Information Security Policy

SECTION 1 - Purpose

This policy aims at ensuring the confidentiality, integrity, availability, and legitimacy of the information assets that belong to Qisda Corporation (hereinafter referred to as Qisda), including hardware, software, data, documents and employees related to information data process, and protecting from internal and external threats of deliberate or accidental, according to business needs.

SECTION 2 - Scope

It applies to all Qisda employees, temporary staff, visitors and vendors (including their employees, temporary staff, etc.) while maintaining, keeping, accessing, managing Qisda's information assets.

SECTION 3 - Policy

A. Objectives

Qisda employees should maintain the confidentiality, integrity, availability, and legitimacy of Qisda's information assets and protect user data privacy to achieve the following targets:

i. Protection of Qisda's business activities information from unauthorized access to ensure confidentiality.

ii. Protection of Qisda's business activities information from unauthorized modifications or human error to ensure integrity.

iii. Ensure the continuity and availability of relevant business information and thus correctly carrying out the operation and service.

iv. Ensure the implementation is compliant with relevant laws.

B. Measures

The measures are defined as follows:

i. Establish an information security organization to supervise the operation of the information security management system, and identify internal and external issues within the information security management system, which meets the requirement from stakeholders.

ii. The executives commit to ensure the security of information assets and the continuity of information services, thus mitigating the threat from and impact of information security incidents in order to ensure the effectiveness of systems and protecting the best interests of our customers and stakeholders.

iii. Information security management system documents should be reviewed and updated regularly. Records are protected with defined mechanism.

iv. Regularly conduct information asset management, information account inventory and risk assessment.

v. All employees of Qisda, including salespersons, have the responsibility and obligation to protect the information assets they own, keep and use.

vi. Work assignment should consider function divisions and job responsibilities to prevent unauthorized modification or usage against information or system functions.

vii. The employees or temporary staffs of the vendors, who having business with Qisda, should follow Qisda 's relevant regulations and be audited when they need to use or access Qisda's information assets. These personnel are also responsible for protecting Qisda's information assets which they possess, keep in custody or use of.

viii. Keep implementing information security scenario drills and routinely execute drills to examine the effectiveness of business continuity drills

ix. Information security indicators should be defined and examined regularly to maintain the effectiveness of the implementation and control of the information security management.

x. Enforce a cybersecurity workplace to reduce the risks of theft, inappropriate use, alteration, or damage of information assets.

xi. The development, modification and construction of information operations or programs must meet and follow the requirements of information security objectives.

xii. Based on the information security incident management regulations, to ensure staff can respond promptly in accordance with the procedures.

xiii. Form the procedures or regulations with compliance and conduct audit work or information security surveys regularly.

xiv. The use of mobile devices should be related to business, and would be authorized after application in accordance with the procedures. The mobile device security measures should be adopted to manage the risks caused by the use of mobile devices.

xv. Information security issues should be included in information operation project management.

C. Annual Review

This policy and operation should be reexamined annually to check for legal compliance with the latest technology and business developments.

SECTION 4 - Enforcement

i. Violators of Information Security Policy will be asked for improvement. While the improvement can not be reached, the supervisor should work with the Human Resources Department and other relevant units about the penalties and legal liabilities accordingly.

ii. Violations of Information Security Policy by vendors that have a business with Qisda shall be dealt with in accordance with the contract or agreement between the two parties.