SUPPLIER SECURITY EXHIBIT

Note: please go to page 20 for Chinese version. 中文版位于第 20 页

This Supplier Security Exhibit ("**Security Exhibit**") applies to the extent that Supplier Processes or has access to Protected Data in connection with its obligations to SHEIN under the applicable agreement for the supply of Products and/or Services (the "**Primary Agreement**"). This Security Exhibit sets forth the information security requirements applicable to Supplier and describes the technical and organizational measures that Supplier shall implement to safeguard Protected Data before and during Processing.

Unless otherwise stated, in the event of a conflict between the Primary Agreement and this Security Exhibit, the terms of this Security Exhibit will control as it relates to the Processing of Protected Data. This Security Exhibit is provided in both English and Chinese for reference. In the event of any inconsistency or conflict between the English version and the Chinese version, the English version shall prevail and control for purposes of interpretation and enforcement.

1. Definitions

"**Backdoor**" means any unauthorized, hidden, or undocumented method of bypassing authentication, access controls, or other security protections in any system, software, or infrastructure within Supplier Systems that is used to provide the Products or Services, or that interacts with SHEIN Systems, including any means of gaining remote or local access without SHEIN's prior written approval.

"**Confidential Information**" means any confidential information or materials relating to the business, products, customers or employees of SHEIN and includes, without limitation, trade secrets, know-how, inventions, techniques, processes, programs, schematics, software source documents, data, customer lists, financial information, pricing, product development, sales and marketing plans, or information that the Supplier knows or has reason to know is confidential, proprietary or trade secret information obtained by Supplier from SHEIN or at the request or direction of SHEIN in the course of performing the Services: (i) that has been marked as confidential; (ii) whose confidential nature has been made known by SHEIN to the Supplier; or (iii) that, due to its character and nature, a reasonable person under like circumstances would treat as confidential.

"**Critical-severity Security Incident**" means a Security Incident affecting Protected Data that has caused, or is highly likely to cause, catastrophic impacts, resulting in extremely severe harm to SHEIN's core business operations, critical infrastructure, financial condition, legal position, or reputation.

"**High-severity Security Incident**" means a Security Incident affecting Protected Data that has caused, or may cause, serious impacts, resulting in significant damage to SHEIN's important business operations, systems, data, or reputation, but not at a catastrophic level.

"**Low-severity Security Incident**" means a Security Incident affecting Protected Data that has caused, or is likely to cause, only minor impacts, resulting in little to no substantive damage to SHEIN's business operations, systems, or data, or that merely presents potential indicators requiring attention.

"**Medium-severity Security Incident**" means a Security Incident affecting Protected Data that has caused, or may cause, moderate impacts, resulting in specific disruptions or damage to SHEIN's routine business operations, non-critical systems, or data, with limited scope and extent.

"**Personal Data**" means any information Processed by Supplier in connection with the performance of the Services under the Primary Agreement that identifies, relates to, describes, is reasonably capable of being associated with,

or could reasonably be linked, directly or indirectly, to an identified or identifiable natural person or household. This includes, without limitation, information pertaining to SHEIN Group Affiliates, customers, partners, contractors, and suppliers. Personal Data is Protected Data.

"**Process**" and any other form of the verb "Process" means any operation or set of operations that is performed upon Protected Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

"Products" means Supplier hardware and software products.

"**Protected Data**" means Personal Data and Confidential Information.

"**Representatives**" means either Party and its affiliate's officers, directors, employees, agents, contractors, temporary personnel, sub-processors, subcontractors, and consultants.

"**Security Incident**" means a confirmed, reasonably suspected, or imminent threat involving unauthorized access, use, disclosure, breach, alteration, theft, loss, corruption, or destruction of Protected Data, or any event that compromises its confidentiality, integrity, or availability within SHEIN Systems or Supplier Systems.

"**Services**" means the services provided by Supplier as described in any service description, offer document, statement of work, or purchase order accepted by SHEIN under the Primary Agreement.

"**SHEIN**" means the SHEIN Group Affiliate that is a party to the Primary Agreement.

"**SHEIN Group Affiliate**" means Roadget Business Pte., Ltd., Infinite Styles Ecommerce Co., Ltd., SHEIN Distribution Corporation, and any entity directly or indirectly controlled by, controlling, or under common control with any of the foregoing, where "control" means either: (i) direct or indirect ownership of more than fifty percent (50%) of the voting interests of the entity; or (ii) the ability to direct or cause the direction of the management or policies of such entity, whether through ownership, contractual rights, or otherwise.

"**SHEIN Systems**" means SHEIN's proprietary or managed information technology infrastructure, including networks, servers, databases, applications, endpoints, and APIs, as well as systems maintained by SHEIN's authorized third parties on SHEIN's behalf.

"Supplier" means the entity that is a party to the Primary Agreement with SHEIN.

"**Supplier Systems**" means any information technology infrastructure, systems, networks, applications, platforms, devices, hardware, software, or tools owned, controlled, or operated by or on behalf of Supplier, including those used to access, store, transmit, or otherwise Process Protected Data or interact with SHEIN Systems.

2. General Security Practices

Supplier has implemented and shall maintain appropriate technical and organizational measures designed to protect Protected Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this Security Exhibit for its personnel, equipment, and facilities at Supplier's locations involved in performing any part of the Primary Agreement.

3. General Compliance

3.1. **Compliance**. Supplier shall implement, document, and maintain processes and procedures designed to ensure compliance with legal, statutory, regulatory, or contractual obligations related to information

security or other security requirements. Such processes and procedures shall be designed to provide appropriate security to protect Protected Data given the risk posed by the nature of the data Processed by Supplier. Supplier shall implement and operate information security in accordance with Supplier's own policies and procedures, which shall be no less strict than the information security requirements set forth in this Security Exhibit.

3.2. **Protection of records**. Supplier shall implement appropriate procedures designed to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.

3.3. **Review of information security**. Supplier's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures) shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

3.4. **Compliance with security policies and standards**. Supplier's management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.

3.5. **Technical compliance review**. Supplier shall regularly review Supplier Systems for compliance with Supplier's information security policies and standards.

3.6. **Information Risk Management ("IRM")**. Supplier shall implement and utilize an appropriate information risk management process to frame, assess, respond to, and monitor risk, consistent with applicable contractual and legal obligations. Supplier is required to have a risk management framework and conduct periodic risk assessments of its environment and systems to understand the risks and apply appropriate controls to manage and mitigate such risks. Threat and vulnerability assessments must be periodically reviewed, and prompt remediation actions taken where material weaknesses are found. Supplier will provide SHEIN with relevant summary reports and analysis upon written request, provided the disclosure of which would not violate Supplier's own information security policies, or applicable laws.

3.7. **Security Assessments**. Supplier shall cooperate with SHEIN's security risk assessment and onboarding processes, including completing any required security questionnaires or related information requests concerning Supplier's Information Security Program and controls for Protected Data. Supplier shall provide accurate and complete information as requested.

3.8. **Audits and Assessments.** Without prejudice to SHEIN's audit rights under the Primary Agreement or any applicable data protection addendum, Supplier shall respond promptly to and cooperate with reasonable requests by SHEIN for security assessments, scans, discovery activities, testing results, and audit reports relating to Supplier's Information Security Program and the Processing of Protected Data.

4. Technical and Organizational Measures for Security

4.1. **Information Security Program**

(a) **Program Implementation and Scope**. Supplier shall implement, maintain, and comply with a comprehensive, written information security program ("**Information Security Program**") that includes appropriate administrative, technical, and physical safeguards. The Information Security Program shall be designed to ensure the confidentiality, integrity, and availability of Supplier Systems, and of all Protected Data that Supplier accesses, Processes, or has in its possession or control.

(b) **Risk-Based Security Objectives**. The Information Security Program shall be reasonably designed to: (i) identify, assess, and protect against reasonably foreseeable internal and external threats to the

security and integrity of Supplier Systems, SHEIN Systems, and Protected Data; (ii) prevent unauthorized access to, use of, alteration of, or destruction of Supplier Systems, SHEIN Systems, and Protected Data; (iii) ensure secure and auditable disposal of Protected Data; and (iv) ensure that SHEIN is promptly notified in the event of a Security Incident in accordance with the requirements of this Security Exhibit.

(c) **Program Maintenance and Continuous Improvement.** Supplier shall regularly monitor, evaluate, and adjust its Information Security Program in response to changes in applicable laws, industry security standards, technology, the sensitivity of Protected Data, the threat environment, and changes to Supplier's operational or technical environment, including mergers, acquisitions, divestitures, joint ventures, outsourcing arrangements, or material modifications to Supplier Systems or data flows.

4.2. **Organization of Information Security**

(a) **Assigned Information Security Responsibility.** Supplier shall appoint one or more security officers or other qualified individuals with appropriate, recognized information security credentials and qualifications to assume overall responsibility for its Information Security Program. Supplier shall provide the names and contact details of its designated security officers to SHEIN and promptly notify SHEIN of any changes.

(b) **Security Roles and Responsibilities.** Supplier shall define internal roles and responsibilities for individuals responsible for security-related tasks and shall establish an information security committee consisting of cross-functional management representatives that meets regularly.

(c) **Project Management.** Supplier shall address information security in project management to identify and appropriately address information security risks.

(d) **Risk Management.** Supplier shall have a risk management framework and conduct periodic risk assessments of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before Processing Protected Data.

4.3. **Human Resources Security**

(a) **General.** Supplier shall ensure that its personnel are under a confidentiality agreement that includes the protection of Protected Data and shall provide adequate training about relevant privacy and security policies and procedures. Supplier shall further inform its personnel of potential consequences of breaching Supplier's security policies and procedures, which shall include disciplinary action, including possible termination of employment for Supplier's employees and termination of contract or assignment for Representatives and temporary personnel.

(b) **Security Awareness and Training.** Supplier personnel with access to Protected Data shall receive appropriate, periodic education and training regarding privacy and security procedures to aid in the prevention of unauthorized use, or inadvertent disclosure, of Protected Data, and training regarding how to effectively respond to security incidents. Training shall be provided before Supplier personnel are granted access to Protected Data or begin providing the Services. Training shall be regularly reinforced at least annually through refresher training and awareness materials.

(c) **Background Checks.** In addition to any other terms in the Primary Agreement related to this subject matter, Supplier shall conduct background checks for its personnel, in compliance with applicable laws and Supplier's policies.

4.4. **Personnel Access Controls**

(a) **Limited Use**. Supplier understands and acknowledges that SHEIN may be granting Supplier access to sensitive and proprietary information and SHEIN Systems. Supplier will not (i) access the Protected Data or SHEIN Systems for any purpose other than as necessary to perform its obligations to SHEIN; or (ii) use any system access information or log-in credentials to gain unauthorized access to Protected Data or SHEIN Systems, or to exceed the scope of any authorized access.

(b) **Authorization**. Supplier shall restrict access to Protected Data, Supplier Systems, and SHEIN Systems at all times solely to those Representatives whose access is necessary to performing Supplier's obligations to SHEIN.

