Information and Communication Security Risk Management

1. Information Security Policy

Our company's information security policy is based on the following guidelines:

1. Establish information security management rules which comply with regulations and customer requirements.
2. Through full employee awareness, create the consensus that everyone is responsible for information security.
3. Protect the confidentiality, integrity, and availability of company, supplier, and customer information.
4. Provide safe production environment to ensure sustainable operation of company business.

For reach these targets, the company focus on three major protection: Anti-Virus, Anti-Hacking, and Anti-Leakage. We build firewall, intrusion detection, anti-virus system, and many internal control systems to improve ability of defense from external attacks and protect internal confidential information.

The company build complete Information Security Management System (ISMS) to reduce threats from system, technology, and procedure, and create a secure environment matching customer need. We continue running "Plan-Do-Check-Act (PDCA)" cycle for improvement.

- **Plan Phase:**
  Focus on security risk management. To strengthen security, this year we refer CNS27001 Information Security Management Standard and create new "Information Security Policy and Operation," and plan to disclose on company website. Let all systems run under standard management rules, reduce human mistake risk causing security vulnerability or production trouble. Through annual review process, we keep improving.
- **Do Phase:**
  Construct multi-layer security defense mechanism. Keep introducing new security risk control technologies, use smart/automated mechanism to improve detection and response process efficiency for various security events. Enhance information security and network security protection flow to protect company important assets.
- **Check Phase:**
  Regular monitoring of information security management indicators, third-party annual audit and company internal security audit, to ensure continuous improvement of security management and defense ability.
- **Act Phase:**
  Review and continue improving. When employee or contractor violate information security rules and procedures, punish according to regulation. Keep external education and internal training for security responsible staff, to raise information security awareness.

2. Information Security Organization Structure

(1) In Year 2023, our company established “Information Security Promotion Team.” Hold meeting at least once a year to promote continuous security improvement.

(2) The “Information Security Promotion Team” is led by the General Manager as convener, and all company departments join. Team is divided into Management Committee and Security Implementation Group.

- **Management Committee:**
  Convener: General Manager, approve all security related policies.
  Members: Department heads, responsible for execution and feedback for feasibility evaluation and improvement suggestion.
- **Security Implementation Group:**
  IT Center: according to new security threats, draft and push related security setups.
  Audit Office: audit implementation status of each security setup.
  Administration Department: arrange security education and training, check personnel attendance.

(3) In 2024 already held one management review meeting. If major security incident happens, will hold meeting immediately, draft response procedures, and execute management measures.

---

3. Specific Information Security Management Plan

In order to achieve security policy and targets, and establish complete protection, we implement following management matters and plans:

(1) **Enhance Defense Ability:**
Perform regular vulnerability analysis and penetration test on security systems, and apply patch and reinforcement to reduce risk. Build network security incident response plan, evaluate impact and loss by event severity level, and take notification and recovery action.

(2) **Improve Security Management Process:**
Besides enhance defense ability, management procedures and awareness also important. Based on NIST (National Institute of Standards and Technology) standard to establish enterprise security framework, and set proper measurement indicators. Employees must follow security rules (for example, strictly control mobile storage devices), and follow SOP operation. Keep applying PDCA cycle for continuous improvement.

(3) **Enhance Network, Endpoint, and Application Security:**
Upgrade endpoint anomaly detection and protection, including Application Whitelisting and EDR (Endpoint Detection and Response) mechanisms. Optimize network security zones, add Multi-Factor Authentication (MFA) for privileged account login on critical servers.

(4) **Risk Control:**
Cooperate with international security vendors, through their professional service to do full security health check. Use third-party objective results as reference for advanced security enhancement, to minimize possible damage when company faces cyber attack.

(5) **Education and Training:**
Conduct company-wide security training and irregular social engineering phishing mail tests, to enhance security awareness. Under support of senior executives and all departments, implement security to every employee.