HengTian

Hengtian Information Security White Paper

March, 2012

HengTian

Contents

Overview

Hengtian has established the Information Security Management System, which is based on the requirements from the interested parties and ISO 27001 controls. Hengtian operates the information security system with PDCA model. (Figure 1 – PDCA model)

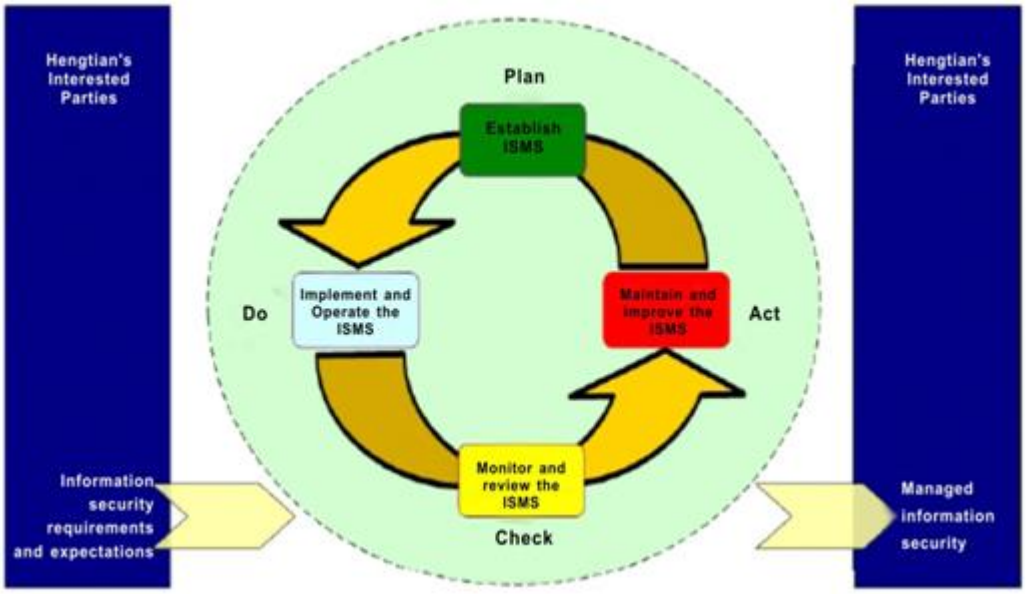

Figure 1 – PDCA model

The input of Hengtian information security system includes:

- State Street information security requirements
- Other global clients' information security requirements
- Information security related laws and regulations
- ISO27001 standards

Hengtian pays special attention to clients' opinions and requirements on information security by all aspects. As one of the most important clients of Hengtian, State Street's information security system has been adopted as a reference by Hengtian. Hengtian's information security system complies with State Street's through:

- Hengtian has about 500 employees working in State Street Hangzhou's office, who have strong awareness with the trainings from State Street corporate information security team
- Hengtian establishes the information security system with the guide and consultancy from State Street security team
- Hengtian receives the sessions from State Street Chief Information Security Officer on a regular basis
- Hengtian's information security team keeps close touch with State Street Hangzhou's security team

- State Street is establishing the ISO27001 information security system

The following figure is the framework of Hengtian's information security system.

