Mega Financial Holding Co., Ltd.
Guidelines for Responses, Reporting, and Prevention of
Personal Data Security Incidents

Approved by the President on March 25, 2014
First amendment made on March 26, 2018
The Board of Directors authorized correcting the name of the unit on October 27, 2020; the amendments took effect on January 1, 2021
Second amendment made on May 27, 2022
Third amendment made on July 27, 2023

Article 1 (Purpose and Basis)

To conform to the “Regulations Governing Security and Maintenance of Personal Data Files of Non-government Agency Designated by the Financial Supervisory Commission,” and the "Mega Financial Holding Co., Ltd. Personal Data File Security Maintenance Guidelines", Mega Financial Holding Co., Ltd. (hereafter referred to as “Mega”) has formulated these Guidelines to establish mechanisms for responding to, reporting, and preventing personal data security incidents.

Article 1-1 (Responsible Unit)

The Compliance Department is the responsible unit of the Guidelines.

Article 2 (Definition of the terms)

The terms used in the Guidelines are defined as follows:

I. Personal data security incidents (hereinafter referred to as “personal data incidents”): Refer to any theft, tampering, damage, loss or leak of personal data .

II. Major personal data incident: Refers to personal data incidents mentioned in the previous Paragraph which will jeopardize the normal operations of Mega or rights of a large number of parties.

Article 3 (Response Measures)

In the event of personal data incidents, the incidents shall be reported, and the following response measures shall be immediately adopted pursuant to Article 3-1:

I. Investigate the reasons of occurrence

The unit where the incident occurred shall investigate and record the extent of personal data affected by the incidents. Furthermore, the unit shall clarify the reasons behind the theft, tampering, damage, loss, or personal data leak. If necessary, the incident site shall be controlled, non-authorized personnel shall be prohibited from accessing the documents, and relevant evidence shall be

preserved.

II. Control the damages

The relevant business units shall examine and assess the extent of damage caused by the incident. They shall immediately implement appropriate remedies and improvements to prevent the damage from spreading further.

III. Formulate Response Measures

Based on the assessment results of the personal data incident, the unit where the incident occurred shall formulate the response measures. After signed off by the Compliance Department, Information Security Department, and Risk Management Department, the measures will be submitted to the President for approval.

If personal data incidents occur due to improper management by Mega, causing harm to parties, negotiation shall be held and compensations shall be provided to the affected parties whose personal data has been violated.

Article 3-1 (Notification Mechanisms)

In the event of a personal data incident, the unit where the incident occurred shall immediately report it to the unit in charge. The unit in charge will then report to the spokesperson and notify the Auditing Office under the Board of Directors, the Risk Management Department, the Administration Department, the Compliance Department, the Information Security Department, and other relevant units simultaneously.

In the event of a major personal data incident, the unit in charge shall report the leak of personal data to the Financial Supervisory Commission within 72 hours (holidays are included in the calculation of the duration) in accordance with the format specified in the attachment of Article 6 of the "Regulations Governing Security and Maintenance of Personal Data Files of Non-government Agency Designated by the Financial Supervisory Commission." However, if other requirements are specified in other laws and regulations, such requirements shall apply. Activate the “Major Contingencies Crisis Management Team” to conduct grouping and assign tasks when necessary.

The unit in charge is the Compliance Department in the preceding two paragraphs. However, for information security personal data incidents, the unit in charge is the Information Security Department.

The Information Security Department is responsible for handling personal data incidents of information security in accordance with the relevant regulations, such as Mega’s “Information Security Policy” and “Guidelines for Information Security Management.” It may collaborate with the Electronic Data Processing Department to

handle the incident if necessary.

Article 4 (Notify affected parties)

In the event of a personal data incident, the unit where the incident occurred shall promptly notify the affected parties in a manner that is sufficient for them to become aware or informed of the incident. This can be done through verbal communication, written form, telephone, text messages, emails, faxes, electronic documents, or any other means after investigation. Designated personnel shall be assigned to respond to any questions from the affected parties. However, if the aforementioned notification methods prove to be excessively costly, feasibility of using technology and protection of the party's privacy shall be contemplated. In such cases, disclosure through the Internet, news media, or other appropriate public channels shall be carried out.

