First Financial Holding Co., Ltd.
Enforcement Rules for Reporting Information Security Events

9 March 2020

20 March 2023

Contents

1. Purpose

These Enforcement Rules are established for subsidiaries to quickly resume business continuity and reduce impact on and the loss from operations, and minimize the possibility of recurrence when there is an information security event.

2. Scope

This shall include all abnormal events involving the damage of the confidentiality, integrity or usability all types of information assets, such as personnel, hardware, software, documents or information files, caused by the willful or unintended negligence of IT personnel or force majeure to affect business continuity.

3. Terms and definitions

Information security event

All kinds of operational anomalies harming this Company or customers in the IT operating process.

4. Levels of information security events and reporting criteria

4.1 Information security events fall into three levels based on their scope and severity of impact.

4.1.1 Level 1 information security events: Complying with any of the following situations

(1) Material contingencies that must be reported in accordance with the "Regulations Governing the Scope, Reporting Procedures and other Compliance Matters of Material Contingencies to be Reported by Financial Institutions" and the announcements of the competent authorities of the subsidiary.

(2) Information security events involving personal injuries or deaths.

(3) Information security events causing severe damage on the goodwill of this Company.

(4) The loss occurred from an information security event is over NT$1 million equivalent.

(5) The information system anomaly, hacker intrusion, or spread of computer viruses has expanded to affect over 50% of all normal business operations for over 30 minutes.

(6) Disruption or suspension of more than 50% of key system operations that cannot be restored to normal operations within a tolerable downtime.

(7) Severe leak or loss of sensitive information.

4.1.2 Level 2 information security events: Complying with any of the following situations

(1) The loss occurred from an information security event is over NT$100,000 equivalent.

(2) The information system anomaly, hacker intrusion, or spread of computer viruses has expanded to affect less than 50% of normal regional business operations for

over 30 minutes, but below the criteria of a level 1 information security event.

(3) Disruption or suspension of more than 50% of key system operations that is restored to normal operations within a tolerable downtime.

4.1.3 Level 3 information security events: Complying with any of the following situations

(1) Failures affecting individual users or single IT equipment.

(2) Hardware or software failures that do not affecting external operations.

(3) Other information security events below the criteria of a level 2 information security event.

4.2 Reporting deadline

(1) Events verified to be major sporadic cybersecurity incidents that result in damage to the rights of customers or impacts the institution's sound operations shall be simultaneously reported via telephone to the Financial Supervisory Commission's competent agency and this Company within 30 minutes of confirmation and approval.

(2) Non major sporadic cybersecurity incidents that have been determined to be a level 1 cybersecurity incident shall be reported within 1-day of occurrence.

(3) Confirmed level 3 information security events will not need to be reported.

4.3 Responsible reporting departments of subsidiaries

(1) The reporting department designated by a subsidiary shall be the responsible reporting department of information security events.

(2) Where a subsidiary does not designate a responsible reporting department, the information security department (or the information department if an information security department is not established) shall be the department responsible for reporting information security events.

4.4 Report accepting department

(1) The Information Technology Department of this Company shall be the responsible report accepting department of information security events of subsidiaries.

(2) After receiving a report of information security events, the report accepting department shall register the report and maintain a record.

4.5 Reporting method

(1) Complete the “Information Security Event Emergency Report (SW-027-F01)”.

(2) During the opening times, notify the responsible report accepting department of this Company by fax or by email.

(3) After the opening times, notify first the responsible report accepting department of this Company by email and contact the responsible report accepting personnel by phone,

then submit the fax on the next business day.

4.6 Subsequent management

(1) After receiving a report, the responsible report accepting department shall report to relevant supervisors according to the level of an information security event.

1) Major sporadic cybersecurity incident: Elevate report through each level until the Chairman.

2) Level 1: Elevate report through each level until the General Manager and initiate cybersecurity emergency response mechanisms under directions from the Chief Security Officer.

3) Level 2 and Level 3: Notify the department supervisor responsible for receiving reports.

(2) The responsible unit of a subsidiary shall handle the situation with reference to its internal procedures and complete handling the information security event by the deadlines specified for respective event levels.

(3) The responsible event handling department of a subsidiary shall notify the responsible report accepting department again after settling an information security event for the responsible report accepting department to close the case.

4.7 Management and Tracking of Completed Cases

(1) After the level 1 and 2 cybersecurity incidents of this Company and its subsidiaries have been concluded, documentation of implemented improvements should be re-submitted to the department responsible for receiving reports.

(2) The department responsible for receiving reports shall track the various improvement measures in the "Cybersecurity Incident Emergency Report Form" in order to conclude the case.

5. Output documents/records

(1) Information Security Event Emergency Report (SW-027-F01)

6. Addendum

This Enforcement Rules and their amendments shall be implemented after obtaining the approval of the IT department chief.