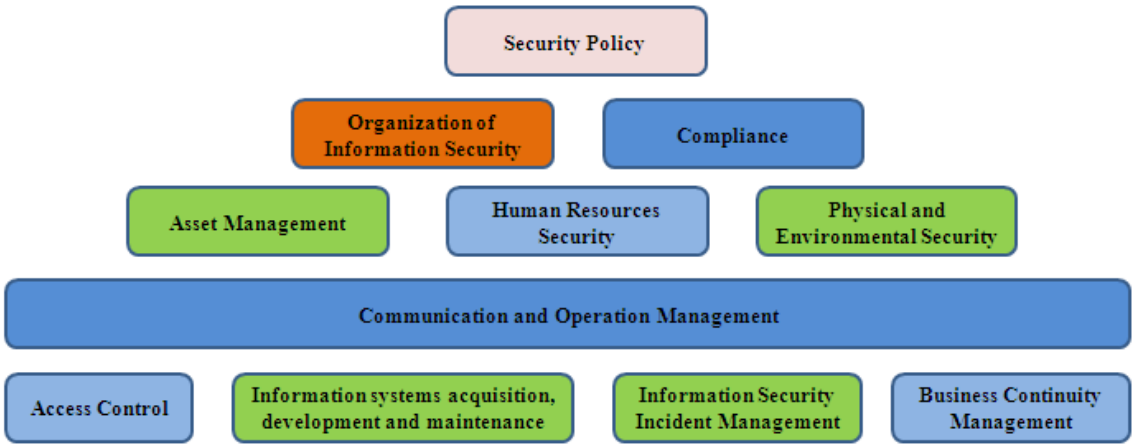

Figure 2 – Hengtian Corporate Information Security Framework

1. Security Policy

1) Objectives

To provide management direction and support for Hengtian information security in accordance with business requirements and relevant laws and regulations.

2) Practice examples

Hengtian has developed a set of corporate information security standards and policies, which covers the control areas of asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, business continuity management and compliance.

2. Organization of information security

1) Objectives

Internal organization
To manage information security within Hengtian.

External parties
To maintain the security of Hengtian information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

2) Practice examples

Hengtian has established an information security organization. The following figure shows the organization structure.

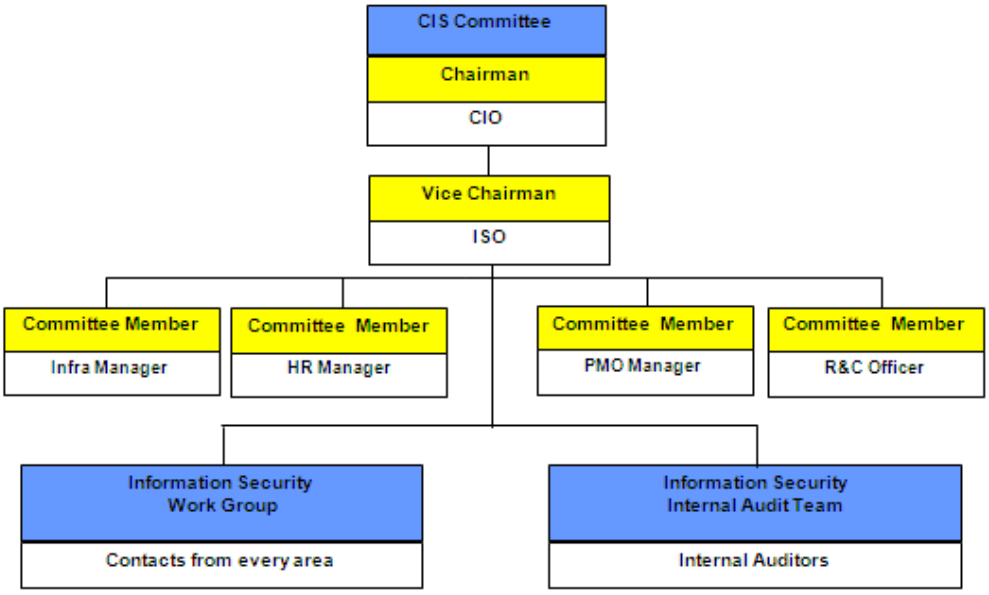

Figure 3 – Hengtian Information Security Organization Chart

- Corporate Information Security (CIS) Committee: The committee is the executive team of Hengtian information security, which is led by Hengtian Chief Information Officer and gets the related managers involved.
- Information Security Officer: It is a dedicated management role of Hengtian Corporate Information Security, which is assigned by Hengtian executive team and reports to Hengtian CIO.
- Information Security Work Group: The work group is responsible for the information security operation and execution, whose members come from the staff of Information Security Office and contacts of related departments or project teams.
- Information Security Internal Audit team: The audit team is responsible for the self-assessment on Hengtian information security system, which conducts the internal audits on a regular basis. Currently, the internal audits are conducted quarterly.

3. Asset management

1) Objectives

Responsibility for assets: To achieve and maintain appropriate protection of Hengtian and clients' assets.

Information classification: To ensure that information receives an appropriate level of protection.

