

# Simplamo Security White Paper

## Table of Contents

1. Security Team and Its Functions.....	3
2. Personnel Security.....	4
2.1 Human Resource Management Process.....	4
2.2 Security Training and Learning.....	4
3. Client-side Security.....	5
3.1 Client-side Operating Environment Security.....	5
3.2 Client-side Data Security.....	5
3.3 Client-side Protection against Security Vulnerability.....	5
3.4 Product Security Capabilities.....	5
4. Network Security.....	6
4.1 Network Access Control.....	6
3.2 Network Firewall.....	6
4.3 DDoS and Network Attack Defence.....	6
4.4 Network Transmission Encryption.....	6
5. Server Security.....	7
5.1 Server Access Control.....	7
5.2 Vulnerability Scanning.....	7
5.3 Intrusion Detection.....	7
5.4 Anomaly Detection.....	7
6. Application Security.....	8
6.1 Security Development Process.....	8
6.2 User Account Security.....	8
6.3 Vulnerability and Security Incident Management.....	8
7. Data Security.....	10
7.1 Data Transmission.....	10
7.2 Data Storage.....	10
7.3 Data Access.....	10
7.4 Disposal of Data.....	11
7.5 Data Security Inspection.....	11
8. Physical Infrastructure Security.....	12
9. Disaster Recovery and Business Continuity.....	13
9.1 Backup and Disaster Recovery.....	13
9.2 Business Continuity Guarantee.....	13
9.3 Emergency drills.....	13
10. Change Control.....	14
10.1 Program Changes.....	14
10.2 Source Code Control.....	14
10.3 Infrastructure Changes.....	14
10.4 Change Monitoring.....	14

## 1. Security Team and Its Functions

As a SaaS service provider, Simplamo has always taken the security of users' business and data as its top priority. With complete infrastructure security and business and data security protection system for users, Simplamo can provide users with all-dimensional protection from the physical to the application and data.

Simplamo's security team consists of full-time security management, compliance, business security, data security, emergency response, security tool development teams and other teams. Its responsibilities include security assessment for product design, code security review, vulnerability scanning, penetration testing, threat intelligence, intrusion detection, emergency response, data security, security compliance, and more

## 2. Personnel Security

### 2.1 Human Resource Management Process

Simplamo has established a secure HR management process:

- The recruitment of new employees must be approved by the human resources specialist and the head of the job requirement department, and the recruitment process and outcome for new employees will be documented in the human resource system;
- Before employing a new employee, the Human Resources Department will conduct a background check on the employee according to the importance of the position and as permitted by national laws and regulations, to ensure that the employment of the employee complies with Simplamo's rules and regulations;
- New employees are required to sign the employment contracts and confidentiality agreements, which describe the responsibilities and obligations employees should undertake in terms of information security;
- The Legal Department shall review the terms enclosed in the employees' confidentiality agreements and third-party confidentiality agreements at least once a year, update them when necessary, and publish them through the internal knowledge platform after their being updated to ensure that all employees and relevant personnel can have access to the latest confidentiality agreements;
- The employee's resignation is required to be initiated in the human resource system by the employee himself/herself or the department head, and the official resignation can only be made after the application is reviewed by the human resource department and relevant functional departments. Before resignation, all accounts shall be cancelled and all hardware and software assets (such as computers, work documents, etc.) shall be returned.

### 2.2 Security Training and Learning

Simplamo has established a comprehensive training and learning system. New employees shall participate in training programs including corporate culture, rules and regulations, information security, and reward and punishment mechanisms. At the same time, Simplamo will organize training programs regarding employees' professional knowledge and skills and information security awareness aperiodically:

- Simplamo will organize information security-related training programs aperiodically to enhance employees' information security skills, at least once a year;
- Simplamo will hold information security activities aperiodically to publicize information security awareness, at least once a year;
- Simplamo will communicate security awareness to employees in multiple ways aperiodically, such as making publicity materials for security awareness and conveying them to employees through the mail, posters, etc.

## 3. Client-side Security

### 3.1 Client-side Operating Environment Security

Simplamo APP will stringently test the operating environment, including root detection, jailbreak detection, debugging detection, injection detection, etc. The purpose of such detections is to ensure that the client-side terminal runs in a trusted environment to prevent the programs from being cracked or exploited by malware.

### 3.2 Client-side Data Security

Simplamo APP adopts the security mechanism embedded in the operating system to isolate permissions between APPs. Local information on the client-side is encrypted for storage. The full-link communications between the client-side and the server are encrypted using HTTPS or WSS. Simplamo has integrated self-developed data security solution on the client-side, providing system-level capabilities for encrypting the client-side's local private data and the unique binding function between data and devices. Even if an attacker steals the user's encrypted data, he cannot decrypt such data to use them in his own devices. As a result, the user's data security boundary has been enhanced significantly, and the chance of user data leakage has been greatly reduced.