(c) **Personnel Access Management**. Supplier shall (i) prohibit personnel from copying or transmitting Protected Data, except as necessary to deliver the Services (and any such copies will be considered Protected Data); (ii) immediately revoke access upon a change in job responsibilities or status; (iii) promptly notify SHEIN of any changes to SHEIN account access resulting from changes in employment status; (iv) maintain written records of the application, approval, and revocation processes for accounts and privileges; (v) implement strong passphrase requirements that align with industry standards for user authentication (or if authentication is not based on passwords, the method shall be assessed and approved by SHEIN in advance); and (vi) prohibit altering or deleting Protected Data, or taking any actions that could compromise the availability, confidentiality, or integrity of SHEIN systems and Protected Data**.**

(d) **Acceptable Use of SHEIN Systems and Facilities**. To the extent Supplier personnel are granted access to SHEIN Systems or SHEIN-controlled facilities, such personnel shall comply with applicable SHEIN internal security and acceptable use policies governing such access. SHEIN shall make such applicable policies available to Supplier upon request or prior to granting such access.

4.5. **Secure Disposal of Protected Data**. Supplier shall use data disposal methods appropriate to the storage medium and consistent with recognized industry standards, including NIST SP 800-88 Rev. 1 (Purge or Destroy) or a functionally equivalent alternative. All such deletion shall render Protected Data permanently unreadable, inaccessible, and irretrievable. Upon SHEIN's written request, Supplier shall provide a written certification confirming that Protected Data has been securely and permanently deleted in accordance with this provision.

4.6. **Device and Media Security**

(a) **Encryption and Transport of Protected Data**. Supplier shall encrypt all devices that store or otherwise Process Protected Data, including without limitation desktops, laptops, mobile devices, servers, and removable media. Any media containing Protected Data that is transferred outside Supplier's facilities shall be encrypted using industry-standard protocols, logged, authorized by appropriate management, and transmitted via a secure, trackable delivery method. Backup and archival media containing Protected Data shall also be encrypted, and access to such off-site media shall be restricted to authorized personnel.

(b) **Device Configuration and Use Restrictions**. Supplier shall ensure that (i) no removable media is used in connection with the Services or Protected Data unless prior written authorization is obtained from SHEIN; (ii) the latest recommended versions of operating systems, software, and firmware are installed on Supplier Systems; (iii) all devices used to provide Services are equipped with effective malware protection and automatically receive updated patches and virus definitions at least daily; and (iv) all devices are properly hardened to address known or reasonably foreseeable security vulnerabilities.

4.7. **Storage Security**

(a) **General**. Supplier shall implement and maintain appropriate and robust measures to protect Protected Data in electronic storage against unauthorized access, use, disclosure, alteration, or destruction.

(b) **Encryption and Data Handling Requirements**. Supplier shall (i) encrypt Protected Data using algorithms and key lengths that meet or exceed industry-recognized security standards; (ii) logically segregate Protected Data from Supplier's other data, and (iii) prohibit the storage of Protected Data in plaintext in any environment.

4.8. **Physical and Environmental Security**

(a) **Physical Access to Facilities**. Supplier shall: (i) limit physical access to facilities where systems that Process Protected Data are located to authorized individuals only; (ii) define and maintain appropriate security perimeters to protect areas containing Protected Data and Processing systems; (iii) ensure such facilities are continuously monitored and access-controlled at all times (24x7); and (iv) implement access control procedures using key card systems and/or appropriate sign-in protocols, register all personnel accessing the facilities, and require them to carry valid identification badges at all times.

(b) **Physical Access to Equipment**. Supplier equipment used to Process Protected Data shall be protected using industry-standard physical security controls to limit access to authorized personnel.

(c) **Protection from Environmental Disruptions**. Supplier shall implement appropriate controls designed to protect against data loss resulting from power supply failures, electrical surges, or line interference affecting Supplier Systems.

(d) **Clean Desk and Screen Policy**. Supplier shall implement and enforce policies requiring a "clean desk" and "clear screen" environment to prevent inadvertent access to or disclosure of Protected Data.

4.9. **Subcontractors and Representatives**. Supplier shall ensure that all Representatives, including subcontractors and sub-processors, who Process Protected Data, access SHEIN Systems, or perform services subject to this Security Exhibit, comply with security measures no less stringent than those set forth in this Security Exhibit, to the extent applicable to their role.

4.10. **Backdoor Prohibition.** Supplier shall ensure that no Backdoors are included in any Products or Services provided or made available to SHEIN. Supplier shall not, under any circumstances, intentionally create, retain or permit any Representatives to create or retain, any Backdoors.

5. Management of Security Incidents

5.1. **Security Incident Response Plan**. Supplier shall document, implement, maintain, and periodically test a comprehensive Security Incident Response Plan ("**Security Incident Response Plan**"). The plan shall include policies and procedures to detect, respond to, and recover from Security Incidents in a timely, effective, and orderly manner. It shall define clear escalation paths, personnel roles and responsibilities, and internal and external communication protocols. The plan shall be regularly reviewed and tested to ensure ongoing effectiveness. All Representatives shall be made aware of their responsibilities to report Security Incidents in accordance with the Security Incident Response Plan.

5.2. **Incident Classification and Impact Assessment**. The Security Incident Response Plan shall include an incident classification framework for determining whether a security event qualifies as a Security Incident. The classification shall be based on the potential or actual impact and scope of the event.

5.3. **Contingency Planning**. Supplier shall maintain emergency and contingency plans for all facilities that host Supplier Systems which Process Protected Data. Supplier shall verify the effectiveness of such information security continuity controls at regular intervals.

5.4. **Response Process and Coordination**. Supplier shall take immediate action to contain and mitigate the impact of any Security Incident. Supplier shall designate one or more points of contact available to SHEIN for coordination during incident response activities. Upon request and to the extent permitted by applicable law and contract, Supplier shall provide SHEIN with access to relevant security logs and supporting information. Supplier shall also deliver detailed incident reports and supporting documentation, including forensic investigation results and remediation steps, on a daily basis or at such other frequency reasonably requested by SHEIN throughout the incident response lifecycle.

5.5. **Data Recovery**. Supplier shall maintain redundant storage and implement data recovery procedures sufficient to reconstruct Protected Data in its original state as recorded in the most recent backup provided by SHEIN.

6. Supplemental Security Annexes

6.1. Supplier shall comply with the supplemental technical and organizational security measures applicable to the type of Services Supplier provides under the Primary Agreement. These requirements are set forth in the following Annexes, each of which forms part of this Security Exhibit and may be updated by SHEIN from time to time. SHEIN shall notify Supplier of any material changes to the Annexes.

(a) **Annex 1 - Software-as-a-Service (SaaS) Requirements**: To the extent Supplier provides hosted or cloud-based software applications to SHEIN (including platforms accessed via web or mobile interfaces), Supplier shall comply with **Annex 1 - Software-as-a-Service (SaaS) Requirements** located here.

(b) **Annex 2 - API Integration Requirements**. To the extent Supplier integrates with SHEIN Systems through application programming interfaces (APIs) developed, operated, or maintained by the Supplier, Supplier shall comply with **Annex 2 - API Integration Requirements** located here.

(c) **Annex 3 - Installed Software Requirements**. To the extent Supplier provides software that is installed and operated by SHEIN within SHEIN's environment or that of a third party acting on SHEIN's behalf (e.g., on-premises or self-hosted applications under SHEIN's control), and such software is not part of a hosted or SaaS offering, Supplier shall comply with **Annex 3 – Installed Software Requirements** located here.

(d) **Annex 4 - SHEIN On-Prem Deployment Requirements**. To the extent Supplier provides software or systems that are managed or operated by Supplier but physically hosted within SHEIN-controlled environments (e.g., server rooms or colocation centers), Supplier shall comply with **Annex 4 – SHEIN On-Prem Deployment Requirements** located here.

(e) **Annex 5 - Third-Party Warehousing Requirements**. To the extent Supplier provides warehousing services on behalf of SHEIN, including the handling of goods, fulfillment activities, or use of systems that collect or Process data related to warehouse operations (e.g., Warehouse Management Systems or sensor-based tracking), Supplier shall comply with **Annex 5 - Third-Party Warehousing Requirements** located here.

7. Notification Obligations

7.1. **Notification**. Supplier shall, within twenty-four (24) hours of confirmation, notify SHEIN at security@sheingroup.com and privacy@sheingroup.com if any of the following events occur: (i) any

unmitigated, material security vulnerability or weakness in SHEIN Systems or Supplier Systems, known to Supplier, that has compromised Protected Data; (ii) any Security Incident that compromises, or is reasonably likely to compromise, the security of Protected Data and materially impair the business operations of SHEIN; (iii) any Security Incident that negatively impacts the confidentiality, integrity, and availability of Protected Data; or (iv) any known and willful failure or inability to maintain material compliance with requirements of this Security Exhibit and applicable laws.

7.2. **Cooperation**. Supplier shall respond promptly to any reasonable requests from SHEIN for information, cooperation, and assistance in any post-incident investigation, remediation, or communication efforts.

7.3. **Security Communication**. Except to the extent required by applicable law or by pre-existing contractual obligations, Supplier shall not disclose to any third party the occurrence of any event described in this Section in any manner that references or identifies SHEIN without obtaining SHEIN's prior written consent. If disclosure is legally required, Supplier shall coordinate in good faith with SHEIN regarding the timing, content, and recipients of such disclosure. Supplier shall also cooperate fully with SHEIN and any applicable law enforcement or regulatory authorities concerning any unauthorized access to SHEIN Systems or Protected Data. To the extent any such event is attributable to Supplier's fault, Supplier shall bear the costs of any necessary remediation, including data reproduction or other corrective actions required to address the incident or compromise.

ANNEX 1 – SOFTWARE-AS-A-SERVICE (SAAS) REQUIREMENTS

This Annex 1 - Software-as-a-Service (SaaS) Requirements ("**Annex 1**") applies to the extent that Supplier provides hosted or cloud-based software applications to SHEIN, including platforms accessed via web or mobile interfaces ("**SaaS Services**"). This Annex 1 describes the technical and organizational security measures that shall be implemented and maintained by Supplier to ensure the confidentiality, integrity, and availability of SHEIN Systems and Protected Data Processed through such SaaS Services.

Unless otherwise stated, in the event of a conflict between the Primary Agreement and this Annex 1, the terms of this Annex 1 shall control with respect to the security of the SaaS Services.

1. Transmission Security

1.1. **General**. Supplier shall implement and maintain robust controls to protect against unauthorized access to or disruption of Supplier Systems, SHEIN Systems, and Protected Data during transmission over electronic communication networks.

1.2. **Specific controls**. Supplier shall: (i) restrict connections between untrusted networks and Supplier Systems containing Protected Data; (ii) implement application firewalls to protect against application-relevant threats, ensuring the firewalls include security capabilities such as access control, boundary protection, and intrusion prevention; (iii) use industry-standard encryption methods for data in transit; and (iv) maintain the ability to control and secure traffic at the internet boundary, internal VPC boundary, and host boundary.

2. Operation and Processing Security

2.1. **General**. Supplier shall implement policies, procedures, and technical controls to safeguard Supplier Systems during operation and ensure the secure Processing of Protected Data within Supplier Systems.