2) Current policies & standards

a) HT-CIS-101 Information Classification
b) HT-CIS-102 Acceptable Use of Information Technology Resources
c) HT-CIS-103 Spreadsheets, Macros & Small Applications
d) HT-CIS-104 Use of Corporate Assets

3) Practice examples

a) Hengtian classifies corporate information as following: Highly Confidential, Confidential, Limited Access, Company Internal or General. All corporate information must be classified into one of the five classifications above. (Figure 4 - A sample of information classification)

b) The Information classified as highly Confidential, Confidential, Limited Access or Company Internal cannot be released to the outside of the work sites without appropriate approvals.

Level	Definition	Examples
General	Information that has been determined by Hengtian and its customers to be available for public distribution or is already available in the public domain. General information is not sensitive in context or content.	1. Recruitment Information 2. www.hengtiansoft.com
Company Internal	Non-public information that bears no material risk if disclosed to employees or authorized third parties.	1. Company policies and standards
Limited Access	Information that can be accessed only by those who "need-to- know".	1. Management Reports 2. General email
Confidential	It is proprietary in nature and/or highly sensitive so that disclosure may cause legal or financial ramifications	1. Employee Personal Info 2. Customer data
Highly Confidential	Corporate information which, if disclosed to unauthorized persons (internal or external), could cause material harm to the corporation	Any information that could result in the loss of competitive advantage or reputation

Figure 4 - A sample of information classification

4. Human Resources Security

1) Objectives

Prior to employment

To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

During employment

To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support Hengtian's security policy in the course of their normal work, and to reduce the risk of human error.

Termination or change of employment

To ensure that employees, contractors and third party users exit Hengtian or change employment in an orderly manner.

2) Current policies & standards

a) HT-CIS-201 Human Resource Security

3) Practice examples

a) All candidates will be conducted background investigations by a professional background investigation company (called ***TOP CREDIT***) prior to receiving Hengtian's identification card and/or system access.
b) All employees are required to sign a Non Disclosure Agreement (NDA) prior to beginning employment.
c) All new hired employees receive corporate information security orientation training and test.
d) Department/projects teams receive special/ customized information security related trainings according to the clients'/project's requirements.
e) Employee's access rights will be revoked upon termination of employment. Employee's access rights will be updated upon job transference.

5. Physical and environmental security

1) Objectives

Secure areas

To prevent unauthorized physical access, damage and interference to Hengtian's premises and information.

Equipment security

To prevent loss, damage, theft or compromise of assets and interruption to Hengtian's activities.

2) Current policies & standards

a) HT-CIS-301 Physical Security

3) Practice examples

a) All important/main entrances and exits of Hengtian's work areas are secured by access control systems. (Figure 5 – Example of Hengtian's access control system)

