Document Title	**Information Security Policy**			No.	**T-AT-1-001-A**
Formulated by	Information Mgmt. Section of Admin. Service Dept.	Amendment Date	Jun. 30, 2017	Page	1/2

1. **Purpose:** RICH HONOUR INTERNATIONAL DESIGNS CO., LTD. (hereinafter referred to as the Company), with the aim to enhance information security management, ensure the confidentiality, integrity and availability of its information assets to provide an information environment for the continuous operation of the Company's information business, and comply with relevant requirements of regulations to protect itself from internal and external intentional or accidental threats, hereby formulates this Policy.

2. **Scope:** The Company establishes an information security management system in accordance with actual needs and in compliance with relevant legal requirements to ensure the confidentiality, integrity and availability of information. The scope of application of this system is set to the maintenance of the operation of the server room, the security management of ERP system maintenance, and related departments and maintenance management personnel, so as to fully grasp the status of information operation and management process and meet various security requirements and expectations.

   The Company has fully grasped the information operation and management process and met various security requirements and expectations.

   The information security management covers 14 management items to avoid abuse, leakage, tampering, and destruction of information due to factors such as human error, intentional or natural disasters which would generate various potential risks and hazards to the Company. The details of management matters are as follows:

   2.1. Information security policy.

   2.2. Information security organization.

   2.3. Human resource security.

   2.4. Assets management.

   2.5. Access control security.

   2.6. Encryption.

   2.7. Physical and environmental security.

   2.8. Operational security.

   2.9. Communication security.

   2.10. Information system acquisition, development and maintenance.

   2.11. Suppliers relationships.

   2.12. Information security incident handling.

   2.13. Operational and continuous management of information security.

   2.14. Legality.

   The Company's internal personnel, contractors and visitors shall abide by this Policy.

3. **Definitions:**

   3.1. Information assets: The hardware, software, services, documents and personnel to maintain the normal operation of the Company's information operation.

3.2. Information environment for continuous business operation: The computer operating environment required to maintain the normal operation of the Company's various business operation.

4. Purpose: Maintain the confidentiality, integrity, and availability of the Company's information assets and protect users' data privacy. With joint efforts of all staff, we intend to achieve the following goals:

4.1. Protect information about the Company's business activities from unauthorized access.

4.2. Protect the information about the Company's business activities from unauthorized modification and ensure correctness and integrity.

4.3. Establish a cross-departmental information security organization to formulate, promote, implement and evaluate the improvement of information security management for ensuring that the Company has an adequate information environment for business continuity.

4.4. Conduct information security education and training to promote employees' awareness of information security and related responsibilities.

4.5. Implement an information security risk assessment mechanism to improve the effectiveness and timeliness of information security management.

4.6. Implement an internal audit system for information security to ensure the proper implementation of information security management.

The performance of any of the Company's business activities shall fully comply with the requirements of relevant laws or regulations.

5. Responsibilities:

5.1. The Company's management formulates and reviews this Policy.

5.2. Information security administrators implement this Policy through appropriate standards and procedures.

5.3. All personnel and service contractors shall follow relevant security management procedures to maintain the information security policy.

5.4. All personnel are responsible for reporting information security incidents and any identified loopholes.

5.5. Any actions that endanger information security will be investigated for civil, criminal and administrative responsibilities or punished in accordance with the relevant regulations of the Company, depending on the severity of the circumstances concerned.