HIWIN Information Security Policy

1. Purpose

To establish a systematic and continuously improving information security management system that ensures the confidentiality, integrity, and availability of the company's information assets, prevents various information security threats, ensures continuous business operations, and complies with regulatory requirements.

2. Scope

This policy applies to all employees, contract staff, outsourced personnel, and all third-party partners. It covers all information assets owned, managed, or controlled by HIWIN, including but not limited to information systems, networks, databases, documents, hardware equipment, and cloud services.

3. Policy Principles

- Emphasis risk management strategies to deliver tiered safeguards for information assets.
- Promote ongoing improvement and active employee engagement to cultivate a robust information security culture.
- Clearly define responsibilities to ensure effective policy implementation.
- Ensure compliance with applicable laws and international standards, including ISO 27001.
- Consistently enhance the information security framework.

4. Management Structure

- An Information Security Management Committee shall be established under the leadership of the General Manager, who also serves as a member of the board. The committee will comprise department heads and designated information security personnel tasked with the development, implementation, oversight, and ongoing enhancement of information security policies.
- The senior director of Information Department acts as the management representative on the Information Security Management Committee, overseeing and coordinating all aspects of information security management.

5. Risk Assessment and Management

- Undertake a thorough information security risk assessment annually to identify threats, vulnerabilities, and potential impacts, as well as to develop an appropriate risk treatment strategy.
- Conduct interim risk assessments in response to new system deployments, significant changes, or elevated external threats.
- Ensure that management reviews the outcomes of all risk assessments and monitors the progress of subsequent improvement initiatives.

6. Audit and Review

- Internal information security audits should be conducted on a regular basis, at minimum annually, to verify effective policy implementation.
- Additionally, an accredited external audit agency performs annual on-site reviews to confirm compliance with ISO 27001 international standards.
- Both internal and external audits generate comprehensive audit reports and establish corrective and preventive actions as needed.

7. Continuous Improvement Mechanism

- Establish information security management objectives (KPIs) with clearly defined quantitative benchmarks and conduct regular evaluations of progress toward these goals.
- Incorporate the organization’s existing proposal improvement methodologies to actively encourage staff to submit recommendations regarding information security, supported by a structured reward system.
- Gather and analyze both domestic and international intelligence on information security developments to systematically enhance information security management procedures.

8. Ensuring Data Integrity and Protection Data Classification

- HIWIN is accredited by the Taiwan Intellectual Property Management System (TIPS), demonstrating its commitment to safeguarding intellectual property and sensitive information. To ensure data integrity and protection, all information assets undergo a comprehensive classification process based on

confidentiality levels, and each item is clearly labeled according to its classification.

- To minimize risks of unauthorized access, leakage, or misuse. Each confidentiality level is governed by specific protocols and controls that define how data should be:
    - Accessed: Permissions are granted strictly on a need-to-know basis, with multi-factor authentication and role-based access control (RBAC) enforced.
    - Transmitted: Sensitive data must be encrypted during transmission using secure communication protocols (e.g., TLS/SSL, VPN tunnels).
    - Stored: Data is stored in secure environments, with encryption at rest and regular integrity checks to prevent tampering.
    - Destroyed: When data reaches the end of its lifecycle, it is disposed of following secure destruction procedures, such as physical shredding or cryptographic wiping.
- Conducts regular audits and compliance checks to ensure adherence to these protocols. Employees receive mandatory training on data protection policies, emphasizing the importance of proper handling, labeling, and reporting of incidents. This systematic approach not only complies with TIPS requirements but also aligns with international best practices for information security management.

9. Access Control

- Implement the principle of least privilege by granting data access permissions strictly according to job responsibilities.
- Any modifications to permissions following role changes require supervisory approval and are subject to regular (annual) review.
- Critical systems utilize multi-factor authentication to strengthen access security.

10. Data Encryption and Backup

- Confidential and highly confidential files should be encrypted prior to external transmission or storage, utilizing well-established encryption algorithms.
- Perform regular data backups (daily or weekly), ensure backup copies are securely stored offsite, and routinely test restoration procedures to verify data integrity.

11. Data Changes and Audit

- All significant data modifications must be documented in logs, which are to be retained for a minimum of at least one year.
- Change records should be reviewed regularly, and any irregularities must be promptly investigated and addressed.