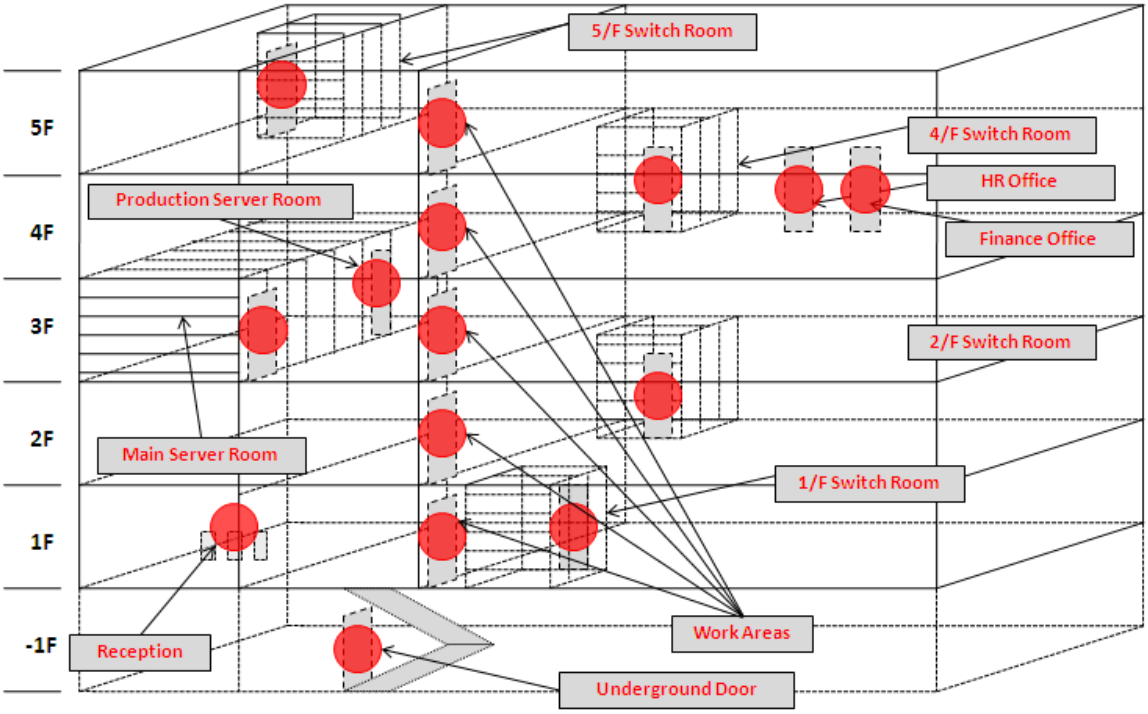

Figure 5 - Example of *Hengtian's access control system*

b) All important/main entrances and exits of Hengtian's work areas are monitored by security guards with a Closed Circuit Television monitoring system, 24×7.

c) All the departments and project teams are located in secured areas. (Figure 6 – A sample of 3-level physical access right control)

Figure 6 – A sample of 3-level physical access right control

6. Communications and operations management

1) Objectives

Operational procedures and responsibilities
To ensure the correct and secure operation of information processing facilities.

System planning and acceptance
To minimize the risk of systems failures.

Protection against malicious and mobile code
To protect the integrity of software and information.

Back-up
To maintain the integrity and availability of information and information processing facilities.

Network security management
To ensure the protection of information in networks and the protection of the supporting infrastructure.

Media handling
To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

Exchange of information
To maintain the security of information and software exchanged within Hengtian's and with any external entity.

Electronic commerce services
To ensure the security of electronic commerce services, and their secure use.

Monitoring
To detect unauthorized information processing activities.

2) Current policies & standards

a) HT-CIS-401 File Transfer
b) HT-CIS-402 Public Data Network Connectivity
c) HT-CIS-403 Remote Access
d) HT-CIS-404 Firewall
e) HT-CIS-405 Web Servers Inside the DMZ
f) HT-CIS-406 Wireless Security
g) HT-CIS-407 Mobile Device Security
h) HT-CIS-408 Desktop Standard

i) HT-CIS-409 UNIX/LINUX Security
j) HT-CIS-410 Virus Protection
k) HT-CIS-411 Windows Security
l) HT-CIS-412 Patch Management
m) HT-CIS-413 Disposal of Technology Hardware
n) HT-CIS-414 Fax Transmission

3) Practice examples

a) Remote access to desktops, workstations, servers is restricted to authorized users and recorded.
b) Firewall rules are reviewed and improved on a regular basis.
c) All USB ports of Hengtian's desktops and laptops are blocked.
d) Employees' and visitors' personal laptops are not allowed to be brought into Hengtian's work area or access to Hengtian's network unless approved by responsible personnel and departments.
e) Desktop equipments are de-certificated before being reassigned to a different user.
f) Only software that licensed to Hengtian and Hengtian approved open source software is permitted to be installed on Hengtian computers.
g) All workstations' auto update function is enabled and security updates will be installed periodically.
h) All workstations have McAfee Anti-Virus\Anti-Spyware (AV\AS) software loaded and are updated periodically.

7. Access control

1) Objectives

Business requirement for access control
To control access to information.

User access management
To ensure authorized user access and to prevent unauthorized access to information systems.

User responsibilities
To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

Network access control
To prevent unauthorized access to networked services.

Operating system access control
To prevent unauthorized access to operating systems.

Application and information access control
To prevent unauthorized access to information held in application systems.

