewall or antivirus protection.
- System malfunctions or overloads.
- Malfunctions of software applications.
- Human errors.

4.1.3.2. Should an appropriate response not be received by the person in Information & Cyber Security Group who owns the logged call within 30 minutes the incident / event must be escalated to the Information Security Champion.

4.1.3.3. Incidents must be reported to the Information Security Champion should the incident become service affecting.

4.1.3.4. An Incident report (see *Appendix 4*) must be completed by the incident owner for all incidents and passed to the Information Security Champion.

4.2 Management of Information Security Incidents and Improvements

- A consistent approach to dealing with all security events must be maintained across the company. The events must be analyzed, and Information & Cyber Security Group must be consulted to establish when security events become escalated to an incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the business on continuing operation during the incident.

- All high and medium incidents must be reported to Information & Cyber Security Group and logged. All low incidents must be logged. To decide what level of impact an incident has users should refer to the Risk Impact Matrix in *Appendix 3*.

4.2.1 Collection of Evidence

If an incident may require information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. The Information Security Champion must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation, for example concerning computer misuse, contact INFORMATION & CYBER SECURITY GROUP on email infosec@premiumtrustbank.com for advice.

4.2.2 Responsibilities and Procedures

4.2.2.1. Management responsibilities and appropriate procedures must be established to ensure an effective response against security events. Information & Cyber Security Group must decide when events are classified as an incident and determine the most appropriate response.

4.2.2.2. An incident management process must be created and include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident. o Corrective action to repair and prevent reoccurrence.
- Communication across the organization to those affected.

4.2.2.3. The process must also include a section referring to the collection of any evidence that might be required for analysis as forensic evidence. The specialist procedure for preserving evidence must be carefully followed.

4.2.2.4. The actions required to recover from the security incident must be under formal control. Only identified and authorized staff should have access to the affected systems during the incident and all the remedial actions should be documented in as much detail as possible.

4.2.2.5. The officer responsible for an incident / event should perform a risk assessment of the incident / event based on the Risk Impact Matrix (please refer to *Appendix 3*). If the impact is deemed to be high or medium this should be reported immediately to Information & Cyber Security Group and the Information Security Champion or their representatives.

4.2.3 Learning from Information Security Incidents

4.2.3.1. To learn from incidents and improve the response process, incidents must be recorded, and a Post Incident Review conducted. The following details must be retained:

- Types of incidents,
- Volumes of incidents and malfunctions, and o Costs incurred during the incidents.

4.2.3.2. The information must be collated and reviewed on a regular basis by Information & Cyber Security Group and any patterns or trends identified. Any changes to the process made as a result of the Post-Incident Review must be formally noted.

5. Responsibilities, Rights and Duties of Personnel

5.1. The Information Security Champion shall ensure enforcement and compliance to this policy through training, awareness, surveys and compliance audits.

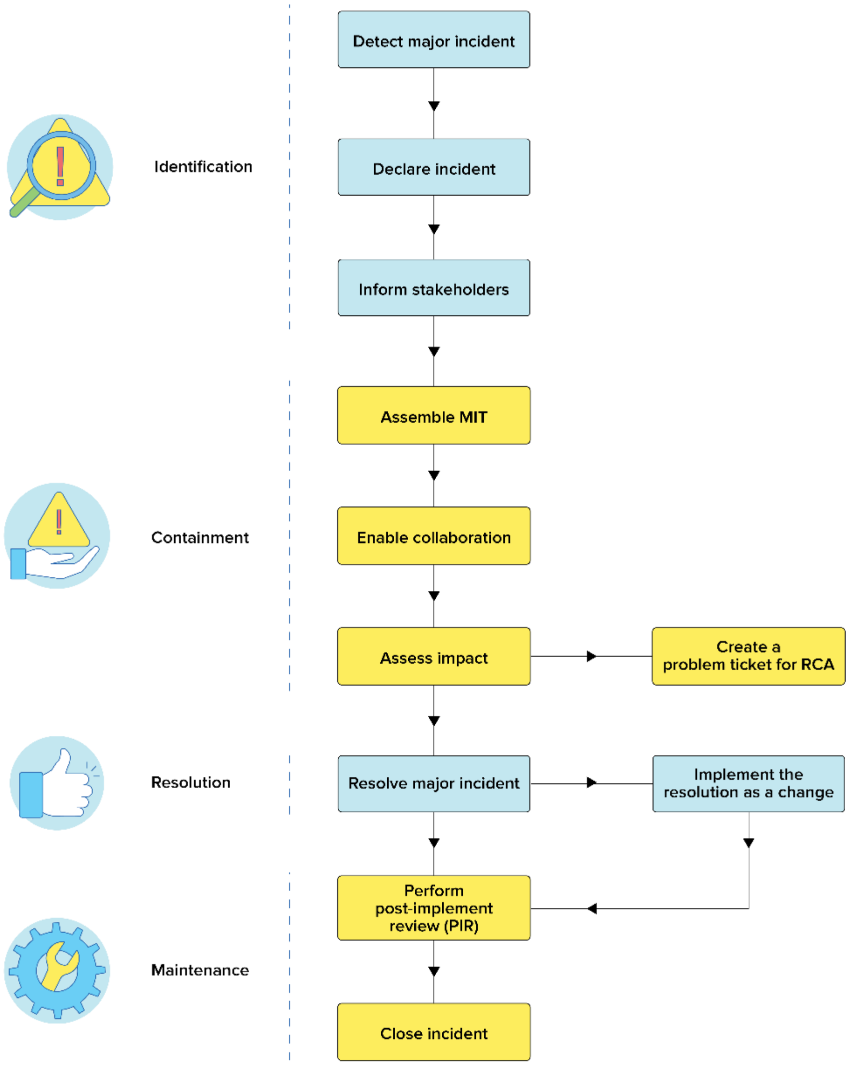
5.2. The Information Security Champion must approve all exceptions to this policy. Violations are subject to disciplinary action, up to and including termination of employment.