### 3.3 Client-side Protection against Security Vulnerability

Simplamo has a full-time mobile security vulnerability mining team, which conducts security assessments and vulnerability mining on Android, iOS, Windows, MacOS, Linux and other client sides, and at the same time conducts vulnerability detection on the third-party components (library, SDK) used, so as to locate the loopholes in the applications to ensure the security of the client side.

### 3.4 Product Security Capabilities

Simplamo provides security capabilities in account security, user permissions, data security and other aspects, including but not limited to: Account security: login method management, login password management, etc. User permissions: communication and collaboration permissions, external communication permissions, file operation permissions, etc.

Information protection: secure label, watermark setting, key word filtering, etc. Mailbox security: anti-phishing, anti-spam, black-and-white lists, and data protection rules. Simplamo's product security capabilities are updated rapidly. For the latest features, you can refer to the official website introduction or contact customer service for consultation.

## 4. Network Security

### 4.1 Network Access Control

Simplamo uses access control lists (ACLs) for network isolation. Different network areas such as guest network, office network, development test network, and production network are divided internally. All employees who are outside Simplamo's network borders need to access Simplamo's internal resources through a VPN connection. Simplamo's internal audit department will audit access logs, etc., find and trace illegal operation records, and impose corresponding penalties. Simplamo has strict employee access control policies in place to limit access to internal resources. Employees need identity-authentication to access internal resources. After the identity is confirmed, employees only have the least privilege by default. The acquisition of new permissions needs to be approved and recorded by the relevant responsible personnel. Permissions have a validity period, and the system will automatically revoke the permissions after the validity period expires. Employees operate online services through the bastion host, and all operation logs are kept for at least 180 days and audited by the internal audit department.

### 3.2 Network Firewall

Simplamo uses a network firewall to intercept common network security vulnerability attacks in the Simplamo suite system, and only authorized security and compliance engineers can uniformly configure the protection rules of the network firewall. Simplamo has set up a combination of automatic and manual methods to update the network firewall configuration.

### 4.3 DDoS and Network Attack Defence

Simplamo service provides customers with network access through CDN and dynamic acceleration, and accesses back-end services through company load balancing; Simplamo has deployed industry-leading anti-DDoS services, which can effectively target traffic-type and connection-type attacks, etc. to defence.

### 4.4 Network Transmission Encryption

Simplamo uses HTTPS and WSS for encrypted transmission in both the internal and external networks, ensuring the security of the transmission process and prevents eavesdropping and tampering.

## 5. Server Security

Simplamo has adopted a series of security control measures for the servers used to ensure the safety of server production and effectively prevent malicious network attacks.

### 5.1 Server Access Control

Simplamo regularly scans server assets, closes unnecessary ports and services in a timely manner, minimizes external permissions, filters unsafe services, and reduces security risks. Security personnel conduct weak password detection on a regular basis, and urge server operation and maintenance personnel to increase the complexity of passwords to prevent brute force cracking. All access to the server must be operated and audited through the bastion host. Simplamo uses the whitelist to control the access source of business services to ensure that only trusted sources can access the service.

### 5.2 Vulnerability Scanning

Simplamo uses automated vulnerability scanning tools to regularly detect server vulnerabilities. After the confirmation by security personnel, it will be notified to relevant personnel for processing and repair. The operation and maintenance personnel will regularly update the system patches to effectively ensure the stable operation of the server.

### 5.3 Intrusion Detection

Simplamo's physical servers are fully deployed with HIDS (Host-based Intrusion Detection System), which can monitor server file baseline changes in real time, discover abnormal processes, capture active abnormal external links, horse backdoors and other abnormal behaviours, and respond in a timely manner. In addition, all traffic from the client end is detected and verified by WAF (Web Application Firewall) to ensure its security and legality, and to block malicious requests in real time. The security team will closely track the security situation and the latest attack methods, study intrusion characteristics, and regularly upgrade defence strategies.

### 5.4 Anomaly Detection

Built on the big data platform and machine learning platform, the security team conducts multi-dimensional security analysis on the massive host logs generated by the server and the data collected by the self-developed HIDS, establishes an anomaly detection model, and timely discovers risky operations and abnormal processes on the server, malicious network connections and other abnormal behaviours, and responds in a timely manner. The security team will closely track the security situation and the latest attack methods, continuously iterate the security algorithm model, update the abnormal behaviour characteristics, and regularly upgrade the defence strategy.

## 6. Application Security

### 6.1 Security Development Process

Simplamo strives to control security risks from the source of security vulnerabilities. By making security courses and providing training in the form of on-site and online classrooms, all developers and product managers must receive security training to understand the causes of relevant security vulnerabilities and strengthen coding knowledge. When the project starts, the security team communicates with the project manager to ensure that security requirements and security tests are reflected in the project plan. At the same time, the security team will evaluate the third-party libraries and tools used by the product, and discover vulnerabilities to ensure that there are no vulnerabilities introduced by the supply chain. The security team conducts design and code security reviews with the product team. Before the product goes online, a penetration test and a security assessment of deployment will be conducted to ensure the security of the service.

