Third Party
Information Security Acknowledgement

This Information Security Acknowledgement (hereinafter referred to as "this Acknowledgement") applies to any individual or entity involved in the operation of the Delta Group, who shall comply with the following provisions:

1. Management of Information Security Operations

   1.1. Shall: (1) adhere to Party A's Information Security Management System, including but not limited to Delta information security policies, relevant regulations of the information security management system, (2) any applicable national laws (such as the Trade Secrets Act, Personal Data Protection Act, Enforcement Rules of the Personal Data Protection Act, Criminal Code, Civil Code, Copyright Act, or Intellectual Property Rights Act), and (3) compliance with information security standards of the industry.

   1.2. Shall not privately collect, disclose, copy, transfer, reuse, or deliver any information to any third party, except as expressly permitted under this Acknowledgement.

   1.3. Shall provide operation manuals, documents, technical support, and educational training related to the architecture, operation, management, and maintenance of equipment, hosts, or system software.

   1.4. Any deliverables, including but not limited to equipment or software delivered to the Delta Group, shall be free from backdoors, covert channels, Trojan horses, malicious code, or viruses.

   1.5. Systems that are developed or maintained in connection with the operation of the Delta Group shall be free from information security vulnerabilities. If any information security vulnerability is identified, such vulnerability shall be remediated at no additional cost. The remediation approach and delivery schedule shall be subject to the approval of the Delta Group.

   1.6. The use of security detection tools, including but not limited to scanning tools, shall require prior approval from the Delta Group.

   1.7. When personnel involved in system development or equipment maintenance for the operation of the Delta Group are transferred or leave their roles, the relevant operational permissions shall be revoked immediately.The Delta Group shall be

notified at least three days prior to such personnel's departure, and any borrowed hardware or software shall be promptly returned.

1.8. Any individual or entity involved in the operation of the Delta Group shall cooperate with the Delta Group in conducting business continuity plan drills.

1.9. If any individual or entity involved in the operation of the Delta Group needs to bring mobile computing devices or storage media, such as disks, CDs, USB flash drives, or external hard drives, into the Delta Group's controlled areas (e.g., computer rooms, laboratories, or production lines), prior consent must be obtained from authorized personnel of the Delta Group, and all relevant regulations of the Delta Group shall be complied with.

1.10. Within the Delta Group's controlled areas, any individual or entity involved in its operations shall not bring mobile devices, cameras, or any equipment with photographic or recording functions. If there is a business need to take photos or videos, prior written approval from the Delta Group must be obtained.

1.11. For the entry and exit of information equipment in Delta Group's controlled areas, any individual or entity involved in its operations shall comply with the Delta Group's relevant regulations and state the reason or purpose for moving the equipment.

1.12. Any individual or entity involved in the operation of the Delta Group shall provide relevant information regarding services or business activities when requested by the Delta Group or a third party, in accordance with applicable regulations and policies.

1.13. Delta Group reserves the right to conduct audits to verify adherence to said cyber security requirements and reserves the right to ask for supporting documentation.

1.14. Any individual or entity involved in the operation of the Delta Group shall obtain prior approval from Delta Group before engaging any subcontractors or third-party service providers for information and communication technology-related activities. They remain responsible for supervising, reviewing, and auditing such subcontractors or third parties, and all information security requirements applicable to them shall also apply to their subcontractors or third-party service providers.

1.15. Any individual or entity involved in the operation of the Delta Group shall notify Delta Group within 72 hours upon becoming aware of any information security incident, violation of applicable personal data protection laws, or breach of contractual obligations. The notification shall, at a minimum, include a description

of the incident, its scope and impact, and the remedial measures undertaken.

2. Liability for Breach of Acknowledgement

Any individual or entity involved in the operation of the Delta Group shall be fully responsible for any damages resulting from a violation of this Acknowledgement. This includes, but is not limited to, additional costs incurred by Delta Group, claims from Delta Group's clients, and any expenses or compensation related to legal proceedings.