SF Group Information Security Policy

SF Group (hereinafter referred to as "SF") firmly believes that in the era of accelerating development of the digital economy, information security and data protection constitute a solid foundation for the sustainable and healthy development of the enterprise. Compliance with all applicable national laws, regulations, and industry standards has always been the core philosophy upheld by SF. SF places the responsibility for information security and privacy protection at the forefront of business development, maintains a high level of vigilance against information security risks, and continuously improves its internal information security management system.

The objectives of SF's information security and privacy protection are to provide customers with secure and reliable digital intelligent logistics services and to safeguard the sustained, stable, and healthy development of the enterprise; to establish and strengthen the information security management system to protect customer information and corporate information assets to the greatest extent, safeguarding the legitimate interests of both customers and the company; to address challenges in information security and data protection through open and cooperative engagement with government regulatory authorities, industry organizations, partners, suppliers, and other stakeholders; to ensure compliant operations in all business activities, lawfully processing data and information of customers, employees, and partners, and striving to become a highly respected, globally leading digital intelligent logistics solutions provider.

1. Purpose and Scope of Application

1.1 Purpose

To establish and improve SF's information security management system, enhance overall information security protection capabilities, and ensure the security of information assets while providing customers with secure and reliable digital intelligent logistics services, SF has formulated this Information Security Policy in accordance with the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, industry best practices, and SF's business realities.

1.2 Scope of Application

This policy applies to all employees of SF (hereinafter referred to as "employees"). Short-term workers engaged due to business needs, including contract workers, interns, and third-party partners, shall also comply with this policy. This policy serves as the fundamental guideline for employee information security management.

2. Guiding Principles

SF adopts "Two Protections, Two Commitments" as the guiding principles for information security work:

Protect Customer Interests: By establishing and strengthening the information security management system, SF maximizes the protection of customer information and safeguards customers' legitimate interests.

Protect Information Assets: SF conducts regular risk assessments, clarifies information security responsibilities, and implements information asset protection requirements.

Uphold Compliance Philosophy: Information security protection must comply with legal and regulatory requirements and align with SF's compliance philosophy, culture, and mechanisms.

Maintain a Pragmatic Approach: SF adheres to the principle of appropriate security, continuously monitoring, reviewing, and improving the company's information security management system.

3. Organizational Structure and Policy Management

3.1 Organizational Structure

SF has established a three-tier information security and privacy protection management structure comprising the decision-making level, management level, and execution level. The Information Security and Privacy Protection Committee serves as the highest decision-making body for information security, responsible for major information security decisions, strategic planning, and resource allocation, ensuring that security measures are effectively implemented.

3.2 Policy Management

SF is committed to building an information security management system aligned with industry best practices. Based on recognized governance frameworks, SF has established a comprehensive policy system covering core areas including information security organization, physical and

environmental security, human resources security, network security, data security, personal information protection, content security, and AI application security. This system aims to provide systematic strategic guidance for information security controls and protection across all operational stages.

4. Data Security Management

4.1 Data Classification and Grading

SF implements classification and grading management for data assets involved in business operations. Based on data sensitivity levels and the principle of data minimization, SF applies differentiated protection measures to ensure data security.

4.2 Full Lifecycle Management

In accordance with data lifecycle management principles, SF implements encryption, de-identification, access control, and data backup measures across the stages of data collection, transmission, usage, and storage, ensuring data integrity, confidentiality, and availability.

4.3 Technical Capability Development

SF continuously strengthens data security technical capabilities, building a technical protection system featuring centralized management, encryption and decryption management, and log management.

4.4 Data Security Assessment

SF conducts regular data security assessments, comprehensively evaluating data security risks based on the latest regulatory requirements, and continuously improves the information security management system based on assessment outcomes.

5. Supply Chain Security Management

5.1 Access Management

SF strengthens data security due diligence for third-party partners, with assessments covering baseline security posture, data and privacy protection, system security, and AI security compliance, ensuring that partners meet the company's security standards.

5.2 Agreement Management

SF executes confidentiality agreements and data security agreements with third-party partners,

clarifying the security responsibilities and obligations of both parties, ensuring that data processing activities comply with applicable laws, regulations, and company security requirements.

5.3 Software Supply Chain Security

SF has established a software supply chain security governance framework deeply integrated with Security Development Lifecycle (SDL) principles. Through implementing a shift-left security and built-in security strategy, leveraging core capabilities including asset management, intelligent auditing, and end-to-end supply chain attack prevention, SF standardizes security controls and seamlessly embeds them throughout the entire software development lifecycle from requirements design to operations and release, enhancing the overall security compliance and incident response capabilities of the software supply chain.

6. Monitoring, Response, and Threat Management

6.1 Monitoring and Response

SF has established a routine monitoring and early warning mechanism for continuous monitoring of information assets, conducting threat analysis and situational assessment with timely alert notifications. SF formulates and continuously updates information security incident emergency response plans to enable rapid and effective restoration of business and system operations when information security threats or incidents are detected or occur.

6.2 Vulnerability Management

SF has established a closed-loop vulnerability management mechanism encompassing four stages: vulnerability detection, vulnerability validation, vulnerability risk assessment, and remediation and repair. SF implements comprehensive closed-loop vulnerability management to strengthen cybersecurity defenses and effectively mitigate threats posed by vulnerabilities.

6.3 Network Attack and Defense Drills

SF regularly conducts practical cybersecurity emergency exercises. By simulating various cyber attack scenarios, SF continuously identifies weaknesses in its information security defenses and conducts post-exercise reviews for improvement, comprehensively enhancing incident emergency response capabilities.

7. Compliance Management

SF continuously maintains ISO 27001, ISO 27701, Cybersecurity Classified Protection Level 3 certification, and conducts data security risk assessments, ensuring that the information security management system's compliance posture and risk control standards remain industry-leading.

8. Employee Information Security Responsibilities

SF has established information security reporting channels, encouraging employees to report suspicious security incidents to the information security department, jointly fostering and maintaining a positive information security culture. SF has also established comprehensive information security training and reward-and-penalty management systems. All employees are required to participate in information security training and education, sign confidentiality agreements and information security commitment letters, continuously cultivate a culture of shared responsibility for information security, and SF will enforce strict penalties for any information security violations.

9. Interpretation and Effectiveness

This policy shall be interpreted by the SF Information Security and Privacy Protection Committee. This policy takes effect from the date of issuance. Where any existing relevant policies are inconsistent with this policy, this policy shall prevail.