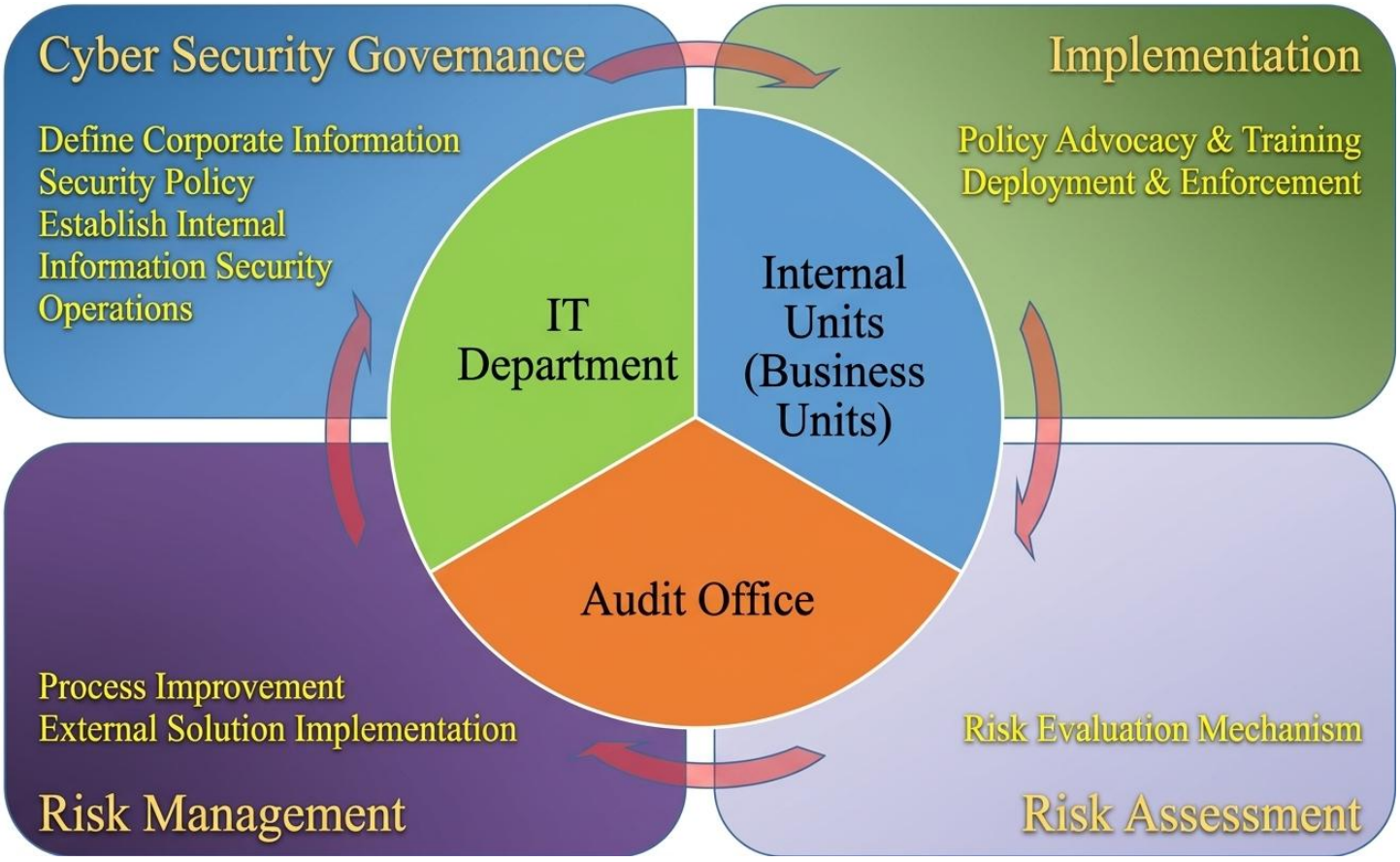
DE LICACY INDUSTRIAL CO., LTD.

Information Security Policy

Information Security Risk Management Framework

- The IT Department serves as the dedicated authority for corporate information security. It is responsible for planning, executing, and promoting information security management initiatives, as well as fostering company-wide security awareness.
- The Internal Audit Office acts as the supervisory and auditing body for information security. Upon detecting any control deficiencies during audits, it immediately requires the audited units to submit comprehensive remediation plans, reports these findings to the Board of Directors, and conducts regular follow-up assessments to mitigate internal cybersecurity risks.
- Operational Management Model: The company adopts the Plan-Do-Check-Act (PDCA) cycle management approach to guarantee the achievement of reliability objectives and drive continuous improvement.



Information Security Policy Statement

To ensure the effective operation and implementation of the company's information management systems, and to maintain the Confidentiality, Integrity, and Availability (CIA triad) of critical information systems, this policy aims to safeguard the secure operation and maintenance of information systems, equipment, and networks, thereby achieving the ultimate goal of business continuity.