2.2. **Specific controls**. Supplier shall: (i) maintain capabilities for identity verification, access control, and operational auditing of maintenance activities; (ii) maintain real-time host intrusion detection and prevention capabilities, as well as antivirus protection; and (iii) implement de-identification or masking of Personal Data displayed through user interfaces. If plaintext Personal Data (e.g., identification numbers) must be viewed, such access shall require manual action and be logged.

3. Security Assessments and Testing

3.1. **General**. Supplier shall perform security assessments, tests, and audits on Supplier Systems to identify and address security vulnerabilities, issues, and findings. These assessments shall cover all relevant administrative, technical, and management controls of Supplier and encompass the entire system lifecycle (requirements, design, coding, testing, deployment, and decommissioning) as well as the data lifecycle (collection, storage, processing, transmission, access, destruction).

3.2. **Specific controls**. Supplier shall: (i) perform vulnerability assessments on Supplier Systems at regular intervals, including applications, infrastructure, containers, web applications, and third-party dependencies, categorizing vulnerabilities based on industry standards (e.g., CVSS); (ii) remediate vulnerabilities based on severity: Critical within seven (7) days, High within fourteen (14) days, Medium within thirty (30) days, and all others within sixty (60) days; (iii) maintain the capability to respond to emergency situations involving zero-day vulnerabilities and promptly address and remediate such issues; (iv) engage independent third parties to conduct network vulnerability assessments at least annually; (v) implement a security audit program to test and remediate controls at least annually or when significant changes impact the security of Protected Data; (vi) conduct an annual risk assessment to evaluate threats

and vulnerabilities related to Supplier Systems, facilities, and processes handling Protected Data, and document a remediation plan; (vii) conduct annual penetration testing by a trusted third party and remediate any Medium, High, or Critical vulnerabilities within thirty (30), fourteen (14), and seven (7) days, respectively; (viii) conduct code security audits annually by a trusted third party, confirming the absence or remediation of any Medium or higher risk vulnerabilities; and (ix) upon request, provide SHEIN with results of any assessments, audits, tests, or related reports from the Supplier's Information Security Program.

3.3. **Security Incident Containment and Remediation Timelines.** Supplier shall cooperate fully in the containment and remediation of Security Incidents as follows: (i) for Critical-severity Security Incidents, containment shall be achieved within one (1) hour and remediation completed within one (1) day; (ii) for High-severity Security Incidents, containment shall be achieved within two (2) hours and remediation completed within three (3) days; (iii) for Medium-severity Security Incidents, containment shall be achieved within four (4) hours and remediation completed within seven (7) days; and (iv) for Low-severity Security Incidents, containment shall be achieved within eight (8) hours and remediation completed within fourteen (14) days.

4. Audit Logging

4.1. **Logging capabilities**. Supplier shall implement and maintain tools and procedures to record and monitor activity within Supplier Systems that Process or store electronic information.

4.2. **Logging requirements**. Supplier shall ensure that logs: (i) capture key user activities (e.g., logins, operations, and relevant actions) and are accessible to SHEIN upon request; and (ii) are retained for a duration of at least six (6) months, and for such additional period as may be necessary to comply with applicable legal, regulatory, and business requirements.

5. Contingency Planning and Disaster Recovery

5.1. **General**. Supplier shall implement and maintain contingency plans to address emergencies or other disruptive events (e.g., system failure, fire, vandalism, natural disaster) that could damage or destroy Supplier Systems or Protected Data. These plans shall include a tested and continuously updated data backup plan and disaster recovery plan.

5.2. **Specific controls**. Supplier shall: (i) perform data backups of Supplier Systems according to a defined schedule, with the capability to execute remote (cross-cloud) data backups; and (ii) maintain formal business continuity and disaster recovery plans for Supplier Systems and processes used to provide Services, with testing conducted at least annually and plans updated as necessary.

6. Access Control.

6.1. **Protocol support**. Supplier shall support Security Assertion Markup Language (SAML) and/or OAuth protocols to enable Single Sign-On (SSO) integration with SHEIN Systems.

7. Server Room Security

7.1. **General**. If Supplier hosts its own server rooms, it shall implement appropriate measures to ensure the availability and integrity of systems supporting SaaS Services.

7.2. **Specific controls**. Supplier shall: (i) maintain IT management standards and operational manuals, and ensure dedicated IT personnel are available to effectively oversee and manage IT systems; (ii) implement access controls and monitoring systems to safeguard infrastructure; and (iii) implement appropriate

environmental controls to mitigate risks related to temperature, humidity, fire, or other environmental hazards.

ANNEX 2 – API INTEGRATION REQUIREMENTS

This Annex 2 – API Integration Requirements ("**Annex 2**") applies to the extent that Supplier connects to SHEIN Systems using Supplier-developed Application Programming Interfaces (APIs) ("**API Services**"). This category includes real-time data synchronization between Supplier Systems and SHEIN Systems and typically involves the exchange of sensitive business, transactional, and customer data. This Annex 2 sets forth the technical and organizational security measures that Supplier shall implement and maintain to ensure the confidentiality, integrity, and availability of SHEIN Systems and Protected Data transmitted or Processed through such API Services.

Unless otherwise stated, in the event of a conflict between the Primary Agreement and this Annex 2, the terms of this Annex 2 shall control with respect to the security of the API Services.

1. Transmission Security

1.1. **General**. Supplier shall implement and maintain robust controls to protect against unauthorized access to or disruption of Supplier Systems, SHEIN Systems, and Protected Data during transmission over electronic communication networks.

1.2. **Specific controls**. Supplier shall: (i) use industry-standard encryption methods for all data transmissions; (ii) maintain the capability to control and secure traffic at the internet boundary, internal VPC boundary, and host boundary; and (iii) implement application firewalls to protect against application-relevant threats, including capabilities such as access control, boundary protection, and intrusion prevention.

2. Audit Logging

2.1. **General**. Supplier shall implement and maintain tools and procedures to record and examine activity within Supplier Systems that Process or store electronic information.

2.2. **Specific controls**. Supplier shall ensure that logs: (i) capture key user activities (e.g., logins, operations, and relevant actions) and are accessible to SHEIN upon request; and (ii) are retained for a duration of at least six (6) months, and for such additional period as may be necessary to comply with applicable legal, regulatory, and business requirements.

2.3. **Security Incident Containment and Remediation Timelines.** Supplier shall cooperate fully in the containment and remediation of Security Incidents as follows: (i) for Critical-severity Security Incidents, containment shall be achieved within one (1) hour and remediation completed within one (1) day; (ii) for High-severity Security Incidents, containment shall be achieved within two (2) hours and remediation completed within three (3) days; (iii) for Medium-severity Security Incidents, containment shall be achieved within four (4) hours and remediation completed within seven (7) days; and (iv) for Low-severity Security Incidents, containment shall be achieved within eight (8) hours and remediation completed within fourteen (14) days.

3. Operation and Processing Security

3.1. **General**. Supplier shall implement policies, procedures, and technical controls to safeguard Supplier Systems during operation.

3.2. **Specific controls**. Supplier shall: (i) maintain capabilities for identity verification, access control, and operational auditing for maintenance activities; (ii) maintain real-time host intrusion detection and prevention capabilities and antivirus protection; and (iii) implement de-identification or masking of Personal Data displayed through interfaces. If plaintext Personal Data must be viewed (e.g., identification numbers), such access shall require manual action and be logged.

4. Authentication

4.1. **General**. Supplier shall implement robust authentication mechanisms in accordance with industry standards for security and privacy, such as OAuth 2.0 or equivalent protocols.

4.2. **Specific controls**. Supplier shall: (i) implement token-based authentication with configurable expiration periods, allowing SHEIN to view and set expiration timeframes as required; and (ii) support Just-In-Time (JIT) access to grant time-limited, on-demand privileged access to resources.

5. Input validation

5.1. **General**. Supplier shall implement robust input validation mechanisms aligned with industry best practices to ensure the integrity and security of API interactions.

5.2. **Specific controls**. Supplier shall: (i) validate all input data received through API connections for type, length, format, and business logic consistency prior to Processing; (ii) employ protective countermeasures such as whitelisting and parameterized queries to prevent malicious command execution or injection attacks; (iii) remove or neutralize any dangerous content to mitigate the risk of code execution, command injection, or data corruption; and (iv) implement rate limiting or throttling measures to mitigate Denial of Service (DoS) risks.

6. Security Assessments and Testing

6.1. **General**. Supplier shall perform security assessments, tests, and audits on Supplier Systems connected to SHEIN Systems to identify and address vulnerabilities. These assessments shall cover all relevant administrative, technical, and management controls, the system lifecycle (requirements through decommissioning), and the data lifecycle.

6.2. **Specific controls**. Supplier shall: (i) perform regular vulnerability assessments on Supplier Systems, categorizing findings using industry standards (e.g., CVSS); (ii) remediate vulnerabilities based on severity: Critical within seven (7) days, High within fourteen (14) days, Medium within thirty (30) days, and all others within sixty (60) days; (iii) maintain capabilities to respond promptly to zero-day vulnerabilities; (iv) implement a security audit program to test and remediate controls at least annually or after significant changes impacting Protected Data; (v) conduct an annual risk assessment documenting threats, vulnerabilities, and remediation plans; (vi) conduct annual penetration tests by a trusted third party, with reports confirming resolution of Medium, High, and Critical vulnerabilities within thirty (30), fourteen (14), and seven (7) days, respectively; (vii) perform annual third-party code security audits, confirming that Medium or higher-risk vulnerabilities are either absent or remediated; and (viii) upon request, provide SHEIN with the results of any related assessments, tests, or audits.

7. Contingency Planning and Disaster Recovery

7.1. **General**. Supplier shall maintain contingency plans to address events that could damage or destroy Supplier Systems or Protected Data (e.g., system failure, fire, vandalism, or natural disaster). These shall include data backup and disaster recovery procedures tested annually and regularly improved.

7.2. **Specific controls**. Supplier shall: (i) perform data backups of Supplier Systems on a defined schedule, with the capability for remote (cross-cloud) execution; and (ii) maintain formal business continuity and disaster recovery plans for Supplier Systems used to provide API Services, with annual testing and continual improvement.

ANNEX 3 – INSTALLED SOFTWARE REQUIREMENTS

This Annex 3 – Installed Software Requirements ("**Annex 3**") applies to the extent that Supplier provides software solutions intended for deployment within environments operated by SHEIN or by a third party on SHEIN's behalf, including SHEIN-managed servers, infrastructure, or other controlled environments, where the software is installed, configured, and operated by SHEIN. This excludes Software-as-a-Service (SaaS) platforms and hosted software managed by Supplier. This category includes customizable software delivered by the Supplier, allowing SHEIN to configure and tailor the platform to meet specific operational and security requirements.

Unless otherwise stated, in the event of a conflict between the Primary Agreement and this Annex 3, the terms of this Annex 3 shall control with respect to the security of the software.

1. Secure Software Development

1.1. **General**. Supplier shall implement and maintain policies and procedures to ensure the security and integrity of all software provided to SHEIN throughout its Software Development Life Cycle (SDLC).