2) Current policies & standards

a) HT-CIS-501 Authentication
b) HT-CIS-502 Access Control
c) HT-CIS-503 Customer Access
d) HT-CIS-504 Logon Security Notice
e) HT-CIS-505 Access to Production Data and Program Code
f) HT-CIS-506 Security Administration
g) HT-CIS-507 Database Security
h) HT-CIS-508 Encryption

3) Practice examples

a) Hengtian adopts strong password strategy:
   - at least 8 characters
   - at least contain 3 of the following 4 elements: upper case, lower case, numbers, and special characters
   - expire every 90 days
b) Staffs can only access files, data and processes that they are authorized to access.

8. Information systems acquisition, development and maintenance

1) Objectives

Security requirements of information systems
To ensure that security is an integral part of information systems.

Correct processing in applications
To prevent errors, loss, unauthorized modification or misuse of information in applications.

Cryptographic controls
To protect the confidentiality, authenticity or integrity of information by cryptographic means.

Security in development and support processes
To maintain the security of application system software and information.

2) Current policies & standards

a) HT-CIS-601 Software Change Control
b) HT-CIS-602 Software Source Code Review
c) HT-CIS-603 Systems Development Lifecycle

3) Practice examples

a) Hengtian has been CMMI3 certified since 2008.

b) All application systems receive the information security assessment and review prior to being deployed into production environment.
c) Hengtian use the secured configuration management tools such as SVN.

9. Information security incident management

1) Objectives

Reporting information security events and weaknesses
To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Management of information security incidents and improvements
To ensure a consistent and effective approach is applied to the management of information security incidents.

2) Current policies & standards

a) Hengtian Information Security Punishment and Reward Policy
b) Related Standard Operation Procedures

3) Practice examples

a) Employees are required to report any suspicious security breaches and threats. (Suspected virus or computer problem, Lost or stolen information/ information asset, unauthorized access, inappropriate activities, Unauthorized/suspicious people or activity in facility, computer virus, hacker intrusion, unauthorized/suspicious people or activity, etc.)
b) Information security incidents are responded quickly, recorded, tracked, and analyzed.

10. Business continuity management

1) Objectives

Information security aspects of business continuity management
To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

2) Current policies & standards

a) HT-CIS-701 Business Continuity Management

3) Practice examples

a) Annual call tree test
b) Evacuation drills
c) Business impact analysis (BIA)
d) Backups sites between two working sites (Sandun office and Buynow office)

11. Compliance

1) Objectives

Compliance with legal requirements
To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

Compliance with security policies and standards, and technical compliance
To ensure compliance of systems with Hengtian's security policies and standards.

2) Current policies & standards

a) HT-CIS-801 Service Provider and Vendor Contracts
b) HT-CIS-802 Software Ownership, Licensing, Testing
c) HT-CIS-803 Intellectual Property
d) HT-CIS-804 Protection of Consumer and Customer Information

3) Practice examples

a) Hengtian strictly complies with domestic and international laws and regulations concerning intellectual property rights (IPR). (Figure 7 – Hengtian Intellectual Property Protection Practices)