12. Personal Data and Regulatory Compliance

- It is essential to fully adhere to the Personal Data Protection Act, GDPR, and applicable regulations. HINWIN should regularly evaluate and revise data management protocols, establish a dedicated channel for handling inquiries and objections, facilitate the exercise of data rights, and maintain comprehensive processing records for auditing purposes.
- Prior to collecting, processing, or utilizing personal data, obtain clear written or electronic consent from individuals. Clearly communicate the purpose of data collection, scope of usage, retention period, and any disclosure to third parties, while providing accessible mechanisms for inquiry, amendment, or deletion of personal information.
- In the event of a personal data breach, report to the relevant authority within the statutory timeframe (such as within 72 hours), and proactively notify affected individuals with details regarding the nature of the leak, its potential effects, and responsive actions taken. Conduct thorough internal investigations, risk assessments, and implement corrective measures to mitigate future risks.

13. Threat Monitoring and Incident Response

- Information Security Monitoring Framework

  To ensure the continuous protection of organizational assets and data, the company shall implement a comprehensive information security monitoring framework that includes both internal and external mechanisms:

  - Outsourced Endpoint Monitoring Services
    HIWIN shall engage qualified third-party cybersecurity service providers to establish and operate endpoint security monitoring centers. These centers shall deliver 24/7 real-time surveillance of endpoint devices, including desktops, laptops, and mobile devices. Services shall include Managed Detection and Response (MDR) capabilities, enabling proactive threat identification, containment, and remediation.

  - Centralized Security Event Management
    A Security Information and Event Management (SIEM) system shall be deployed to aggregate, correlate, and analyze logs and security events from across the enterprise. This system shall serve as the central hub for incident detection, forensic analysis, and compliance reporting.

  - Continuous Security Posture Assessment
    Security monitoring shall be continuously evaluated and improved based on threat intelligence, audit findings, and evolving regulatory requirements.

14. Threat Detection Mechanisms

- To proactively identify and mitigate potential threats, HIWIN shall implement a layered defense strategy comprising the following components:

  - Network and Endpoint Protection
    Deploy Intrusion Detection and Prevention Systems (IDS/IPS), Endpoint Detection and Response (EDR) tools, and advanced malware protection solutions across all critical infrastructure and user devices.

  - Vulnerability Management
    Conduct regular vulnerability assessments and penetration testing at least quarterly or upon significant system changes. All identified high-risk

vulnerabilities shall be remediated within defined timelines based on severity ratings.

- Threat Hunting and Behavioral Analytics
  Utilize threat hunting techniques and behavioral analytics to detect anomalous activities that may indicate insider threats or advanced persistent threats (APTs).

15. Information Security Incident Response Protocol

HIWIN shall maintain a formalized and structured approach to managing information security incidents:

- Incident Response Procedures
  Develop and enforce documented Information Security Incident Reporting and Response Procedures, which shall define incident classification levels, escalation paths, reporting timelines, investigation protocols, recovery actions, and post-incident reviews.
- Incident Response Team (IRT)
  Establish a cross-functional Information Security Incident Response Team comprising representatives from IT, Legal, Public Relations, Compliance, and Executive Management. The team shall be responsible for coordinating incident response activities and ensuring timely resolution.
- Incident Simulation Exercises
  Conduct biannual incident response drills to validate the effectiveness of response procedures and improve organizational readiness. Lessons learned shall be incorporated into policy updates and training programs.

16. Incident Handling Lifecycle

All security incidents shall be managed through a standardized lifecycle process:

- Anomaly Detection – Via automated systems or employee reporting.
- Immediate Notification – Report to designated information security personnel.
- Incident Classification and Preliminary Assessment – Determine severity and scope.

- Response Team Activation – Initiate investigation and containment.
- Mitigation Measures – Apply isolation, system repair, data restoration, and other corrective actions.
- Closure and Documentation – Finalize incident report and archive evidence.
- Post-Incident Review – Conduct root cause analysis and revise policies as needed.

17. Log Management and Security Analytics

To support forensic investigations and compliance requirements:

- Mandatory Logging
  All critical systems, applications, and network devices must enable and retain security logs. Logs shall be transmitted to a centralized, secure log repository with access controls and tamper-proof mechanisms.
- Log Review and Analysis
  Perform routine log analysis to identify suspicious activities, unauthorized access attempts, and policy violations. Alerts shall be generated for anomalies requiring immediate attention.

18. Threat Intelligence and Information Sharing

To stay ahead of emerging threats and foster industry collaboration:

- Participation in Threat Intelligence Networks
  Actively engage with industry-specific cybersecurity alliances, ISACs (Information Sharing and Analysis Centers), and governmental threat intelligence platforms to receive timely updates on threat vectors and attack campaigns.
- Internal Dissemination of Alerts
  Issue periodic security bulletins and preventive advisories to all employees, including actionable recommendations to mitigate identified risks.