1.2. **Specific controls**. Supplier shall: (i) integrate security requirements into every phase of the SDLC to ensure vulnerabilities are identified and addressed early, including during requirements gathering, design, development, testing, deployment, and maintenance; (ii) perform rigorous security testing throughout the SDLC, including static application security testing (SAST), dynamic application security testing (DAST), and vulnerability assessments; (iii) adhere to industry-recognized secure coding practices (e.g., OWASP or SANS/CWE) and conduct regular secure code reviews; (iv) ensure that all third-party components, libraries, and frameworks used in the software are regularly scanned, patched, and validated for known vulnerabilities; and (v) ensure that testing environments operate on infrastructure that is logically or physically separated from production environments, and that test data is controlled, protected, and removed before deployment.

2. Security Assessments and Testing

2.1. **General**. Supplier shall perform regular security assessments, tests, and audits on the software to identify and address vulnerabilities. These assessments shall cover the system and data lifecycle.

2.2. **Specific controls**. Supplier shall: (i) perform regular vulnerability assessments on the software, categorizing findings using industry standards (e.g., CVSS); (ii) remediate vulnerabilities based on severity: Critical within seven (7) days, High within fourteen (14) days, Medium within thirty (30) days, and all others within sixty (60) days; (iii) maintain capabilities to respond promptly to zero-day vulnerabilities; (iv) conduct annual penetration testing by a trusted third party, with reports confirming resolution of Medium, High, and Critical vulnerabilities within thirty (30), fourteen (14), and seven (7) days, respectively; (v) conduct annual third-party code security audits, confirming that Medium or higher-risk vulnerabilities are either absent or remediated; and (vi) upon request, provide SHEIN with the results of any related assessments, tests, or audits.

3. Change and Configuration Management

3.1. **General**. Supplier shall maintain policies and procedures for managing changes and configurations to ensure system integrity, security, and reliability. Supplier shall communicate all material changes to SHEIN in a timely manner.

3.2. **Specific controls**. Supplier shall: (i) maintain a process for documenting, testing, and approving changes before production deployment; (ii) implement version control systems to track configuration changes and maintain detailed change records; (iii) review and validate configurations regularly for compliance

with security and regulatory standards; and (iv) implement a rollback process to restore systems to a stable state if a change causes instability.

4. Software Updates

4.1. **General**. Supplier shall implement a robust patch management process to identify and resolve software vulnerabilities.

4.2. **Specific controls**. Supplier shall maintain a security patching process that requires applying critical patches to software within twenty-four (24) hours and all other patches to software in a timely manner.

5. Third-party Management

5.1. **General**. Supplier shall establish, implement, and enforce security policies and procedures governing third-party vendors (including fourth-party developers) involved in software development, to ensure the security, quality, and compliance of the software.

5.2. **Specific controls**. Supplier shall: (i) conduct security due diligence, including security posture reviews and risk assessments on third-party providers; (ii) perform security assessments of subcontractors and ensure they implement security controls equivalent to those of Supplier; and (iii) implement a secure handover or exit process requiring all source code, documentation, and sensitive data to be returned or securely destroyed, and all access to be revoked, upon termination.

6. Asset Confidentiality. Supplier shall ensure that all assets delivered to SHEIN, including but not limited to application source code, compiled installation packages/images, and specific runtime environment configuration files, are not published or stored on any publicly accessible channels (such as public container registries, public code hosting platforms, public forums, etc.). Supplier is obligated to implement effective measures to prevent unauthorized public disclosure of such assets and shall cooperate with SHEIN in conducting necessary audits to verify compliance.

ANNEX 4 – SHEIN ON-PREM DEPLOYMENT REQUIREMENTS

This Annex 4 – SHEIN On-Prem Deployment Requirements ("**Annex 4**") applies to the extent that Supplier installs, manages, or operates Warehouse Automation software or systems within SHEIN-controlled physical environments (e.g., server rooms or colocation centers) for localized deployment. "**Warehouse Automation**" means the use of advanced technologies, systems, and equipment to automate warehouse operations and management tasks, including but not limited to the storage, handling, sorting, and inventory tracking of goods, as well as associated data processing activities. Warehouse Automation is intended to reduce manual intervention and improve operational efficiency and management standards. This category includes software solutions that are managed by the Supplier but physically hosted in SHEIN's in-house server rooms. Warehouse Automation software or systems are typically accessed by SHEIN through a web browser or proprietary interface and commonly involve the storage, Processing, and transmission of data.

Unless otherwise stated, in the event of a conflict between the Primary Agreement and this Annex 4, the terms of this Annex 4 shall control with respect to the security of the on-premise deployment.

1. Secure Software Development

1.1. **General.** Supplier shall implement and maintain policies and procedures to ensure the security and integrity of all software provided to SHEIN throughout its Software Development Life Cycle (SDLC).

1.2. **Specific Controls.** Supplier shall: (i) integrate security requirements into each phase of the SDLC; (ii) conduct static (SAST) and dynamic (DAST) security testing and vulnerability assessments; (iii) follow industry-recognized secure coding practices (e.g., OWASP, SANS/CWE) and perform secure code reviews; (iv) regularly scan and patch third-party components for vulnerabilities; and (v) separate test environments from production, ensuring test data is controlled and removed before deployment.

2. Security Assessments and Testing

2.1. **General.** Supplier shall perform regular assessments to identify and remediate vulnerabilities throughout the system and data lifecycle.

2.2. **Specific Controls.** Supplier shall: (i) conduct vulnerability assessments regularly, categorizing findings using industry standards (e.g., CVSS); (ii) remediate vulnerabilities based on severity: Critical within seven (7) days, High within fourteen (14) days, Medium within thirty (30) days, and all others within sixty (60) days; (iii) maintain readiness to respond to zero-day vulnerabilities; (iv) conduct annual penetration testing by a trusted third party, confirming resolution of Medium, High, and Critical issues within thirty (30), fourteen (14), and seven (7) days, respectively; (v) conduct annual third-party code audits with confirmation of resolution or absence of Medium or higher-risk vulnerabilities.

3. Change and Configuration Management

3.1. **General.** Supplier shall maintain policies and procedures for secure change and configuration management. Supplier shall notify SHEIN of material changes in a timely manner.

3.2. **Specific Controls.** Supplier shall: (i) document, test, and approve changes before production deployment; (ii) implement version control and maintain change records; (iii) review configurations for policy and regulatory compliance; and (iv) maintain rollback procedures.

4. Software Updates

4.1. **Patch Management.** Supplier shall maintain a robust patch management program and apply critical patches within twenty-four (24) hours and all others in a timely manner aligned with industry practices.

5. Third-Party Management

5.1. **General.** Supplier shall implement policies for managing risks associated with subcontractors or other third parties involved in the software development or deployment process.

5.2. **Specific Controls.** Supplier shall: (i) conduct security due diligence on subcontractors, including security posture and risk assessments; (ii) ensure equivalent or stronger security measures are maintained by subcontractors; and (iii) implement secure transition procedures upon contract termination, including secure return or disposal of data and revocation of access.

6. IT Management. Supplier shall maintain IT management standards and operational manuals. Dedicated IT personnel shall oversee daily operations, maintenance, monitoring, and emergency response.

7. Network Security. Supplier shall implement strict access controls for network connections and limit exposure to insecure or unauthorized processes.

8. On-Site Office Endpoint Environment. Supplier shall ensure all on-site endpoint devices have SHEIN-approved software installed and conform to SHEIN's standardization requirements.

9. Server Security. Supplier shall: (i) assign unique user accounts per server; (ii) ensure server accounts are configured with passwords that comply with industry-recognized best practices for strength and complexity; (iii) implement account lockout after five failed authentication attempts (excluding the fifth); (iv) maintain lifecycle account management; (v) ensure proper upgrade and operational workflows; (vi) configure active-standby hot-switch capabilities; and (vii) ensure no High or Medium vulnerabilities remain present on any production servers.

10. Asset Management. Supplier shall: (i) prohibit the use of removable media by on-site personnel to transfer data without SHEIN's prior written authorization; and (ii) implement an authorization mechanism for installing or using media drives.

11. Personnel Security. Supplier shall: (i) establish standardized onboarding/offboarding procedures for employees involved in on-prem operations consistent with SHEIN's policies; (ii) promptly notify SHEIN of onboarding/offboarding events; and (iii) implement disciplinary protocols for violations of data security policies.

12. Emergency Planning. Supplier shall develop and test emergency response plans regularly to support business continuity and ensure timely production recovery in the event of incidents.

13. Database Security. Supplier shall prohibit the use of default or weak passwords for database accounts and implement security best practices for database access control and encryption.

ANNEX 5 – THIRD-PARTY WAREHOUSE REQUIREMENTS

This Annex 5 – Third-Party Warehouse Requirements ("**Annex 5**") applies to the extent that Supplier provides warehousing services on behalf of SHEIN, including but not limited to inventory storage, order fulfillment, returns processing, or other related logistics functions. Vendors subject to this Annex 5 may operate third-party warehouse facilities, networks, and personnel that support SHEIN's operations. This Annex sets forth the applicable technical, physical, and organizational security measures that Supplier shall implement and maintain.

Unless otherwise stated, in the event of a conflict between the Primary Agreement and this Annex 5, the terms of this Annex 5 shall control with respect to the security requirements of the warehousing services.

1. **Business Continuity and Disaster Recovery**

   1.1. **General.** Supplier shall maintain comprehensive business continuity and disaster recovery capabilities to ensure operational resilience and the continued delivery of warehousing services to SHEIN.

   1.2. **Specific controls.** Supplier shall: (i) maintain documented Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) addressing physical facility-related disruptions; (ii) review and test BCPs and DRPs at least annually; and (iii) implement contingencies to support continued service delivery, including alternate personnel, infrastructure, or logistics providers as needed.

2. **Personnel Management.** To the extent Supplier provides labor or workforce services within warehouse operations supporting SHEIN, Supplier shall: (i) ensure that personnel do not privately install or operate routers, wireless networks, hotspots, or similar infrastructure within the warehouse; and (ii) ensure compliance by all assigned personnel with SHEIN policies, guidelines, and security protocols.

3. **Physical and Environmental Security**. To the extent Supplier provides warehouse facilities for SHEIN's operational needs, Supplier shall: (i) implement environmental controls to protect standardized IT environments within the warehouse, including HVAC systems, humidity sensors, fire suppression systems, and uninterruptible power supplies (UPS); (ii) implement physical security controls, including comprehensive perimeter and interior surveillance systems with high-resolution, HDR, and night vision capabilities, with all recordings securely retained; and (iii) implement secure access procedures such as visitor management, escorts, access logs, identity verification, and regular audits.

4. **Network and IT Infrastructure**. To the extent Supplier provides network infrastructure and connectivity within warehouses that support SHEIN operations, Supplier shall: (i) deploy and maintain a firewall at the internet gateway, with a clearly defined firewall management policy specifying five key elements (Source Address, Destination Address, Service or Port, Action, and Logging), and prohibit the use of 'any, any, any' rules; (ii) ensure the network is properly segmented, with both wired and wireless deployments supporting strong signal coverage and fast roaming capabilities; (iii) maintain continuous internet connectivity through at least two redundant circuits; (iv) implement an intrusion prevention system (IPS) and intrusion detection system (IDS) that covers IP reputation; (v) respond to security alerts and assist in resolution efforts to maintain connectivity and operations; (vi) coordinate the allocation of routable static IP addresses for SHEIN's use; (vii) implement access controls such as 802.1x and MAC address filtering; (viii) conduct regular security assessments of network equipment including switch configurations and access point reviews; and (ix) review and disable unauthorized internet functions on warehouse endpoints.

