정보보호 정책

(Information Security Policy)

2025.5

<Information Security Policy>

1. Employees shall understand and faithfully comply with the company's information security policies and relevant laws and regulations.
2. Information assets shall only be used for authorized purposes, and unauthorized access or leakage is strictly prohibited.
3. In the event of a security incident, employees must report it to the relevant departments and government agencies and respond immediately.
4. Employees shall comply with all applicable security-related laws, including each country's personal data protection regulations.

1. Overview of Information Security Policy

1.1 Information Security Awareness Training

1) Regular information security training (online or offline) shall be provided to ensure all employees understand and comply with information security policies.

2) New hires shall receive security policy guidelines and be trained accordingly.

1.2 Regular Information Security Audits

- Internal audits shall be conducted periodically to prevent security violations and ensure compliance with protection policies.

1.3 Information Security Risk Assessment

- Regular risk assessments shall be performed to identify potential threats in advance and establish countermeasures.

1.4 Protection of Customer and Third-Party Data

- Protective measures shall be implemented to prevent unauthorized access or disclosure of customer and third-party data.

1.5 Stakeholder Consent Policy

1) Clear procedures shall be in place for the handling, sharing, and storage of confidential information.
2) Prior consent must be obtained from stakeholders including employees and partners.

1.6 Personal Data Protection Policy

1) Personal data shall be processed in compliance with the legal requirements of each country.
2) Personal information shall not be processed or shared without the data subject's consent.

2. Implementation Measures

2.1 Information Security Violation Handling Procedure

1) An internal reporting channel and procedure shall be established to enable employees and stakeholders to promptly and safely report security violations such as data leaks.
2) Upon receipt of a report, the responsible department shall promptly review the incident and implement corrective actions.
3) The identity and personal information of the reporter shall be kept strictly confidential, and no disadvantage shall be imposed on the individual.

<Information Security Reporting Channel>

- Contact Person: Samuel Park
- Email: samuel.park@hanwhaus.com

2.2 Information Security Incident Response Procedure

1) In the event of an information security incident, the network shall be immediately and entirely disconnected to minimize damage to the company's operations, and the incident shall be reported in accordance with the reporting criteria outlined below.

- Reporting Criteria by Incident Type
  - Minor incidents (e.g., early-stage ransomware infection): Handled by each subsidiary independently
  - Major incidents (e.g., widespread ransomware infection, network shutdown): Reported to the responsible department at headquarters

※ In accordance with the laws of each country, incidents shall be reported to relevant government authorities and law enforcement agencies.

2) The root cause of the incident shall be promptly identified, and actions taken to prevent further damage. The severity of the data breach shall also be assessed immediately.