When notifying the affected parties in accordance with the aforementioned regulations, the content shall include the following:

I. The fact that personal data is violated, reasons for the occurrence and responsive measures adopted.
II. Mega's contact information.

Article 5 (Disclosure method for personal data incidents)

When personal data incidents occur and media interviews are involved, the media shall be directed to contact the spokesperson of Mega. Employees shall refrain from expressing personal opinions.

When information on personal data incidents is disclosed to the public through the Internet, news media, or other appropriate channels, the whole incident and the responsive measures adopted shall be explained to the general public.

In the event of misinformation, press release shall be issued in a timely manner to prevent damage to Mega's reputation. If necessary, public notices shall be published in the media. However, the content of such public statements shall not include personal data.

Article 6 (Corrective and preventive measures)

After the personal data incident is resolved, reviews, and assessments shall be conducted to find out the reasons for the occurrence, extent of impact, damage costs, and handling processes. Corrective and preventive measures shall be formulated to reduce similar incidents from reoccurring.

The corrective and preventive measures mentioned in the preceding paragraph shall include inspecting operating procedures, strengthening control mechanisms, and providing education and training to relevant units. For major personal data incidents, any corrective or preventive measures developed by Mega shall be analyzed in their

entirety and reviewed by experts who are impartial and independent and whose qualifications have been publicly certified.

For personnel negligence which leads to failure of complying with the Personal Data Protection Act and relevant regulations, and results in major personal data incidents or substantial losses, according to the internal company code, we will report to the management team for penalty. Depending on the severity of the case, the unlawful employee may possibly face warnings, reprimands, demerits and other punishment,and corresponding legal action may be taken when necessary.

Article 7 (Document Retention Period)

The unit where the incident occurred shall properly retain records, paper trail, and evidence of data related to the personal data incident. These documents shall be retained for at least five (5) years.

Article 8 (Other Matters)

Matters not specified in the Guidelines shall be governed by applicable laws and regulations and relevant regulations of Mega.

Article 9 (Level of Approval Authority)

The Guidelines shall become effective following the approval of the President. The same procedures shall apply to all future amendments or rescission.

Format in the attachment for Article 6 of the Regulations Governing Security and Maintenance of Personal Data Files of Non-government Agency Designated by the Financial Supervisory Commission

<table>
<tr><td colspan="3">Personal Data Infringement Incident Report and Record Table</td></tr>
<tr><td>Name of the non-government agency:
_____
Reporting agency/unit:
_____</td><td colspan="2">Report time: (year) (month) (date) (hour) (minute)
Reported by: Signature (seal)
Title:
Tel:
Email:
Address:</td></tr>
<tr><td>Incident occurrence time</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Incident type</td><td rowspan="2">□ Theft
□ Leak
□ Tampering
□ Damage
□ Loss
□ Other infringements</td><td>Total number of personal data infringements (estimated)
_____</td></tr>
<tr><td>□ General personal data: ___ entries
□ Special category personal data: ___ entries</td></tr>
<tr><td>Reason(s) for the occurrence of the incident and summary</td><td colspan="2"></td></tr>
<tr><td>Status of damage</td><td colspan="2"></td></tr>
<tr><td>Possible outcomes due to leak of personal data</td><td colspan="2"></td></tr>
<tr><td>Proposed response measures</td><td colspan="2"></td></tr>
<tr><td>Proposed time and method for notifying the party</td><td colspan="2"></td></tr>
</table>

Whether the leak of personal data is reported to the Financial Supervisory Commission within 72 hours after discovery	□ Yes □ No, reasons

Note 1: If the information for a field is not yet known, it may be specified as "unknown" and the information shall be reported and updated when it is known.

Note 2: Holidays are included in the calculation of the duration for the aforementioned reports to the Financial Supervisory Commission within 72 hours.