5. **Asset Management**

   5.1. **General.** Supplier shall implement asset management practices to ensure the integrity, accountability, and secure handling of all warehouse and IT assets.

5.2. **Specific controls.** Supplier shall: (i) implement a lifecycle asset tracking program for all warehouse and IT equipment; (ii) ensure the ability to remotely wipe sensitive data from lost or stolen devices; (iii) require encryption, access controls, and authorization for all removable media; and (iv) securely decommission assets, ensuring complete data erasure or physical destruction prior to disposal or reuse.

供应商安全附件

本《供应商安全附件》（“**安全附件**”）适用于供应商在依据适用产品和/或服务供应协议（“**主协议**”）向SHEIN履行义务过程中处理或接触受保护数据的情况。本安全附件规定了适用于供应商的信息安全要求，并列明了供应商在处理受保护数据前及处理过程中须实施的技术和组织措施，以保障受保护数据的安全。

除非另有声明，如主协议与本安全附件存在冲突，则以本安全附件中关于受保护数据处理相关条款为准。本安全附件同时提供英文和中文版本以供参考。如英文版本与中文版本存在任何不一致或冲突，解释和执行时应以英文版本为准。

1. 定义

“后门”指任何未经授权、隐藏或未记录的方法，能够绕过任何系统、软件或基础设施（用于提供产品或服务，或与 SHEIN 系统交互的供应商系统）中的身份验证、访问控制或其他安全防护措施，包括在未事先获得SHEIN书面批准的情况下实现远程或本地访问的任何手段。

“保密信息”指与SHEIN的业务、产品、客户或员工相关的任何保密信息或资料，包括但不限于商业秘密、专有技术、发明、技术、工艺、程序、原理图、软件源代码、数据、客户名单、财务信息、定价、产品开发、销售和营销计划，或供应商知晓或有理由知晓为机密、专有或商业秘密的信息，此类信息系供应商在履行服务过程中由SHEIN直接提供、按照SHEIN指示获取或经SHEIN请求所获取的：(i) 已被标明为保密的信息；(ii) SHEIN已向供应商表明其保密性质的信息；或(iii) 根据信息本身的特征与性质，处于类似情形的合理人士均会视为保密的信息。

“重大安全事件”指影响受保护数据的安全事件，该事件已经造成或极有可能造成灾难性影响，导致SHEIN的核心业务运营、关键基础设施、财务状况、法律地位或声誉遭受极其严重的损害。

“高危安全事件”指影响受保护数据的安全事件，该事件已经造成或可能造成严重影响，导致 SHEIN 重要业务运营、系统、数据或声誉遭受重大但未达到灾难性程度的损害。

“低危安全事件”指影响受保护数据的安全事件，该事件已经造成或可能造成轻微影响，仅导致 SHEIN 业务运营、系统或数据遭受极小或无实质性损害，或仅为需关注的潜在警示指标。

“中危安全事件”指影响受保护数据的安全事件，该事件已经造成或可能造成中等影响，导致 SHEIN 日常业务运营、非关键系统或数据遭受特定范围和程度有限的中度损害或中断。

“个人数据”指供应商在履行主协议项下服务过程中所处理的、能够识别、关联、描述或可合理与特定已识别或可识别的自然人或家庭直接或间接相关的任何信息，包括但不限于与 SHEIN 集团关联公司、客户、合作伙伴、承包商及供应商相关的信息。个人数据属受保护数据。

“处理”及其相关动词，指对受保护数据采取的任何操作或一组操作，无论是否通过自动化方式进行，包括收集、记录、加固、组织、存储、调整或变更、访问、检索、查询、使用、通过传输披露、传播或以其他方式提供、比对或组合、阻断、删除或销毁等活动。

“**产品**”指供应商的硬件和软件产品。

“**受保护数据**”指个人数据和保密信息。

“代表”指任一方及其关联公司的高管、董事、员工、代理人、承包商、临时人员、分处理方、分包商和顾问。

“安全事件”指涉及未经授权访问、使用、披露、泄露、篡改、盗窃、丢失、损坏或销毁受保护数据的已确认、合理怀疑或即将发生的威胁，或任何在 SHEIN 系统或供应商系统内危及受保护数据的机密性、完整性或可用性的事件。

“服务”指供应商根据主协议项下 SHEIN 所接受的任何服务说明、报价文件、工作说明书或采购订单中所描述的服务。

“SHEIN”指作为主协议一方的 SHEIN 集团关联公司。

“SHEIN 集团关联公司”指 Roadget Business Pte., Ltd.、Infinite Styles Ecommerce Co., Ltd.、SHEIN Distribution Corporation，以及任何直接或间接受上述任一实体控制、控制上述实体或与上述实体处于共同控制下的实体，其中，“控制”指：(i)直接或间接拥有该实体超过百分之五十（50%）的表决权；或(ii)无论通过所有权、合同权利或其他方式，能够直接或引导该实体的管理或政策方向。

“SHEIN 系统”指 SHEIN 拥有或管理的信息技术基础设施，包括网络、服务器、数据库、应用程序、终端和 API，以及 SHEIN 授权第三方代表 SHEIN 维护的系统。

“供应商”指与 SHEIN 签署主协议的实体。

“供应商系统”指由供应商或代表供应商拥有、控制或运营的任何信息技术基础设施、系统、网络、应用、平台、设备、硬件、软件或工具，包括用于访问、存储、传输或其他方式处理受保护数据或与 SHEIN 系统交互的系统。

2. 一般安全实践

供应商已实施并将持续维护适当的技术和组织措施，以保护受保护数据免于意外丢失、毁损或篡改、未经授权的披露或访问、或非法销毁，这些措施包括本安全附件中针对供应商在执行主协议任何部分时所涉人员、设备和设施而制定的政策、程序和内部控制措施。

3. 合规要求总则

3.1 合规。供应商应实施、记录并维护相关流程及程序，以确保遵守与信息安全或其他安全要求有关的法律、法规、监管要求或合同义务。此类流程和程序应设计为提供适当的安全保障，以保护供应商处理的受保护数据，考虑到该数据性质所带来的风险。供应商应根据其自身政策和程序实施并运营信息安全措施，且其严格程度不得低于本安全附件中规定的信息安全要求。

3.2 记录保护。供应商应根据相关法律、法规及合同要求，实施适当的程序，以防止记录丢失、毁损、伪造、未经授权的访问和未经授权的泄露。

3.3 信息安全审查。供应商对信息安全管理方法及其实施情况（即控制目标、控制措施、政策、流程和程序）应由适当的内部或外部评估人员在计划时间间隔内或发生重大变更时进行审查。

3.4 遵守安全政策和标准。供应商管理层应定期审查信息处理及程序是否符合适用的安全政策和标准。

3.5 技术合规性审查。供应商应定期检查供应商系统是否符合供应商自身信息安全政策和标准。

3.6 信息风险管理（“IRM”）。供应商应实施并采用适当的信息风险管理流程，对风险进行界定、评估、应对和监控，并与适用的合同及法律义务保持一致。供应商须建立风险管理框架，定期对其

环境和系统进行风险评估，以全面了解风险，并采取适当控制措施加以管理和减缓。威胁与漏洞评估应定期复查，发现重大薄弱环节时须及时采取补救措施。如不会违反供应商自有信息安全政策或适用法律，在书面请求下，供应商应向 SHEIN 提供相关的摘要报告和分析。

3.7 **安全评估。**供应商应配合 SHEIN 的安全风险评估与准入流程，包括填写与供应商信息安全项目及受保护数据控制措施相关的任何必要安全问卷或信息请求。供应商须按要求准确、完整地提供相关信息。

3.8 **审计与评估。**在不影响 SHEIN 根据主协议或任何适用数据保护附录享有的审计权利的前提下，供应商应及时响应并配合 SHEIN 提出的与供应商信息安全计划及受保护数据处理相关的合理请求，包括但不限于：进行安全评估、扫描、发现活动，提供测试结果及审计报告。

4 安全的技术和组织措施

4.1 信息安全项目

a. **项目实施与范围。**供应商应建立、维护并遵守一套全面、书面的信息安全项目（“信息安全项目”），涵盖适当的管理、技术及物理防护措施。该信息安全项目应确保供应商系统以及供应商访问、处理或拥有或控制的所有受保护数据的机密性、完整性和可用性。

b. **基于风险的安全目标。**信息安全项目应合理设计以：（i）识别、评估并防范对供应商系统、SHEIN 系统和受保护数据的可预见的内部及外部安全威胁及完整性风险；（ii）防止未经授权访问、使用、篡改或破坏供应商系统、SHEIN 系统和受保护数据；（iii）确保受保护数据的安全、可审计的处置；（iv）按照本安全附件的要求，在发生安全事件时及时通知 SHEIN。

c. **程序维护与持续改进。**供应商应定期监控、评估并根据适用法律、行业安全标准、技术、受保护数据的敏感性、威胁环境以及供应商运营或技术环境的变化（包括并购、资产剥离、合资企业、外包安排或对供应商系统或数据流的重大调整）对其信息安全计划进行调整。

4.2 信息安全的组织管理

a. **信息安全责任分配。**供应商应指派一名或多名拥有适当且被认可的信息安全资质和资格的安全官员或其他合格人员，全面负责其信息安全项目的实施。供应商应向 SHEIN 提供所指定安全官员的姓名及联系方式，并在有任何更改时及时通知 SHEIN。

b. **安全职责与分工。**供应商应明确负责安全相关任务人员的内部角色与职责，并组建由跨职能管理代表组成的信息安全委员会，并定期召开会议。

c. **项目管理。**供应商应在项目管理中考虑信息安全，以识别并妥善应对信息安全风险。

d. **风险管理。**供应商应建立风险管理框架，并定期对其环境和系统进行风险评估，以了解所面临的风险，在处理受保护数据前采取适当的控制措施进行管理和减缓风险。

4.3 人力资源安全

a. **通用要求。**供应商应确保其员工签署涵盖受保护数据保护内容的保密协议，并向其员工提供有关隐私和安全政策、程序的充分培训。供应商还应告知员工违反供应商安全政策

