CHLITINA HOLDING LIMITED

Regulations Governing the Protection of Personal Data

I. General Provisions

1. These regulations apply to the Company and its subsidiaries.
2. The collection, processing, and use of personal data shall comply with relevant laws and regulations, including providing the data subject with the following rights:
   2.1 The right to inquire about or request access to their personal data.
   2.2 The right to request copies.
   2.3 The right to request supplementation or correction.
   2.4 The right to request the cessation of collection, processing, or use.
   2.5 The right to request deletion.
3. The collection, processing, or use of personal data shall be conducted in good faith and in a trustworthy manner, and shall not exceed the scope necessary for the specific purpose.

II. Protection of Written Documents

1. When collecting written documents containing personal data, appropriate protective measures shall be taken, including indicating the purpose or scope of use on the written documents.
2. When processing or using written documents containing personal data, such documents shall be properly kept and shall not be left unattended.
3. When written documents containing personal data must be provided to external entities due to business needs, they shall be retrieved after the outsourced matters are completed.
4. Written documents containing personal data that are subject to destruction shall be destroyed on a regular basis.

III. Protection of electronically stored files

1. When personal data are stored electronically, the storage device shall be equipped with user IDs and login passwords, and there shall be an automatic logout function after the application is closed.
2. User IDs and login passwords shall not be shared with others, and login passwords shall be changed at least once every three months. Passwords shall be at least eight characters in length and include both letters and numbers.
3. When electronic files containing personal data must be provided to external entities due to business needs, reliable transmission methods with confidentiality mechanisms shall be used, such as compressing and encrypting the data files, and transmission activities shall be recorded.
4. When processing or using personal data with electronic equipment, the input, output, editing, or correction of personal data shall be verified against the originals. If any doubt arises as to data consistency, the originals shall be reviewed for verification.
5. Electronic equipment storing personal data shall be protected from external networks by a firewall and shall have antivirus software installed. In addition to regularly updating

virus definitions, scheduled scans shall also be performed regularly.

6. A designated person shall regularly review and update the operating systems of electronic equipment storing personal data and apply patches to remedy any vulnerabilities.
7. Electronic equipment storing personal data shall be placed in secure areas, such as offices with access control or locked drawers. Such equipment shall not be taken out without the approval of the competent authority.
8. Backup mechanisms shall be established for electronic equipment storing personal data to prevent data damage, loss, or theft.
9. When electronic equipment storing personal data is to be scrapped or reassigned for other use, personal data stored on the equipment shall be completely deleted.
10. When external parties update or repair electronic equipment storing personal data, a designated person shall be present to ensure the security of personal data and prevent any leakage of such data.

IV. Personal Management

1. The Company shall provide information security education and training (internal or external) to personnel who collect, process, or use personal data, and shall regularly promote the importance of personal data protection and the policy that computers must be shut down at the end of each workday.
2. When personnel responsible for collecting, processing, or using personal data are reassigned or their duties change, they shall hand over an inventory of the written documents under their custody. For electronic equipment, the successor shall reset login passwords in relevant systems and, where necessary, change the user ID.
3. Personnel engaged in the collection, processing, or use of personal data shall sign a confidentiality agreement. Upon resignation or termination of contract, their user IDs and login passwords shall be cancelled or deactivated, and their access cards and related identification documents shall be recovered. ◦
4. It is prohibited to collect, process, or use personal data through instant messaging software, peer-to-peer transmission software, cloud drives, or other insecure Internet media.
5. It is prohibited to disclose personal data obtained in the course of business on social networking sites, blogs, public forums, or other Internet-based public platforms.

V. System Development and Outsourcing Management

1. Information systems that process personal data, whether developed in-house or outsourced, shall take into account the security requirements of personal data (such as logic testing) at the initial stage of the system development life. System maintenance, updates, launches, and version changes shall be subject to security controls to prevent harm to personal data security.
2. Maintenance personnel or system service providers should be avoided from using

remote login methods to perform maintenance or operations involving personal data. If remote login is necessary, it shall be approved by the competent authority and conducted through an encrypted channel (such as VPN).

3. For information systems developed in-house or outsourced that process personal data, appropriate protection and control shall be applied to personal data, including personal data used for testing.
4. Where personal data printing is outsourced, the outsourcing contract shall specify confidentiality obligations, responsibilities related to information security, and penalties for violations, and on-site audits shall be carried out when necessary.

VI. Control Points

1. Protection of Written Documents
   - 1.1 Are written documents containing personal data properly safeguarded, without being left unattended or placed arbitrarily?
   - 1.2 When personal data are provided to external entities, are appropriate records kept at the time of delivery and retrieval?
   - 1.3 For written documents containing personal data that are eligible for destruction, is document destruction carried out on a regular basis?

2. Protection of Electronically Stored Files
   - 2.1 Do electronic devices used to collect or process personal data have user IDs and login passwords set up?
   - 2.2 Are there any instances of sharing user IDs and login passwords with others?
   - 2.3 Are login passwords changed at least once every three months, and are they at least eight characters long including both letters and numbers?
   - 2.4 When electronic files containing personal data are provided to external entities, are the data files compressed and encrypted before transmission?
   - 2.5 When electronic devices storing personal data are to be scrapped or reassigned for other uses, is the personal data stored on such devices completely deleted?

3. Personal Management
   - 3.1 Is information security education and training being implemented?
   - 3.2 Are computers shut down at the end of each workday?
   - 3.3 After relevant personnel resign, do successors reset login passwords in relevant systems and, where necessary, change user IDs?
   - 3.4 Is any unsafe Internet medium being used to collect, process, or use personal data?

4. System Development and Outsourcing Management
   - 4.1. For information systems developed in-house or outsourced that process personal data, is appropriate protection and control applied to personal data (including

personal data used for testing)?

4.2. When the printing of personal data is outsourced, are confidentiality obligations, responsibilities related to information security, and penalties for violations specified in the outsourcing contract?

VII. Reference Documents

1. Personal Data Protection Act

VIII. Implementation and Revision

These regulations shall be implemented upon approval by the Board of Directors, and the same shall apply to any amendments.

IX. Version Record

Version	Description	Date
1	New Document	2014.12.19