# Sunny Optical Technology (Group) Co., Ltd.
# Information Security Management Policy

## I. Policy Statement

Sunny Optical Technology (Group) Co., Ltd. (hereinafter referred to as "the Group") recognizes that information security is the cornerstone of sustainable business development and stakeholder trust. The Group is committed to the core principles of proactive prevention, continuous optimization, risk control, security and efficiency, and customer trust, using international standards as the framework and institutional mechanisms as the driving force, to establish and continuously improve a systematic and standardized information security management system covering the full lifecycle of Group data, comprehensively safeguarding the confidentiality, integrity, and availability of all information assets of the Group.

As the highest guiding document for the Group's information security management, this Policy applies to the Group and all subsidiaries, all employees (full-time and part-time), contractors, suppliers, and all internal and external parties who access, process, store, or transmit the Group's information assets.

## II. Policy Objectives

The Group's Information Security Management Policy is committed to achieving the following core objectives:

1. Ensure data integrity and security: establish full-lifecycle control mechanisms to protect customer information, business partner information, the Group's technical secrets, personal information, and other critical information assets from security threats such as leakage, tampering, loss, or destruction.
2. Monitor and respond to information security threats: deploy a proactive security protection technology foundation, establish a 24/7 threat monitoring, security alerting, and incident emergency response mechanism, and achieve rapid identification, containment, response, and business recovery for information security incidents.
3. Define information security individual responsibilities for all employees: implement an information security responsibility system for all positions, incorporate information security performance into the employee individual performance evaluation system, and ensure that security responsibilities are assigned to individuals.
4. Define information security requirements for third parties: extend information security

control requirements throughout the supply chain, implement security admission, risk assessment, and periodic audits for contractors, service providers, and suppliers, and safeguard the overall information security of the value chain.

5. Continuously improve the information security system: follow the Plan-Do-Check Act(PDCA) cycle management model, regularly review the effectiveness of the security system, benchmark against industry and international standards, and dynamically iterate the Group's information security protection capabilities.

**III. Information Security Governance Structure**

The Group has established a Board of Directors-led, top-down information security governance oversight mechanism with clear rights and responsibilities, ensuring that the information security strategy is aligned with the Group's overall business strategy.

1. Board of Directors Level Oversight

The Board of Directors bears ultimate oversight responsibility for the Group's information security work. The Board is responsible for reviewing the Group's top-level information security policies, medium- and long-term strategies, annual security work plans, and significant risk matters, and approving major security resource investments, ensuring that security resource investments are commensurate with risk levels.

The Strategy and Development Committee established under the Board of Directors fulfills information security strategic decision-making and regular oversight functions. At least one Board member shall have a professional background or experience in information security, cybersecurity, or data governance, ensuring that the Board can make professional judgments on information security matters.

2. Executive Layer Management Responsibility

The Group designates the Group's Chief Executive Officer (CEO) as the primary person in charge of the Group's information security, with overall responsibility for information security management.Main responsibilities: review the Group's information security policies, strategic planning, annual work plans, management principles, and regulatory system documents; make management decisions on major information security risks and significant security incidents; and coordinate security resource allocation.

The Group designates an Information Security Management Representative, who is responsible for establishing the information security operational structure within the Group, namely the Group's Information Security Working Group. Each subsidiary shall establish an independent information security management department, responsible for the implementation of the Group's information security control measures, daily operational maintenance, risk

management, and compliance oversight.

**IV. Information Security Management Principles**

All information security management system development, execution, and improvement work of the Group shall follow the following guiding principles:

1. Compliance First

The Group strictly complies with information security-related laws and regulations in the countries and regions where it operates, including but not limited to:

*the Cybersecurity Law of the People's Republic of China*, *the Data Security Law of the People's Republic of China*, and *the Personal Information Protection Law of the People's Republic of China*, while also complying with international information security-related regulations, automotive industry regulatory requirements, and customer compliance requirements.

2. Risk-Based Approach

Comprehensively adopt a risk-based management approach to identify, assess, and address information security risks, ensuring that security resource investments are commensurate with risk levels. Regularly conduct Group-level information security risk assessments and control effectiveness reviews, and dynamically adjust security control plans based on risk changes.