和程序的潜在后果，包括纪律处分，如对员工采取的可能解雇，以及对代表人员和临时人员的合同或任务终止。

b. **安全意识与培训。**可以接触受保护数据的供应商员工，应接受适当的、定期的隐私和安全程序教育及培训，以协助防止受保护数据被未经授权使用或无意披露，并培训其有效应对安全事件的能力。培训应在供应商员工获得受保护数据访问权限或开始提供服务前完成，并每年至少通过重复培训及宣传材料进行定期巩固。

c. **背景调查。**除主协议中有关此事宜的其他条款外，供应商还应依照适用法律及其自身政策，对员工进行背景调查。

4.4 人员访问控制

a. **受限使用。**供应商理解并确认，SHEIN 可能会授予供应商访问其敏感和专有信息及 SHEIN 系统的权限。供应商不得：(i) 为履行对 SHEIN 的义务所必需之外的任何目的访问受保护数据或 SHEIN 系统；或(ii) 利用系统访问信息或登录凭证，获得对受保护数据或 SHEIN 系统的未授权访问，或超出任何已授权访问范围的行为。

b. **授权。**供应商应始终仅将受保护数据、供应商系统及 SHEIN 系统的访问权限限制于为履行其对 SHEIN 义务所必需的相关代表。

c. **人员访问管理。**供应商应：（i）禁止员工复制或传输受保护数据，除非为提供服务所必需（且任何该等副本亦视为受保护数据）；（ii）在岗位职责或身份发生变更时，立即撤销其访问权限；（iii）因雇佣状态变更导致 SHEIN 账户访问权限有变时，及时通知 SHEIN；（iv）对账户及权限的申请、审批与撤销流程保持书面记录；（v）实施符合行业标准的强密码要求以进行用户身份验证（如身份验证非基于密码，则所用方法须事先获得 SHEIN 评估并批准）；以及（vi）禁止更改或删除受保护数据，或采取任何可能危及 SHEIN 系统及受保护数据可用性、保密性或完整性的行为。

d. **SHEIN 系统及设施的可接受使用。**若供应商人员获准访问 SHEIN 系统或 SHEIN 管控的设施，上述人员应遵守 SHEIN 关于该类访问的内部安全及可接受使用政策。SHEIN 将在供应商要求或在授予此类访问权限前，向供应商提供相关适用政策。

4.5 受保护数据的安全处置。供应商应采用适合存储介质并符合公认行业标准的数据销毁方法，包括 NIST SP 800-88 修订 1（清除或销毁）或功能等同的替代方法。所有此类删除应使受保护数据永久不可读取、访问及恢复。经 SHEIN 书面要求，供应商应提供书面证明，确认依照本条规定，受保护数据已被安全且永久删除。

4.6 设备与介质安全

a. **受保护数据的加密与传输。**供应商应对存储或处理受保护数据的所有设备实施加密，包括但不限于台式机、笔记本电脑、移动设备、服务器及可移动介质。任何含有受保护数据并转移至供应商设施外部的介质，均应采用行业标准协议进行加密，记录在案，经适当管理层批准，并通过安全、可追踪的传递方式进行传输。含有受保护数据的备份及归档介质亦须加密，且对该类异地介质的访问应仅限获授权人员。

b. **设备配置与使用限制。**供应商应确保：（i）除非事先获得 SHEIN 书面授权，不得在与服务或受保护数据相关的操作中使用可移动介质；（ii）在供应商系统上安装操作系统、软件及固件的最新推荐版本；（iii）用于提供服务的所有设备配备有效的恶意软件防护

措施，并至少每日自动接收补丁及病毒定义更新；（iv）所有设备均经过妥善加固，以解决已知或可合理预见的安全漏洞。

4.7 **存储安全**

a. **一般要求。**供应商应实施并维持适当且强有力的措施，以防止电子存储中的受保护数据遭受未经授权的访问、使用、披露、篡改或销毁。

b. **加密与数据处理要求。**供应商应：(i) 使用符合或高于业内认可安全标准的算法和密钥长度对受保护数据进行加密；(ii) 将受保护数据在逻辑上与供应商的其他数据隔离；(iii) 严禁在任何环境下以明文形式存储受保护数据。

4.8 **物理与环境安全**

a. **设施的物理访问。**供应商应：(i) 限制仅授权人员进入存放处理受保护数据系统的设施；(ii) 明确并维持适当的安全边界，保护存有受保护数据及处理系统的区域；(iii) 确保此类设施 24 小时持续监控并实施访问管控；(iv) 采用门禁卡系统和/或适当的签到流程实施访问控制，对进入设施的所有人员登记，并要求其始终携带有效身份识别证件。

b. **设备的物理访问。**用于处理受保护数据的供应商设备应采取行业标准的物理安全控制措施，仅限授权人员访问。

c. **防范环境干扰。**供应商应实施适当的控制措施，旨在防范因电力供应故障、电涌或线路干扰影响供应商系统而导致的数据丢失。

d. **清桌和清屏政策。**供应商应制定并强制执行“清桌面”及“清屏”政策，以防止意外访问或泄露受保护数据。

4.9 **分包商及代表。**供应商应确保所有代表（包括分包商和次级处理方）在处理受保护数据、访问 SHEIN 系统或履行本安全附件项下服务时，须遵守与本安全附件规定同等严苛的安全措施，并保证其角色范围内的适用性。

4.10 **禁止后门。**供应商应确保在向 SHEIN 提供或交付的任何产品或服务中均不包含后门。供应商在任何情况下均不得有意创建、保留或允许任何代表创建或保留任何后门。

5 安全事件管理

5.1 **安全事件响应计划。**供应商应编制、实施、维护并定期测试一套全面的安全事件响应计划（“安全事件响应计划”）。该计划应包括检测、响应和恢复安全事件的政策和程序，确保及时、高效、有序地应对安全事件。计划应明确上报路径、人员角色与职责，以及内部和外部沟通流程。计划应定期审查和测试，以确保持续有效。所有代表应被告知其按照安全事件响应计划报告安全事件的责任。

5.2 **事件分类与影响评估。**安全事件响应计划应包括一个事件分类框架，用于判定安全事件是否构成安全事故。该分类应基于该事件的潜在或实际影响及范围进行。

5.3 **应急预案。**供应商应为承载处理受保护数据的供应商系统的所有设施，维护应急和应变预案。供应商应定期验证此类信息安全持续性控制措施的有效性。

5.4 **响应流程与协调。**供应商应立即采取措施控制并减轻任何安全事故的影响。供应商应指定一名或多名可供 SHEIN 在事件响应期间联络的联系人。根据 SHEIN 要求，并在适用法律及合同允许的范围内，供应商应向 SHEIN 提供相关安全日志及支持信息。供应商还应在整个事件响应周期内，每日或根据 SHEIN 合理要求的其他频率，向 SHEIN 提交详细的事件报告与支持文件，包括取证调查结果和整改措施。

5.5 **数据恢复。**供应商应维护冗余存储，并实施足以根据 SHEIN 提供的最近一次备份记录以原始状态重建受保护数据的数据恢复流程。

6 补充安全附件

6.1 供应商应遵守适用于其根据主协议提供的服务类型的补充技术及组织安全措施。这些要求载明于以下附件，每一份附件均为本安全附件的一部分，SHEIN 可以不时对其进行更新。如有实质性变更，SHEIN 将通知供应商。

a. **附件 1——软件即服务（SaaS）要求：**如供应商向 SHEIN 提供托管或云端软件应用（包括通过网页或移动界面访问的平台），则供应商应遵守附件 1——软件即服务（SaaS）要求，详见此处。

b. **附件 2——API 集成要求：**如供应商通过由其开发、运营或维护的应用程序接口（API）与 SHEIN 系统进行集成，供应商应遵守附件 2——API 集成要求，详见此处。

c. **附件 3——本地安装软件要求：**如供应商向 SHEIN 提供需在 SHEIN 环境或由代表 SHEIN 的第三方环境内安装和运行的软件（例如 SHEIN 自有管控的本地部署或自托管应用），且该类软件不属于托管或 SaaS 产品，供应商应遵守附件 3——本地安装软件要求，详见此处。

d. **附件 4 - SHEIN 本地部署要求：**若供应商提供由其管理或运营、但物理上托管于 SHEIN 控制环境（如服务器机房或托管中心）内的软件或系统，供应商应遵守附件 4 - SHEIN 本地部署要求，详见。

e. **附件 5 - 第三方仓储要求：**若供应商代表 SHEIN 提供仓储服务，包括货物处理、履约活动，或使用收集或处理与仓库运营相关数据的系统（如仓库管理系统或基于传感器的追踪系统），供应商应遵守附件 5 - 第三方仓储要求，详见。

7 通知义务

7.1 **通知。**若发生以下任何事件，供应商应在确认后的二十四（24）小时内，通过 security@sheingroup.com 及 privacy@sheingroup.com 通知 SHEIN：（i）供应商已知悉、且尚未缓解的 SHEIN 系统或供应商系统中的重大安全漏洞或弱点，已导致受保护数据受到损害；（ii）任何安全事件导致或合理预期会导致受保护数据的安全遭到破坏，并对 SHEIN 业务运行造成重大影响；（iii）任何安全事件对受保护数据的保密性、完整性和可用性造成负面影响；或（iv）任何已知且故意未能或无法在本安全附件及相关法律要求范围内保持实质性合规的情况。

7.2 **合作。**针对 SHEIN 在事故后调查、补救或沟通方面提出的任何合理信息、协作与协助要求，供应商应及时予以回应。

7.3 **安全沟通。**除非适用法律或既有合同义务要求，否则供应商未经 SHEIN 事先书面同意，不得以任何方式向第三方披露本条所述事件的发生，且不得包含任何涉及或识别 SHEIN 的内容。若依据法律必须披露，供应商应与 SHEIN 就披露的时间、内容及接收方本着诚信原则进行协调。供应商还应充分

配合 SHEIN 及任何适用的执法或监管机关，就任何对 SHEIN 系统或受保护数据的未经授权访问事宜进行合作。若相关事件由于供应商原因导致，供应商应承担必要补救措施（包括数据再生产或其他纠正措施）所需费用，以解决该事件或损害。

附件 1 – 软件即服务（SAAS）要求

本附件 1—软件即服务（SaaS）要求（“**附件 1**”）适用于供应商向 SHEIN 提供托管或基于云的软件应用，包括通过网页或移动端访问的平台（“SaaS 服务”）。本附件 1 描述了供应商应实施和维持的技术与组织安全措施，以确保 SHEIN 系统以及通过 SaaS 服务处理的受保护数据的保密性、完整性和可用性。

除非另有说明，如主协议与本附件一之间存在冲突，则就 SaaS 服务安全事项，以本附件一的条款为准。

1. **传输安全**

1.1 **通用要求。**供应商应实施并维持健全的管控措施，以防止在通过电子通信网络传输过程中，未经授权访问或中断供应商系统、SHEIN 系统及受保护数据的情况发生。

1.2 **具体管控措施。**供应商应：(i) 限制不受信任网络与包含受保护数据的供应商系统之间的连接；(ii) 部署应用防火墙以防御与应用相关的威胁，并确保防火墙具备访问控制、边界防护和入侵防御等安全功能；(iii) 对传输中的数据采用行业标准的加密方法；及 (iv) 保持对互联网边界、内部 VPC（虚拟专用云）边界及主机边界流量的控制和安全能力。

2 **运营与处理安全**

2.1 **通用要求。**供应商应实施各项政策、程序及技术管控措施，以保障供应商系统在运营期间的安全，并确保在供应商系统内受保护数据的安全处理。

2.2 **具体管控措施。**供应商应：(i) 具备身份验证、访问控制及维护操作的操作审计能力；(ii) 保持实时主机入侵检测与防御能力，并提供防病毒保护；(iii) 对通过用户界面展示的个人数据实施去标识化或数据脱敏处理。如确需查看明文个人数据（如身份证号），此类访问应需手动操作，并进行日志记录。

