V5 TECHNOLOGIES CO., LTD. | CORPORATE SUSTAINABILITY & GOVERNANCE DISCLOSURE

Information Security Governance & Practice Report

Annual Cybersecurity Disclosure & Operational Resilience Overview (2025–2026)

ISO/IEC 27001:2022	Critical / High Risks	XDR & Security Training	Major Security Incidents
SGS Certified for 2 Consecutive Years	Reduced by 91% / 89% YoY	100% Endpoint & Staff Coverage	0 Breaches or Leaks in 2026

1. Information Security Management Policy & International Certification

To safeguard customer data, maintain operational continuity, and strengthen corporate trust, V5 Technologies Co., Ltd. actively advances a systematic Information Security Management System (ISMS). Anchored on the three core pillars of Confidentiality, Integrity, and Availability (CIA), the Company continuously reinforces its internal cybersecurity protection mechanisms.

In 2024, V5 Technologies formally established the Information Management Committee and the Information Security Task Force, enacting the V5 Technologies Information Security Policy and deploying an internationally aligned ISMS framework. Through institutionalized governance workflows, regular risk assessments, and ongoing drills, the Company demonstrates its steadfast commitment to information security governance.

International Certification Milestone: ISO/IEC 27001:2022 Certified

• Certification History: Initially awarded the ISO/IEC 27001:2022 certificate on June 28, 2025, and successfully passed the SGS annual surveillance audit in May 2026, maintaining continuous certification into its second year (Certificate No.: TW25/00000581; valid until June 28, 2028).

• Certification Scope (Statement of Applicability V02): (1) Development and unit testing (excluding software integration testing and release) of Macro Inspection, Micro Inspection, and Micro Measure algorithms by the R&D Department; (2) Operation and maintenance of supporting systems, data center, and network environment by the IT Department.

2. Information Security Governance Organization & Responsibilities

To ensure effective policy execution and cross-functional coordination, V5 Technologies has established an executive-led information security governance structure that clearly delineates decision-making, operational execution, incident response, and independent internal auditing. In 2026, the Committee completed a structural optimization (comprising 8 members) with seamless handover and uninterrupted security operations:

Governance Body	Leadership & Core Members	Key Responsibilities & Operating Mechanism
Information Management Committee (Top Decision-Making Body)	Chair: President Executive Secretary、Members: 8 Senior Executives across Operating Divisions	Reviews and approves information security policies and KPIs, oversees ISMS effectiveness, convenes annual Management Review Meetings, and authorizes key cybersecurity resources.
Information Security Task Force (Dedicated Execution Team)	Leader、Core Members: 6 persons	Executes daily ISMS operations, threat intelligence analysis, vulnerability scanning and remediation, access privilege

		reviews, security training, and social engineering drills; holds monthly security meetings.
Emergency Response Team (Incident Response Unit)	Core Members: Technical Specialists from the InfoSec Task Force	Establishes incident reporting and emergency response SOPs; manages anomaly detection, damage containment, system recovery, and annual Business Continuity Plan (BCP) drills.
Independent Audit Team (Internal Oversight)	Lead Auditor Coordinating with Departmental Audit Representatives	Independently conducts annual ISO/IEC 27001 internal audits, objectively evaluates regulatory and policy compliance across departments, and tracks corrective actions to 100% closure.

3. Year-over-Year Cybersecurity Governance Evolution (2025 vs. 2026)

In 2026, V5 Technologies transitioned its information security program from the Initial Establishment Phase into the Continuous Operation & Optimization Phase, driving measurable risk reduction through quantitative metrics and technical upgrades:

Governance Pillar	2025 Baseline Achievements	2026 Progress & Milestones	Key Delta & Governance Impact
Management System & Certification	Launched ISMS in March 2025; achieved initial ISO/IEC 27001:2022 certification on June 28, 2025.	Passed SGS annual surveillance audit in May 2026; second-year certification remains active and valid.	Transitioned smoothly from system establishment to ongoing operational maturity with continuous risk reviews and audits.
Governance Structure & Accountability	9-member Committee; internal audit led by Miao-Ju Chi; Emergency Response Team led by Senior Director Ching-Chu Lin.	Streamlined to 8-member Committee (adding Deputy Director Chien-Jung Huang); audit led by Yi-Ning Cheng; Emergency Response led by Manager Yu-Ting Wu.	Task Force leadership and core technical staff remained unchanged, ensuring seamless transition with zero operational disruption.
Technical Defense & Quantitative KPIs	Remediated 100% of initial scan findings (22 critical, 90 high); deployed XDR; 100% training completion; 2.80% phishing click rate.	Critical risks cut from 22 to 2 (-91%) and high risks from 90 to 10 (-89%); 14 threat improvements completed; phishing click rate down to 2.17%; 100% XDR coverage; integrated into ERM R01.	Defense-in-depth and employee security awareness advanced in tandem, sharply shrinking attack surfaces and aligning with Enterprise Risk Management.