3. Defense in Depth, Equal Emphasis on Management and Technology

Maintain equal emphasis on management measures and technical protection, and establish a multi-layer defense-in-depth security system. The protection scope comprehensively covers assets, personnel, physical security, network security, data security, business continuity, and other dimensions, achieving refined closed-loop control from top-level management principles to frontline operational procedures.

At the technical level, deploy security protection tools such as Data Loss Prevention (DLP), Endpoint Detection and Response (EDR), Intrusion Prevention System (IPS), Next-Generation Firewall (NGFW), and Security Situational Awareness Platform.

4. Continuous Improvement

Strictly follow the PDCA(Plan-Do-Check-Act) cycle management model, and regularly review the operational effectiveness of the information security management system. Based on risk assessment results, internal and external audit findings, new regulatory requirements, and industry security threat changes, continuously iterate and optimize the Group's security control measures.

5. Full Participation, Equal Rights and Responsibilities

Information security is the inherent responsibility of every employee of the Group. The Group builds an information security culture for all employees from top to bottom and promotes all

employees to actively fulfill their information security obligations through regular security awareness training, institutional constraints, and performance evaluation.

**V. Information Security Management Measures**

1. Policy System

The Group has established and continuously improves a policy system covering key areas with regulatory documents, specifically including the following key areas:

| Control Domain | Scope of Coverage |
|---|---|
| Information Asset Management | Identification and ledger management of critical information assets, full-lifecycle control of information assets |
| Personnel Security | Employee onboarding/offboarding security review, confidentiality agreement signing, non-compete agreement signing, security awareness education and training |
| Area and Facility Security | Office area and server room access control, server room infrastructure protection, on-site physical security protection |
| Network Security | Network access control, internet behavior management, network boundary protection |
| Data Security | Data classification and grading protection, data leakage protection, personal information protection, data flow permission control |
| Incident Management | Information security incident determination criteria, incident reporting procedures, incident handling and post-incident review management |
| Business Continuity | Business continuity plans, disaster recovery plans, emergency incident response management |
| Supplier Security | Third-party information security requirements, supplier information security assessment |

2. Certification and Audits

The Group ensures the continuous and effective operation of the information security system through multiple certification, internal audit, and external audit mechanisms:

(1) Internal Audit: regularly conduct internal audits of the Group's IT infrastructure and information security management system each year. The audit scope includes privacy protection compliance implementation, verifying the execution of policy implementation.
(2) Independent External Audit: annually undergo independent external audits by ISO 27001 certification bodies, and complete TISAX re-audits on a cyclical basis, issuing external audit reports.

3. Data Security Lifecycle Management

The Group establishes general data security control mechanisms, covering general security requirements for the full process of data creation, storage, use, transmission, sharing, and destruction:
(1) Data Classification and Grading: the Group's information assets are divided into four levels: Secret 1, Secret 2, General, and Public. Differentiated security protection strategies are implemented for different classification levels. The classification and special protection rules for personal information are detailed in the Data Privacy and Security Policy.
(2) Access Control: strictly follow the principle of least privilege, and implement physical and system-logical-level access permission controls based on job roles and work responsibilities.
(3) Transmission Security: all sensitive information shall be encrypted when transmitted across systems or entities, ensuring data confidentiality and integrity during transmission.
(4) Storage Security: critical information assets shall be encrypted at storage, with regular backups and off-site disaster recovery protection mechanisms implemented.
(5) Destruction Security: establish standardized data and storage media destruction processes to ensure that expired and discarded information assets are securely and irrecoverably destroyed.

4. Personal Information Protection

All detailed management requirements for personal information collection, use, storage, transmission, deletion, cross-border transfer, privacy impact assessment, data subject rights response, privacy incident handling, third-party supplier privacy control, and privacy complaint channels shall be implemented in accordance with the Group's independent special document, the Data Privacy and Security Policy. This Policy is a supporting special document of this Information Security Management Policy and has the same legal effect.