3 **安全评估与测试**

3.1 **通用要求。**供应商应对供应商系统开展安全评估、测试与审计，以识别并解决安全漏洞、问题及发现。该等评估应覆盖供应商所有相关的管理、技术和管理控制措施，涵盖整个系统生命周期（需求、设计、编码、测试、部署与退役）及数据生命周期（收集、存储、处理、传输、访问、销毁）。

3.2 **具体管控措施。**供应商应：(i) 定期对供应商系统开展漏洞评估，覆盖应用程序、基础设施、容器、Web 应用及第三方依赖，并根据行业标准（如 CVSS）对漏洞进行分类；(ii) 按（i）中分类标准的严重程度制定漏洞修复时限：严重级（Critical）7 日内、高危级（High）14 日内、中危级（Medium）30 日内，其余所有 60 日内完成修复；(iii) 具备应对“零日”漏洞等紧急情况的响应能力，并及时修复相关问题；(iv) 每年至少委托独立第三方进行一次网络漏洞评估；(v) 实施安全审计计划，至少每年或在影响受保护数据安全的重大变更后测试和修复相关控制措施；(vi) 每年进行一次风险评估，评估供应商系统、场所及处理受保护数据的流程面临的威胁和漏洞，并形成修复计划文档；(vii) 每年委托可信第三方开展渗透测试，并分别在 30 日、14 日和 7 日内修复发现的中危、高危和严重漏洞；(viii) 每年委托可信第三方对代码进行安全审计，确认不存在或已修复任何中等或以上风险级别的漏洞；(ix) 应 SHEIN 要求，向其提供供应商信息安全计划中的所有评估、审计、测试结果或相关报告。

a. **安全事件遏制与修复时限。**供应商应全面配合安全事件的遏制与修复，具体要求如下：（i）对于重大级别安全事件，应在一（1）小时内实现遏制，并在一（1）天内完成修复；（ii）对于高危级别安全事件，应在两（2）小时内实现遏制，并在三（3）天内完成修复；（iii）对于中等级别安全事件，应在四（4）小时内实现遏制，并在七（7）

天内完成修复；（iv）对于低危级别安全事件，应在八（8）小时内实现遏制，并在十四（14）天内完成修复。

4 审计日志记录

4.1 日志能力。供应商应建立并维护工具和流程，以记录和监控处理或存储电子信息的供应商系统中的活动。

4.2 日志要求。供应商应确保日志：（i）能够记录关键用户活动（如登录、操作及相关行为），并可根据 SHEIN 要求进行访问；（ii）日志应至少保留六（6）个月，如为遵守适用的法律、法规及业务要求需要更长时间的，应相应延长保留期限。

5 应急计划与灾难恢复

5.1 通用要求。供应商应制定并维护应急计划，以应对可能损害或破坏供应商系统或受保护数据的紧急或其他突发事件（如系统故障、火灾、破坏行为、自然灾害）。这些计划应包括经过测试且持续更新的数据备份方案和灾难恢复计划。

5.2 具体控制措施。供应商应：（i）根据既定计划对供应商系统进行数据备份，并具备执行远程（跨云）数据备份的能力；（ii）针对供应商系统及用于提供服务的流程，建立正式的业务连续性和灾难恢复方案，并至少每年进行测试，根据需要及时更新相关方案。

6 访问控制。

6.1 协议支持。供应商应支持安全断言标记语言（SAML）和/或 OAuth 协议，以实现与 SHEIN 系统的单点登录（SSO）集成。

7 服务器机房安全

7.1 通用要求。如供应商自有服务器机房，应采取适当措施保障支撑 SaaS 服务系统的可用性和完整性。

7.2 具体控制措施。供应商应：（i）维护 IT 管理规范与操作手册，并确保有专职 IT 人员有效监控和管理 IT 系统；（ii）实行访问控制与监控系统，以保护基础设施安全；（iii）采取适当的环境控制措施，以防范温度、湿度、火灾或其他环境风险。

附件 2 - API 集成要求

本附件 2—API 集成要求（“**附件 2**”）适用于供应商通过供应商开发的应用程序接口（API）（“API 服务”）连接 SHEIN 系统的情形。本类别包括供应商系统与 SHEIN 系统之间的实时数据同步，并通常涉及敏感的业务、交易及客户数据的交换。本附件 2 规定了供应商为确保通过该 API 服务传输或处理的 SHEIN 系统及受保护数据的机密性、完整性和可用性所应实施和维护的技术和组织安全措施。

除非另有说明，如主协议与本附件 2 之间存在冲突，就 API 服务的安全性而言，以本附件 2 的条款为准。

1. **传输安全**

1.1 通用要求。供应商应实施并维持健全的管控措施，以防止在通过电子通信网络传输过程中，未经授权访问或中断供应商系统、SHEIN 系统及受保护数据的情况发生。

1.2 具体控制要求。供应商应：（i）对所有数据传输采用行业标准的加密方法；（ii）具备在互联网边界、内部 VPC 边界及主机边界上对流量进行管控和安全防护的能力；以及（iii）实施应用层防火墙，以防范与应用相关的威胁，包括访问控制、边界防护、入侵防御等功能。

2 **审计日志记录**

2.1 通用要求。供应商应实施并维护工具与程序，以记录和审查在处理或存储电子信息的供应商系统内的活动。

2.2 具体控制要求。供应商应确保日志：（i）记录关键用户活动（如登录、操作和相关行为），并可按 SHEIN 要求提供访问；（ii）保留期限不少于六（6）个月，并根据适用的法律、法规和业务要求，按需延长保存期限。

安全事件遏制与修复时限。供应商应全面配合安全事件的遏制与修复，具体要求如下：（i）对于重大级别安全事件，应在一（1）小时内实现遏制，并在一（1）天内完成修复；（ii）对于高危级别安全事件，应在两（2）小时内实现遏制，并在三（3）天内完成修复；（iii）对于中等级别安全事件，应在四（4）小时内实现遏制，并在七（7）天内完成修复；（iv）对于低危级别安全事件，应在八（8）小时内实现遏制，并在十四（14）天内完成修复。

3 **运营与处理安全**

3.1 通用要求。供应商应制定政策、流程和技术控制措施，以在运行过程中保护供应商系统的安全。

3.2 具体控制措施。供应商应：（i）具备身份验证、访问控制和运维审计的能力，用于维护操作活动；（ii）具备实时主机入侵检测与防护能力，并部署防病毒保护措施；（iii）通过接口展示时，对个人数据实施脱敏或掩码处理。如确需查看明文个人数据（例如身份证号码），此类访问须经人工操作并予以记录。

4 **身份认证**

4.1 通用要求。供应商须按照行业安全与隐私标准（如 OAuth 2.0 或同等协议）实施稳健的身份认证机制。

4.2 具体控制措施。供应商应：（i）实施基于令牌的身份认证机制，支持配置过期时间，允许 SHEIN 根据需求查看及设定令牌有效期；（ii）支持即时访问（Just-In-Time, JIT）以便按需、限时授予对资源的特权访问权限。

5 输入验证

5.1 通用要求。供应商应根据行业最佳实践实施强健的输入验证机制，确保 API 交互的完整性和安全性。

5.2 具体控制措施。供应商应：（i）对通过 API 接口接收的所有输入数据在处理前进行类型、长度、格式及业务逻辑一致性等验证；（ii）采用白名单、参数化查询等防护措施，以防止恶意命令执行或注入攻击；（iii）移除或中和所有危险内容，以降低代码执行、命令注入或数据损坏的风险；（iv）实施速率限制或流量调节措施，降低拒绝服务（DoS）攻击风险。

6 安全评估与测试

6.1 通用要求。供应商应对与SHEIN系统互联的供应商系统进行安全评估、测试和审计，以识别并消除安全漏洞。评估范围覆盖所有相关的管理性、技术性及运维控制措施，涵盖系统全生命周期（从需求提出至退役）及数据生命周期。

6.2 具体控制措施。供应商应：（i）定期对供应商系统进行漏洞评估，并采用行业标准（如 CVSS）对发现的问题进行分类；（ii）根据漏洞严重等级修复：严重级 7 天内、高危级 14 天内、中危级 30 天内，其余60天内完成修复；（iii）具备快速响应零日漏洞的能力；（iv）实施安全审计计划，至少每年或在受保护数据发生重大变更后，对系统控制措施进行测试和修复；（v）每年开展风险评估，记录威胁、漏洞及整改计划；（vi）每年由可信第三方进行渗透测试，出具报告并确认中危、高危、严重级别漏洞分别在30天、14天、7天内完成修复；（vii）每年委托第三方进行代码安全审计，确保中危及以上风险漏洞已消除或修复；（viii）根据SHEIN要求，向SHEIN提供相关评估、测试或审计结果。

7 应急计划与灾难恢复

7.1 通用要求。供应商应制定应急计划，以应对可能损坏或破坏供应商系统或受保护数据的事件（如系统故障、火灾、破坏行为或自然灾害）。该等计划应包括每年进行测试并定期完善的数据备份和灾难恢复程序。

7.2 具体控制措施。供应商应：（i）按照既定计划对供应商系统进行数据备份，并具备远程（跨云）执行能力；以及（ii）对用于提供 API 服务的供应商系统，制定正式的业务连续性和灾难恢复计划，并保证每年进行测试和持续改进。

附件 3 – 独立部署软件要求

本附件 3—独立部署软件要求（“**附件 3**”）适用于供应商提供的软件解决方案拟部署于 SHEIN 运营的环境或 SHEIN 授权第三方代表 SHEIN 运营的环境，包括 SHEIN 管理的服务器、基础设施或其他控制环境，且该软件由 SHEIN 进行安装、配置和操作的场景。本附件不适用于供应商管理的软件即软件即服务（SaaS）平台和托管软件。本类别还包括由供应商交付、可由 SHEIN 配置并定制以满足特定运营和安全需求的可定制软件。

除非另有说明，如主协议与本附件 3 存在冲突，以本附件 3 关于软件安全的条款为准。

1. **安全软件开发**

1.1 通用要求。供应商应制定并保持相关政策和程序，以确保向 SHEIN 提供的所有软件在其软件开发生命周期（SDLC）期间的安全性和完整性。

1.2 具体控制措施。供应商应：（i）在软件开发生命周期的每个阶段（包括需求收集、设计、开发、测试、部署和维护）纳入安全要求，确保尽早发现和解决安全漏洞；（ii）在软件开发生命周期中进行严格的安全测试，包括静态应用安全测试（SAST）、动态应用安全测试（DAST）和漏洞评估；（iii）遵循行业公认的安全编码规范（例如 OWASP 或 SANS/CWE），并定期开展安全代码审查；（iv）确保软件所使用的所有第三方组件、库和框架均定期进行漏洞扫描、补丁更新及验证；以及（v）确保测试环境在逻辑上或物理上与生产环境隔离，测试数据须受控、受保护，并在部署前予以删除。

