Corporate Information Security

Overview

To maintain an information security program that allows Hengtian to meet customer, partners, employees and regulators expectations for privacy and confidentiality, Hengtian has set up the Corporate Information Security (CIS) Committee and has assigned Information Security Officer to establish and deploy information security management system. Our approach is to adopt and enforce the appropriate industry best-practice policies, solutions and controls required to protect corporate assets and attract new business while retaining existing customers.

Mission

- Enable our clients, partners and employees to conduct business and exchange information in a secure environment
- Protect corporate and clients information assets

Our Information Security Physical Environment

Hengtian high-quality information security physical environment enables our meet customers, partners and employee to conduct business and exchange information in a secure environment where risk is carefully managed and protection of assets is both comprehensive and pervasive.

➢ All entrances are physically secured with badge access controls
➢ Computer centers, HR and Finance offices are located in a secure environment with authorized access
➢ All the entries/exits are equipped with Camera System, 24x7
➢ Employees must ensure that client confidential documents and property are kept safely. Hard copy of confidential documents and information are not allowed to be taken out of office and the electronic version is not allowed to upload to any unauthorized places

Our Information Security Policy

Hengtian establishes and implements corporate information security policies both with the information security requirements and expectations of our customers, partners and employees and ISO 27001/27002 control clauses. The framework and cover range of CIS policies is as below.
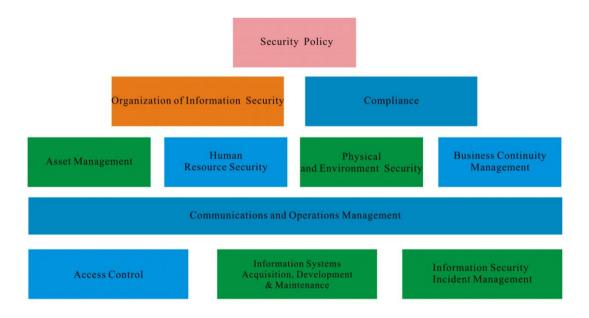

Figure. Hengtian Corporate Information Security Framework

The index of Hengtian Corporate Information Security Policies is as below.

HT-CIS-1 Asset Management Policy

      HT-CIS-101 Information Classification

      HT-CIS-102 Acceptable Use of Information Technology Resource

      HT-CIS-103 Spreadsheets, Macros & Small Applications

      HT-CIS-104 Use of Corporate Assets

HT-CIS-2 Human Resource Security Policy

      HT-CIS-201 Human Resource Security

HT-CIS-3 Physical and Environment Security Policy

      HT-CIS-301 Secure Areas and Physical Access Controls

      HT-CIS-302 Telecommunication Equipment

      HT-CIS-303 Computer Systems

      HT-CIS-304 Printer/Fax Physical Security

      HT-CIS-305 Environmental and Hazard Protection

HT-CIS-4 Communications and Operations Security Policy

      HT-CIS-401 File Transfer

      HT-CIS-402 Public Data Network Connectivity

HT-CIS-403 Remote Access

HT-CIS-404 Firewall

HT-CIS-405 Web Servers inside the DMZ

HT-CIS-406 Wireless Security

HT-CIS-407 Mobile Device Security

HT-CIS-408 Desktop Standard

HT-CIS-409 UNIX/LINUX Security

HT-CIS-4010 Virus Protection

HT-CIS-4011 Windows Security

HT-CIS-4012 Patch Management

HT-CIS-4013 Disposal of Technology Hardware

HT-CIS-4014 Fax Transmission

HT-CIS-5 Access Control Policy

HT-CIS-501 Authentication

HT-CIS-502 Access Control

HT-CIS-503 Customer Access

HT-CIS-504 Logon Security Notice

HT-CIS-505 Access to Production Data and Program Code

HT-CIS-506 Security Administration

HT-CIS-507 Database Security

HT-CIS-508 Encryption

HT-CIS-6 Information Systems Development and Maintenance Policy

HT-CIS-601 Software Change Control

HT-CIS-602 Software Source Code Review

HT-CIS-603 Systems Development Lifecycle

HT-CIS-7 Business Continuity Management Policy

HT-CIS-701 Business Continuity Management

HT-CIS-8 Compliance Policy

HT-CIS-801 Service Provider and Vendor Contracts

HT-CIS-802 Software Ownership, Licensing, Testing

HT-CIS-803 Intellectual Property

HT-CIS-804 Protection of Consumer and Customer Information

Our Monitoring and Improvement Method

Hengtian follows strict and normative measures to enforce and monitor the execution of CIS policies and standards.

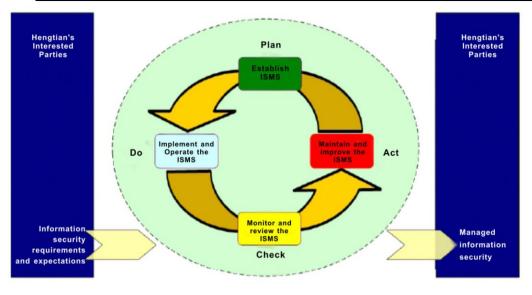1. Hengtian adopts "Plan-Do-Check-Act" model to design and implement information security management system.

Figure. Hengtian Corporate Information Security Implement Process

2. Hengtian does information security trainings regularly to all employees to improve corporate sense and awareness.
3. Corporate Audit Committee takes an internal audit semi-annually.
4. Corporate Information Security Committee reviews the implementation status of CIS policies.
5. Corporate Information Security Committee reviews and refines CIS policies semi-annually.

Achievements

- Corporate Information Security Committee
- Information Security Officer
- Information security Work Group
- Information security Audit Work Group
- High-quality physical environment
- 36 Corporate Information Security Policies
- All employee training and awareness
- Monitoring & Audit
- ISO27001 certification

ISO 27001 REGISTERED

DNV Certification BV

UKAS
INFORMATION SECURITY
MANAGEMENT
013