Information Security Management Controls

Control Category	Description	Operational Management Standards
Information Access Control	Enforces authorization controls, privilege management, and account administration across all corporate information systems.	**1.** Establish system access policies and authorization regulations. Inform employees and system users of their designated privileges and liabilities through written, electronic, or other official formats. **2.** Upon employee termination or leave of absence, all access privileges to information resources must be revoked immediately as a mandatory off-boarding procedure. Internal job rotations and transfers must trigger prompt privilege adjustments within a specified deadline aligned with access control policies. **3.** Implement a formal user registration and management system to enforce strong password hygiene. The maximum rotation cycle for user passwords shall not exceed three months. **4.** Enforce stringent security controls on external service vendors performing remote system maintenance. Maintain an authorized personnel roster and bind vendors to strict non-disclosure and security liabilities. **5.** Establish an information security audit program to conduct routine and ad-hoc information security compliance audits.
Host & Infrastructure Security Controls	Maintains the security, integrity, and operational availability of internal servers, hosts, and network infrastructure.	**1.** Deploy firewalls at all external network boundaries to inspect and control inbound/outbound data transmission and resource access, backed by rigorous authentication mechanisms. **2.** Utilize Network Intrusion Detection Systems (NIDS) to monitor network traffic for unauthorized upload attempts, web defacement, malicious tampering, or sabotage. **3.** Deploy enterprise anti-malware software with regular definitions update schedules to provide users with a secure web-browsing environment. **4.** Establish system redundancy infrastructure. Perform regular data and software backups alongside disaster recovery readiness operations to guarantee rapid system restoration on new hardware in the event of a disaster or storage media failure. **5.** Disaster Recovery (DR): Conduct ad-hoc simulated cyberattack drills to exercise incident response and system restoration workflows, ensuring alignment with defined security defense-in-depth levels. **6.** Prohibit the storage of confidential or sensitive data/documents on publicly accessible systems. Confidential files must not be transmitted via unencrypted email. **7.** Configure automatic ingestion of security advisories from operating system and application vendors, and

Control Category	Description	Operational Management Standards
		promptly deploy appropriate security patches as recommended. **8.** Perform daily operational health checks on all servers and network infrastructure. Monitor indicators such as chassis system status LEDs, storage array/HDD indicators, storage capacity thresholds, network connectivity link status, and system event logs for anomalies. **9.** Execute vulnerability scanning at least once a year, ensuring all discovered host and system vulnerabilities are formally logged, tracked, and remediated.
Firewall Security Management	Safeguards the enterprise perimeter network to protect internal hosts and core systems from external cyber intrusions and malicious attacks.	**1.** As firewalls constitute the core nexus of the corporate network architecture, redundant sets of firewall host hardware and software configurations must be maintained for failover readiness. **2.** Configure firewalls to continuously log network events. Security log entries must include essential data points such as event date, timestamp, source/destination IP addresses, and network protocols to facilitate operational management and forensic auditing. **3.** Firewall administrators must review and analyze firewall security reports regularly for anomalous activities. Log data must be retained for at least one rolling year. **4.** Restrict firewall administration access exclusively to dedicated, internal management interfaces within the corporate network. Disallow any external terminal logins to ensure management plane security. **5.** Review firewall rule sets and security configurations periodically, making necessary optimizations to ensure alignment with defined security control objectives. **6.** Perform scheduled firewall configuration backups. Backups must be executed locally on a standalone basis; network-based backup paths for firewall configurations are strictly prohibited. **7.** Ensure regular updates to firewall system software. Intrusive signatures and anti-virus definition patterns must be updated daily to counter emerging cyber threats. **8.** Conduct penetration testing at least once a year to evaluate firewall efficacy, identify potential security gaps or misconfigured rules, and log all findings for formal remediation.
Data Backup Principles	Implements scheduled, redundant backups of critical corporate systems	**1.** Enforce the 3-2-1 backup strategy for critical data: maintain at least three copies of essential data distributed across distinct storage media (including off-site storage), with a baseline data retention period of one month.

Control Category	Description	Operational Management Standards
	and enterprise data asset repositories.	**2.** Apply stringent physical and environmental security controls to backup storage repositories, matching the security baselines of primary data centers. Primary site media control standards must extend to secondary/backup sites. **3.** Conduct periodic backup restoration tests to validate data availability, recovery integrity, and media readability. **4.** Enforce encryption for all backup datasets at rest and in transit to prevent unauthorized decryption and data exposure.
Data Restoration Guidelines	Guarantees rapid failover and operational restoration onto alternative infrastructure during unforeseen host or storage hardware outages.	**1.** Barring catastrophic Force Majeure events where the primary data center or network infrastructure is entirely unrecoverable, the Recovery Time Objective (RTO) for core data shall be within 24 hours. The Recovery Point Objective (RPO) must guarantee data freshness within a 48-hour window. Upon restoration, all applications and databases must achieve immediate operational readiness. **2.** Test data restoration procedures regularly to verify the structural integrity and technical usability of backup archives. **3.** Following any major data restoration event, designated technical personnel must monitor the system continuously for three consecutive days to ensure operational stability and validate input data accuracy.
Endpoint Security Management & Awareness	Mitigates the risk of internal endpoint malware infections, data exfiltration, and human-centric insider threats.	**1.** Maintain an updated asset registry detailing user assignments, computer hostnames, and IP addresses for every endpoint. Universally disable USB external storage capabilities; urgent file transfer exceptions require management approval and must be mediated by IT personnel. **2.** Install enterprise Endpoint Detection and Response (EDR) or anti-virus solutions on all endpoints. Implement web filtering and internet access controls; specialized web access requests require a business justification, formal application, and management sign-off. **3.** Conduct ongoing security awareness campaigns covering topics such as phishing email identification, the danger of opening unverified attachments, and out-of-band verification protocols for suspicious customer or vendor communications. **4.** Perform periodic, unannounced Social Engineering and phishing simulations to evaluate user vigilance. Non-compliant users who fail the exercise will be routed to mandatory security awareness training to reinforce corporate security culture.

Control Category	Description	Operational Management Standards
		5. Deploy Endpoint Detection and Response (EDR) agents across all enterprise hosts to gain real-time visibility into anomalous connections or malicious behaviors, minimizing endpoint breach risks while boosting proactive threat alerting and defense capabilities.