2 **安全评估与测试**

2.1 通用要求。供应商应定期对软件进行安全性评估、测试和审计，以识别和消除安全漏洞。上述评估应覆盖系统与数据的全生命周期。

2.2 具体控制措施。供应商应：（i）定期对软件进行漏洞评估，并使用行业标准（例如 CVSS）对发现的问题进行分类；（ii）根据漏洞严重程度进行修复：严重漏洞（Critical）在七（7）天内，高危漏洞（High）在十四（14）天内，中危漏洞（Medium）在三十（30）天内，其他所有漏洞在六十（60）天内修复；（iii）具备及时应对零日漏洞的能力；（iv）每年由可信赖的第三方进行渗透测试，测试报告需确认中危、高危和严重等级漏洞已分别在三十（30）、十四（14）和七（7）天内解决；（v）每年进行第三方代码安全审计，确保中等或以上风险等级的漏洞不存在或已被修复；以及（vi）根据要求，向 SHEIN 提供任何相关评估、测试或审计的结果。

3 **变更与配置管理**

3.1 通用要求。供应商应制定并维护变更与配置管理政策和程序，以确保系统的完整性、安全性和可靠性。供应商应及时将所有重大变更告知 SHEIN。

3.2 具体控制措施。供应商应：（i）建立在生产环境部署之前记录、测试及审批变更的流程；（ii）实施版本控制系统以跟踪配置变更并保留详细变更记录；（iii）定期审查与验证配置，确保其符合安全和监管标准的要求；（iv）实施回退流程，以便在变更导致系统不稳定时将系统恢复至稳定状态。

4 **软件更新**

4.1 通用要求。供应商应实施健全的补丁管理流程，以识别和解决软件漏洞。

4.2 **具体控制措施。**供应商应维护安全补丁管理流程，要求在二十四（24）小时内对软件应用关键补丁，其他补丁则应及时应用。

5 第三方管理

5.1 **通用要求。**供应商应建立、实施及执行针对参与软件开发的第三方供应商（包括四方开发者）的安全政策和程序，以确保软件的安全性、质量和合规性。

5.2 **具体控制措施。**供应商应：（i）对第三方服务提供商进行安全尽职调查，包括安全状况审查与风险评估；（ii）对分包商进行安全评估，并确保其实施的安全控制措施不低于供应商自身的标准；（iii）实施安全交接或退出流程，要求所有源代码、文档和敏感数据在终止合作时予以返还或安全销毁，并撤销所有访问权限。

6 **资产保密性。**供应商应确保交付给 SHEIN 的所有资产，包括但不限于应用源代码、已编译安装包/镜像及特定运行环境配置文件，不得在任何公开可访问的渠道（如公共容器仓库、公共代码托管平台、公开论坛等）上发布或存储。供应商有义务采取有效措施防止此类资产被未经授权公开披露，并应配合 SHEIN 开展必要的审计，以验证合规性。

附件 4 – 部署于 SHEIN 管理的服务器机房的仓库自动化软件要求

本附件 4—部署于 SHEIN 管理的服务器机房的仓库自动化软件要求（“**附件 4**”）适用于供应商在 SHEIN 控制的物理环境（如服务器机房或托管中心）内进行仓库自动化软件或系统的安装、管理或运营以实现本地化部署的场景。“仓库自动化”是指利用先进的技术、系统和设备，对仓库的运营和管理任务进行自动化处理，包括但不限于货物的存储、搬运、分拣和库存跟踪，以及相关的数据处理活动。仓库自动化旨在减少人工干预，提高运营效率与管理水平。此类别包括由供应商管理但物理上托管于 SHEIN 内部服务器机房的软件解决方案。SHEIN 通常通过网页浏览器或者专有界面访问这些解决方案，这些方案通常涉及数据的存储、处理和传输。

除非另有规定，如主协议与本附件 4 存在冲突，则在本地部署安全方面以本附件 4 的条款为准。

1. 安全软件开发

1.1 通用要求。供应商应制定并保持相关政策和程序，以确保向 SHEIN 提供的所有软件在其软件开发生命周期（SDLC）期间的安全性和完整性。

1.2 具体控制措施。供应商应：（i）在 SDLC 的每一个阶段融入安全性要求；（ii）进行静态（SAST）和动态（DAST）安全测试及漏洞评估；（iii）遵循业界公认的安全编码规范（如 OWASP、SANS/CWE）并开展安全代码审查；（iv）定期对第三方组件进行漏洞扫描和修补；且（v）将测试环境与生产环境分离，确保测试数据在部署前被有效控制及清除。

2 安全评估与测试

2.1 一般要求。供应商应定期开展评估，识别并修复系统和数据生命周期中存在的漏洞。

2.2 具体控制措施。供应商应：（i）定期进行漏洞评估，并采用业界标准（如 CVSS）对发现的问题进行分类；（ii）根据严重性修复漏洞：关键级别在七（7）天内，高危级别在十四（14）天内，中危级别在三十（30）天内，其他所有级别在六十（60）天内完成修复；（iii）始终保持应对零日漏洞的响应准备；（iv）每年委托可信第三方进行渗透测试，并分别在三十（30）、十四（14）和七（7）天内确认中危、高危及关键问题的整改；（v）每年进行一次第三方代码审计，并确认所有中等风险及以上漏洞已修复或不存在。

3 变更与配置管理

3.1 一般要求。供应商应维护安全的变更与配置管理政策及流程，并及时将重大变更通知 SHEIN。

3.2 具体管控措施。供应商应：(i) 在生产部署前对变更进行记录、测试并批准；(ii) 实施版本控制并维护变更记录；(iii) 审查配置以符合政策和法规要求；(iv) 维护回滚操作程序。

4 软件更新

4.1 补丁管理。供应商应维护健全的补丁管理程序，对于关键补丁应在二十四（24）小时内应用，其他补丁按照行业惯例及时应用。

5 第三方管理

5.1 总体要求。供应商应制定政策以管理涉及软件开发或部署流程中分包商或其他第三方相关的风险。

5.2 **具体管控措施。**供应商应：(i) 对分包商进行安全尽职调查，包括安全状态和风险评估；(ii) 确保分包商具备不低于自身的等同或更高等级的安全防护措施；(iii) 在合同终止时实施安全的过渡程序，包括数据的安全返还或销毁与访问权限的撤销。

6 **IT 管理。**供应商应维护 IT 管理标准和运维手册。专职 IT 人员应负责日常运营、维护、监控和应急响应。

7 **网络安全。**供应商应对网络连接实施严格的访问控制，限制暴露于不安全或未经授权的进程。

8 **现场办公终端环境。**供应商应确保所有现场终端设备已安装 SHEIN 认可的软件，并符合 SHEIN 的标准化要求。

9 **服务器安全。**供应商应：(i) 为每台服务器分配唯一用户账户；(ii) 确保服务器账户设置的密码符合行业公认的强度和复杂度最佳实践；(iii) 实现连续五次（不包括第五次）认证失败后的账户锁定；(iv) 维护账户全生命周期管理；(v) 确保升级与运维流程规范；(vi) 配置主备热切换能力；(vii) 确保所有生产服务器上不存在任何高危或中危漏洞。

10 **资产管理。**供应商应：(i) 禁止现场人员未经 SHEIN 事先书面授权使用可移动介质传输数据；(ii) 实施介质驱动器安装与使用的授权机制。

11 **人员安全。**供应商应：(i) 为涉及本地运营的员工建立标准化入职/离职流程，并符合 SHEIN 的相关政策；(ii) 及时将员工入职/离职信息通知 SHEIN；(iii) 对违反数据安全政策的行为实施相应的纪律处分程序。

12 **应急预案。**供应商应定期制定并测试应急响应预案，以支持业务连续性并确保在发生事件时及时恢复生产。

13 **数据库安全。**供应商应禁止数据库账户使用默认或弱密码，并按照数据库访问控制及加密的安全最佳实践执行管理措施。

附件 5 – 第三方仓库要求

本附件 5—第三方仓库要求（“**附件 5**”）适用于供应商代表 SHEIN 提供仓储服务的情形，包括但不限于库存存储、订单履行、退货处理或其他相关物流职能。受本附件 5 约束的供应商，可能运营支持 SHEIN 运营的第三方仓库设施、网络和人员。本附件规定了供应商应实施和维护的适用技术、物理及组织安全措施。

除非另有说明，如主协议与本附件 5 存在冲突，就仓储服务的安全要求而言，应以本附件 5 的条款为准。

1. **业务连续性与灾难恢复**

1.1 通用要求。供应商应保持全面的业务连续性及灾难恢复能力，以确保运营韧性及对 SHEIN 持续提供仓储服务。

1.2 **具体控制措施。**供应商应：（i）制定并维护涵盖物理设施相关中断的书面业务连续性计划（BCP）及灾难恢复计划（DRP）；（ii）至少每年对 BCP 及 DRP 进行审查和测试；（iii）实施应急措施以支持服务的持续交付，包括必要时的替代人员、基础设施或物流服务提供商。

2 **人员管理。**若供应商在支持 SHEIN 仓库的运营中提供人力或劳务服务，供应商应：（i）确保人员不得在仓库内私自安装或操作路由器、无线网络、热点或类似基础设施；（ii）确保所有指派人员遵守 SHEIN 的政策、指南及安全协议。

3 **物理与环境安全。**若供应商为 SHEIN 的运营需求提供仓库设施，供应商应：（i）实施环境控制措施，保护仓库内标准化 IT 环境，包括空调系统（HVAC）、湿度传感器、消防抑制系统和不间断电源（UPS）；（ii）实施物理安全控制，包括具备高清、高动态范围和夜视能力的全方位周界及内部监控系统，并安全保管所有录像资料；（iii）实施安全的访客管理程序，如访客登记、陪同、访问日志、身份验证及定期审计。

4 **网络与 IT 基础设施。**若供应商在支持 SHEIN 运营的仓库内提供网络基础设施及连接服务，供应商应：（i）在互联网网关处部署并维护防火墙，制定明确的防火墙管理策略，规定五个关键要素（源地址、目的地址、服务或端口、动作、日志），严禁使用“any，any，any”规则；（ii）确保网络适当分段，有线和无线部署均支持强信号覆盖及快速漫游功能；（iii）通过至少两条冗余线路维持持续的互联网连接；（iv）实施入侵防御系统（IPS）与入侵检测系统（IDS），涵盖 IP 信誉管理；（v）响应安全警报并协助解决，以维护连接和运营；（vi）协调为 SHEIN 分配可路由静态 IP 地址；（vii）实施 802.1x 及 MAC 地址过滤等访问控制；（viii）定期对网络设备进行安全评估，包括交换机配置及接入点检查；（ix）对仓库终端设备定期审查并禁用未授权的互联网功能。

5 **资产管理**

5.1 **总体要求。**供应商应实施资产管理措施，以确保所有仓库及 IT 资产的完整性、可追溯性和安全处理。

5.2 **具体控制措施。**供应商应：(i) 对所有仓库及 IT 设备实施全生命周期资产追踪管理；(ii) 确保能够对遗失或被盗设备远程擦除敏感数据；(iii) 要求对所有可移动介质进行加密、访问控制及授权管理；(iv) 以安全方式停用资产，确保在处置或再次使用前完成数据彻底擦除或物理销毁。