4. Six Core Execution Pillars, Management KPIs & Performance Results

V5 Technologies enforces quantifiable performance metrics across six strategic domains—governance, access control, physical and network security, risk response, workforce awareness, and supply chain protection—tracking execution progress throughout the year:

Strategic Pillar	Target Management KPIs	Core Execution Initiatives	2026 Performance Outcomes

1. Governance & Organizational Mechanism	• Mgmt. Review ≥ 1/yr • InfoSec Meeting ≥ 1/mo • Internal Audit ≥ 1/yr • Asset Inventory ≥ 1/yr • ISMS Measurement non-conformities ≤ 2/yr	Convene monthly security meetings and annual Management Reviews; execute annual internal audits, information asset inventories, and ISMS effectiveness evaluations.	• Completed Management Review & ISMS effectiveness evaluation in April. • Held 9 monthly InfoSec meetings (May & June combined). • Completed internal audit in March with 100% corrective closure. • Annual asset inventory scheduled for December.
2. System & Access Control Management	• Access review non-conformities ≤ 1/yr • Vulnerability & change review non-conformities ≤ 2/qtr	Enforce Principle of Least Privilege (PoLP) via periodic account and folder permission audits; continuously monitor threat intelligence, software changes, and patch management.	• Completed company-wide account and folder privilege audit in February. • Continuously monitored external threat intelligence, completing 14 targeted security risk enhancements.
3. Physical & Network Security	• Physical access review ≥ 2/yr • Network & backup monitoring non-conformities ≤ 1/half-yr	Enforce strict physical access control and 24/7 surveillance for data centers and offices; deploy automated real-time network monitoring and system redundancy.	• Completed physical access and surveillance configuration audit in April (100% execution rate). • Maintained 24/7 automated monitoring with full audit logs.
4. Risk Control & Incident Response	• Risk & vulnerability scan ≥ 1/yr • Security drill ≥ 1/yr • Endpoint protection anomalies ≤ 1/qtr	Conduct annual risk assessments and vulnerability scans; execute emergency response and BCP drills; deploy Extended Detection and Response (XDR) across endpoints.	• Completed annual vulnerability scan in March: critical risks dropped from 22 to 2 (-91%) and high risks from 90 to 10 (-89%). • Achieved 100% XDR endpoint coverage across office areas.
5. Security Training & Cultural Awareness	• Mandatory annual training ≥ 1 hr/employee • Periodic social engineering simulations	Require all active and newly onboarded employees to complete annual cybersecurity training; reinforce vigilance via internal emails, videos, screensavers, and town halls.	• Achieved 100% training completion across all active and new employees. • Phishing simulation click rate improved from 2.80% (Nov 2025) to 2.17% (Mar 2026), a 0.63 percentage point reduction.
6. Customer & Supply Chain Data Protection	• Privilege & compliance review non-conformities ≤ 1/qtr	Enforce least-privilege data controls aligned with Taiwan's Personal Data Protection Act (PDPA) and EU GDPR principles; mandate supplier Non-Disclosure Agreements (NDAs).	• Completed customer and project account access review in February.

5. Information Security Risk Management & Operational Resilience Roadmap

Integrating cybersecurity into its Enterprise Risk Management framework (ERM R01), V5 Technologies maintains structured controls and forward-looking enhancement roadmaps across six critical IT infrastructure and operational risk scenarios:

Risk Domain & Scenario	Current Control Environment	Enhancement Measures & Roadmap	Timeline / Status
IT Infrastructure & Governance (System Outage or Data Loss)	Security policies & training, ISO 27001 Management Reviews, periodic core system inspections, access controls, and behavioral monitoring / DLP.	Sustain ISO/IEC 27001 management mechanisms and periodic management reviews.	**Completed in 2026 (Ongoing Maintenance)**

Confidential & Personal Data Leakage (Insider Risk or Unauthorized Access)	Security awareness campaigns, network segmentation, least-privilege access, and automated anti-spam / email protection.	Deploy Network Access Control (NAC) device authentication, tighten cleanroom (FAB) USB controls, and deepen network isolation.	**In Progress (Target: Dec 31, 2026)**
External Network & System Intrusion (Exploits & Malware)	Regular vulnerability scanning & patching, XDR / antivirus real-time monitoring, backup & redundancy, firewall rule audits, and external service controls.	Maintain defense-in-depth monitoring, review emerging threat intelligence, and execute continuous patch remediation.	**Continuous Execution (Active & Stable)**
Critical Service Disruption (Server or Storage Failure)	Real-time hardware health monitoring, system redundancy & data backups, and availability planning for core servers and shared storage.	Deploy enterprise-grade Shared Storage infrastructure to establish a High Availability (HA) architecture.	**Jun 30, 2026 (Completed)**
Geopolitical & Supply Chain Risk (Operational & Hardware Uncertainty)	Perimeter intrusion prevention, VPN device authentication, and continuous monitoring & backup of critical network services.	Completed enterprise Shared Storage HA deployment; evaluating safety stock levels and hardware standardization.	**Jun 30, 2026 (Core Milestone Completed)**
Natural Disasters (Power Outage, Earthquake & Continuity)	Data center UPS & environmental alerts, seismic-braced server racks, BCP, Business Impact Analysis (BIA), and local / core offsite backups.	Conduct annual BCP drills and plan the expansion of offsite backup coverage to further strengthen disaster recovery.	**Core Offsite Backup Done; Expansion Planned (2027)**

6. Annual Governance Summary & Ongoing Commitment

- **Sustaining Information Security Governance:** Strictly adhering to the ISO/IEC 27001:2022 standard through regular management reviews, independent internal audits, and risk evaluations. In 2026, V5 Technologies recorded zero major information security incidents and zero customer data breaches.
- **Strengthening Technical Defense & Risk Control:** Enforcing least-privilege access controls, 100% XDR endpoint protection, rapid vulnerability remediation, and 100% workforce security training completion to minimize exposure of critical information assets.
- **Advancing High Availability & Operational Resilience:** Advancing enterprise High Availability (HA) storage architectures, NAC network access enforcement, and expanded offsite backup capabilities to ensure resilient business continuity against evolving cyber threats and meet global customer expectations.