19. Common Threats and Preventive Controls

HIWIN shall implement targeted controls to address prevalent information security threats:

- Phishing Attacks
  Conduct regular employee awareness training and simulated phishing campaigns. Deploy email filtering and anti-spam technologies to block malicious messages and enhance detection capabilities.
- Malware Infections
  Require installation of certified antivirus and anti-malware software on all endpoints. Ensure automatic updates of virus definitions and system patches to minimize exposure.
- Social Engineering
  Promote organization-wide social engineering awareness programs, including interactive drills and incident reporting mechanisms. Reinforce vigilance against impersonation, baiting, and pretexting tactics.
- Data Leakage
  Enforce data classification and encryption policies for sensitive information. Implement role-based access controls (RBAC) and anomaly detection systems to monitor and prevent unauthorized data access or exfiltration.

20. Employee Responsibilities and Information Security Culture

- Information Security Responsibility Division
  - All employees serve as the first line of defense in safeguarding the organization’s information assets. They are required to strictly comply with this policy, relevant internal regulations, and applicable laws.
  - Department heads are accountable for ensuring that their teams implement and adhere to information security measures, including monitoring compliance and addressing deficiencies promptly.
  - The Information Technology (IT) Department is responsible for implementing technical safeguards, maintaining systems, and ensuring the resilience of IT infrastructure.

- The Information Security Committee, through its designated management representative, oversees the promotion, enforcement, and continuous improvement of information security policies and practices across the organization.

21. Information Security Awareness and Training

- All new employees must complete mandatory information security training during the onboarding process to understand their roles and responsibilities in protecting company data.
- All employees are required to participate in annual information security training sessions, which cover essential topics such as:
    - Social engineering and phishing prevention
    - Secure password creation and management
    - Data protection and privacy obligations
    - Safe handling of confidential and proprietary information
    - Employees in system administration, network management, or other high-privilege roles must undergo advanced, role-specific security training to ensure they are equipped to manage elevated risks.
    - Periodic awareness campaigns, including simulated phishing exercises and security bulletins, will be conducted to reinforce best practices and maintain a strong security culture.
- Reporting and Feedback Mechanism
    - Employees are required to promptly report any observed or suspected information security anomalies, vulnerabilities, or incidents to the designated information security personnel.
    - A dedicated reporting channel, including an official email address and hotline extension, is maintained to ensure prompt and confidential reporting.

        - The organization encourages proactive risk disclosure and will recognize or reward employees who provide valuable security improvement suggestions or report potential threats in a timely manner.

- Violation Handling
    - Any violation of this policy or related security requirements will be addressed in accordance with established disciplinary procedures. Severe breaches may result in termination of employment and referral to legal authorities.
    - All incidents of non-compliance will be documented, analyzed, and reviewed periodically to identify root causes and inform updates to policies, training programs, and preventive measures.

22. Third-Party Information Security Requirements

- Supplier Information Security Management Obligations
    - All supplier and contractor agreements must contain explicit information security clauses that address:
        - Obligations related to data protection and confidentiality
        - Requirements for reporting requirements
        - Liability provisions for breaches and non-compliance
    - All third parties, including suppliers, contractors, and business partners, must sign confidentiality and non-disclosure agreements prior to engagement.
    - The organization will periodically assess the security posture of information-related suppliers, including:
        - Information security policies and technical controls
        - Employee cybersecurity training programs
        - Records of past incidents and corresponding remediation actions

23. Third-Party Access Management

- Any third-party access to company systems or data must be pre-approved by the appropriate department head and granted only through temporary accounts with time-bound permissions.
- Comprehensive access logs must be maintained and reviewed on a regular basis to detect unauthorized or anomalous activities.
- Remote access by third parties must be protected through multi-factor authentication and encrypted communication channels.

24. Third-Party Information Security Incident Response

- Third parties are required to immediately notify the company of any actual or suspected information security incidents and fully cooperate with investigation and remediation efforts.
- The company reserves the right to suspend or revoke third-party access privileges until identified risks have been mitigated and confirmed as resolved.

25. Regular Evaluation and Audit

- HIWIN will conduct formal information security assessments of critical third parties at least once per year. Any identified deficiencies must be addressed within a defined timeframe.
- Additional reviews will be initiated immediately following any major information security incident involving a third party.

26. Policy Maintenance and Regulatory Compliance

- Policy Review and Maintenance
    - The Information Security Management Committee is responsible for drafting, reviewing, and updating this policy to ensure its ongoing relevance and effectiveness.
    - This policy shall be reviewed at least once per year and revised promptly in response to significant regulatory changes, emerging threats, or major business developments.

27. Regulatory Compliance

- This policy is designed to comply with applicable laws and regulations, including but not limited to:
    - Personal Data Protection Act (PDPA)
    - Cybersecurity Management Act
    - Relevant international standards such as ISO/IEC 27001 and GDPR
- HIWIN shall undergo periodic regular third-party audits to validate compliance and verify the effective implementation of information security controls.