5.3. The Information Security Champion is the owner of this policy and shall ensure its revision at least once annually.

6. References

1) PREMIUMTRUST BANK Information Security Policy

Appendix 1 – Process Flow: Reporting an Information Security Event or Weakness



KEY:

MIT	-	Major Incident Team
RCA	-	Root Cause Analysis

Appendix 2 – Examples of Information Security Incidents and Events

Examples of the most common Information Security incidents and events are listed below. It should be noted that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a virus or other malware.
- Sending a sensitive e-mail to 'all staff' by mistake.
- Non reporting of the receipt of unsolicited mail of an offensive nature.
- Non reporting of the receipt of unsolicited mail that requires you to enter personal data.
- Changing data that has been done by an unauthorized person.
- Forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others. (Chain letters can be disturbing to those who receive them by implying bad luck if it is not forwarded for example. These are in fact just either at best a piece of fun which clogs up corporate and international email services wasting resource and at worse an attempt to harvest information from the recipient's machine including contacts information, details of corporate firewalls etc. They should be deleted straight away and not forwarded anywhere.)
- Unknown people asking for information that could gain them access to company data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on company equipment.
- Accessing a computer or database using someone else's authorization (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Theft / loss of a hard copy file.
- Theft / loss of any company computer equipment.
- Theft / loss of any company or third-party data through hacking.

Appendix 3 - Risk Impact Matrix

Impact Description and Value		Confidentiality Descriptions/Guidelines
Insignificant	**1**	No negative publicity in public media. non-sensitive information available for public disclosure. The impact of unauthorized disclosure of such information shall not harm organization anyway. e.g. Press releases, Company's Newsletters e.g. Information published on company's website
Minor	**2**	"Routine" snipping in the Press or posted on internet about PremiumTrust Bank system non-sensitive information available for internal disclosure. The impact of unauthorized disclosure of such information may cause negligible harm to the organization. e.g. Information published on company's portal
Moderate	**3**	May result in adverse publicity that gives an indication of poor service delivery culture and process inefficiency. Information belonging to the company and not for disclosure to public or external parties. The unauthorized disclosure of information here can cause a limited harm to the organization. e.g. organization charts, internal telephone directory
High	**4**	May result in negative publicity that gives and indication of weak management and inadequate internal control mechanism. Information which is very sensitive and intended to be used by named individuals only. The unauthorized disclosure of such information can cause harm (e.g. legal or financial liability). e.g. client's pricing information
Significant	**5**	May result in negative publicity that gives an indication of signs of distress or inefficiency. Information which is very sensitive or private, of highest value to the organization . The unauthorized disclosure of such information can cause severe harm (e.g. legal or financial liability, adverse competitive impact, loss of brand name). e.g. customer database, Merger and Acquisition related information, Marketing strategy

Appendix 4 - Incident Report

GENERAL INFORMATION			
Reported By:		**Date/Time Detected:**	
Department:		**Date/Time Reported:**	
Title:		**Mobile:**	
Phone:		**Additional Information:**	
Email Address:			
Postal Address:			
INCIDENT DETAILS			
Incident Type (Type of Data And Equipment Involved)			
Status of the Department (total failure, business as usual etc.)			
Classification of affected System:			

Incident Details (is anyone at risk?):	
Site Details:	
Site Point of Contact:	
Actions Taken:	