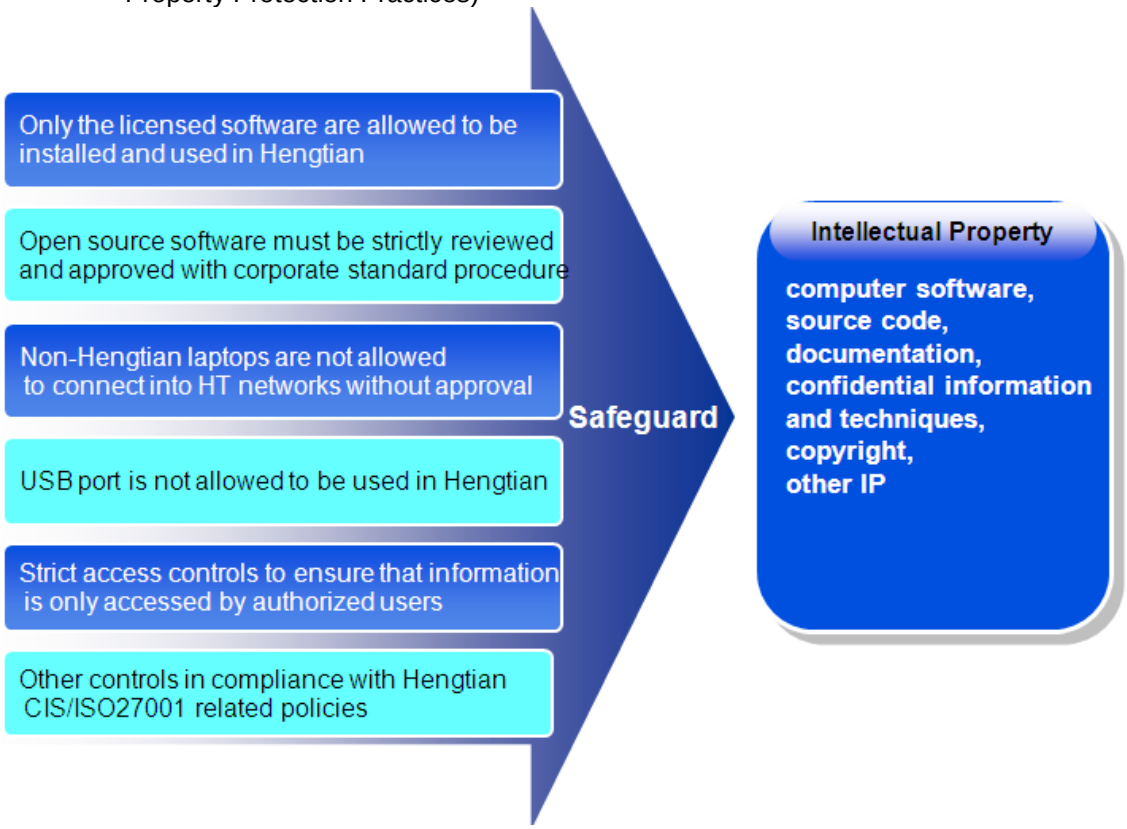

Figure 7 – Hengtian Intellectual Property Protection Practices

b) Hengtian strictly complies with ISO27001 information security standards.(Figure 8 – Hengtian's ISO27001 Certificate)

DET NORSKE VERITAS

MANAGEMENT SYSTEM CERTIFICATE

Certificate No. 43855-2008-AIS-RGC-UKAS

This is to certify that

Insigma Hengtian Software Ltd.

Registration Address: 3F, Building 8, 1st Jiaogong Road, Hangzhou, 310013, P.R. China
Office Address: Building J1, 18#, 1st Xiyuan Road, West Lake District, Hangzhou, 310030, P.R. China
Office Address: 17F&18F, Buynow Technology Building, 23 Jiaogong Road, Hangzhou, 310013, P.R. China

has been found to conform to the Management System Standard:

ISO/IEC 27001:2005

This Certificate is valid for the following product or service ranges:

Information Security Management System Covers Software Development, Testing, Software Technology Transfer, Software Technology Consulting and Related Service Providing, Business Process Outsourcing, Data Processing, Computer System Maintenance and Proprietary Software Products Distribution and Related Technology Services Providing; The Related Facilities and Infrastructure for above Services. This is in Accordance with the Latest Version of Statement of Applicability.

Initial Certification date: December 11th, 2008

Place and date: Shanghai, November 28th, 2011

This Certificate is valid until: December 11th, 2014

for the Accredited Unit: DNV CERTIFICATION LIMITED, UNITED KINGDOM

UKAS MANAGEMENT SYSTEMS 013

The audit has been performed under the supervision of
Li Kun
Lead Auditor

Chen Yi
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.

DNV CERTIFICATION LIMITED, PALACE HOUSE, 3 CATHEDRAL STREET, LONDON SE1 9DE, UNITED KINGDOM - WWW.DNVGA.COM

Figure 8 – Hengtian's ISO27001 Certificate

c) Hengtian conducts information security internal audits quarterly.
d) Hengtian receives information security annual audit by a well-known European audit authority (DNV) every year.

Conclusion

As a leading innovative technology service provider for global financial institutions, Hengtian strictly follows domestic laws and regulations and takes the protections of clients' information, data, and intellectual property rights very seriously. Hengtian has invested a lot of money, people, time and energy on the protections and is ISO27001-certified. Meanwhile, Hengtian continuously

improves the protections according to business development, clients' security requirements and industry standards.