## VI. Information Security Incidents, Vulnerabilities, and Business Continuity Management

1. Employee Incident, Vulnerability, and Suspicious Activity Reporting and Escalation Process

The Group establishes a clear and actionable multi-level reporting and escalation process:

All employees and third-party personnel who discover information security incidents, system security vulnerabilities, or suspicious risk activities must immediately report them to the Group's Information Security Working Group through designated channels.

The Group's Information Security Working Group shall conduct incident classification upon receiving reported information, and escalate reports to the Information Security Management Representative, CEO, and even the Board of Directors based on the scope of impact and loss level.

The complete incident handling process is divided into five stages: discovery and reporting, incident assessment, evaluation and response, classification and handling, and rectification and filing.

When an incident triggers legal, regulatory, or commercial contract disclosure obligations, the Group shall promptly disclose the security incident to regulatory authorities, customers, and affected stakeholders. For personal information breach incidents, in addition to following this general handling process, privacy-specific notification and data subject notification requirements shall be implemented in accordance with the Data Privacy and Security Policy.

2. Annual Statistics and Disclosure of Security Violation Incidents

The Group maintains an information security violation incident ledger, completely recording all information security violation incidents that occurred and were handled during the year. The Group discloses the total number of information security violation incidents from the previous fiscal year in its annual ESG report. If there are no significant violation incidents in a given year, the disclosed value shall be 0. The statistical scope for privacy-related violation incidents shall also follow the Data Privacy and Security Policy.

3. Business Continuity Plan

The Group develops business continuity plans for information security scenarios, ensuring that when major information security disaster events such as ransomware attacks, system outages, or large-scale data breaches occur, the Group's critical business operations can be restored within preset recovery times. The Group regularly conducts disaster recovery and business continuity emergency drills to verify plan feasibility and continuously optimize.

4. Information Security Vulnerability Analysis Closed-Loop Management

Conduct routine vulnerability scanning and penetration testing, and regularly perform security vulnerability analysis on IT infrastructure and business systems. Rank identified vulnerabilities by risk level, establish vulnerability remediation tracking ledgers, and ensure closed-loop remediation within deadlines. Continuously track external industry security advisories and

high-risk vulnerability intelligence, and promptly deploy security patches and update protection strategies.

**VII. Information Security Awareness Training Program**

The Group treats information security training as a routine management program, establishing a tiered, comprehensive information security training system:

New Employee Onboarding Training: all new employees must complete basic information security training before taking up their positions and sign confidentiality and security responsibility commitments.

Annual Security Awareness Training for All Employees: conduct information security awareness training for all employees each year, achieving 100% employee coverage.

Position-Specific Training: conduct in-depth security skills training for dedicated information security personnel, IT operations and maintenance personnel, and employees in core classified positions.

Special data privacy training content requirements shall be implemented in accordance with the Data Privacy and Security Policy.

**VIII. Third-Party and Supply Chain Information Security Control**

The Group establishes clear general information security control requirements for third-party entities such as suppliers, contractors, and service providers:

1. Include information security-specific clauses in commercial contracts, defining the security obligations and responsibility boundaries of third parties.
2. For key suppliers processing the Group's sensitive information, conduct pre-entry security admission reviews and information security risk assessments, and require third parties to sign confidentiality agreements.
3. Conduct periodic security audits of high-risk third-party partners, and oversee the implementation of third-party security controls.
4. Actively promote upstream and downstream supply chain partners to enhance their information security governance capabilities and jointly build a secure value chain.
5. Third-party privacy-specific constraints and privacy assessment requirements involving personal information processing shall be implemented in accordance with the Data Privacy and Security Policy.

**IX. Continuous Improvement**

The Group's Information Security Working Group organizes at least one management review each year, comprehensively evaluating the operation of the Group's information security management system (including overall privacy compliance). Based on internal audit, external

audit, risk assessment, and security incident review results, the Group benchmarks against international standards such as ISO 27001 and TISAX, follows legal and regulatory updates and emerging cybersecurity threat trends, and continuously optimizes the Group's information security management policies, system documents, and technical protection plans.

**X. Supplementary Provisions**

This Policy shall be implemented from the date of issuance, published upon CEO approval, and is interpreted and revised by the Group's Information Security Working Group.