### 6.2 User Account Security

The user's access to the Simplamo system is authenticated through a password. For logins initiated on unidentified devices, the risk control strategy will increase the difficulty of login verification. At the same time, the accounting system has defence capabilities against abnormal and violent login attempts.

Simplamo is connected to the self-developed risk control and anti-cheating system, which has protection functions such as anti-malicious registration, anti-crash database, and anti-violent login cracking. Users use password to log in.

### 6.3 Vulnerability and Security Incident Management

Simplamo monitors internal and external security vulnerabilities and threat intelligence information through various means. The security team uses automated security scanning tools to scan its own services and operating systems, and conducts security checks on application systems through regular penetration tests. After the vulnerability and threat intelligence information is confirmed, the risk level will be determined according to the hazard situation, and it will be pushed to the relevant team for repair and processing as soon as possible. Simplamo has a complete vulnerability lifecycle management strategy, and a professional security team follows up on all security problem solving.

At the same time, Simplamo's security team maintains close cooperation and communication with the industry's top third-party evaluation companies and White Hat Communities. It will occasionally invite external companies and white hats to conduct penetration tests on the service and reward them to find out as many security holes as possible.

Simplamo has a complete incident management process and implements a 24/7 emergency response strategy. When a security incident occurs, the security team will quickly classify the incident according to the security emergency plan and start the emergency response process to prevent the security incident from expanding. After the security incident is 15 processed, the incident will be reviewed. The content of the review includes the cause of the incident, the process and results of the incident handling, the main person in charge of the





incident, and follow-up measures, etc., and record the results of the review and follow-up measures to ensure a closed loop of events. When a security incident affects users or customers, we will promptly notify users, customers or other relevant parties in accordance with the incident handling process.

## 7. Data Security

Simplamo has a complete life cycle management of data, and has a clear process and technical guarantees from the creation, storage, transmission, use, and destruction of data. Simplamo has corresponding control measures to ensure data transmission, data storage, and data access and the security of the data destruction process.

### 7.1 Data Transmission

Simplamo provides users with data transmission links that support strong encryption protocols. Data transmissions such as message pulls, identity verification, and operation instructions are all encrypted using HTTPS and using 2048-bit RSA keys; the transmitted data is encrypted and protected.

### 7.2 Data Storage

Simplamo uses a secure key mechanism to encrypt and store data, and has encrypted and stored all customer data such as messages and documents.

Simplamo has developed a comprehensive data classification and classification management method, and has implemented strict classification and classification management of user information collected by Simplamo and tenant information in the background management system, encrypted all sensitive information stored in the system, effectively protecting users' information security.

The encryption algorithm is embedded in the source code of each application; the key is generated by the key management system (referred to as "KMS system") and called by each application. The KMS service is responsible for the lifecycle management of keys and sensitive configuration information, including creation, storage, distribution, use, update, deletion, etc. The master key used for data encryption of tenants and various other sensitive information of Simplamo services (such as database accounts, passwords, etc.) are stored in the KMS system maintained by Simplamo, and access must be performed through KMS access. The root key of the KMS system is maintained by a hardware security module (HSM). The management of the HSM requires the cooperation of multiple keys. These keys are distributed to different functional roles for management. The KMS system uses envelope encryption to encrypt and decrypt data. The master keys used by different tenants are isolated from each other.

In addition to using the standard tenant master key and the AES-256 algorithm to encrypt data and data keys, Simplamo supports customer-independent keys, that is, KMS generates data keys, and uses customer-defined master keys for data and data keys. The key and the specified encryption algorithm are encrypted and stored in the database. Customers can choose the encryption algorithm and control the key rotation independently.

### 7.3 Data Access

Access to user data is strictly isolated with permissions. Users cannot access each other without authorization. Access to data must be explicitly authorized by the data owner, such as sharing operations, etc. (for example, the document created by user A is only visible to user A by default, unless he actively grants access to others).

By default, employees of Simplamo do not have access to any user data, and all operations of employees are strictly restricted and audited. At the same time, real-time audits of illegal access and risky operations are performed through automatic detection, and alerts are generated.

## 7.4 Disposal of Data

Individual accounts can request to delete personal information. After receiving the application for account cancellation or personal information deletion, Simplamo will delete or anonymize the relevant data of the cancelled account.

The resigned employees of the user organization can submit an account cancellation application to the tenant administrator. After the user organization confirms that the group owner, schedule, documents and other data in the resigned employee's account have been transferred, the tenant administrator contacts Simplamo through Simplamo's customer service function. Simplamo deletes or anonymizes the data related to the account that needs to be cancelled according to the application of the tenant administrator of the user organization.

When Simplamo signed a cooperation agreement with the user organization, it agreed with the user organization that when the cooperation is terminated, Simplamo will process account-related data in accordance with laws and regulations, including but not limited to deletion and anonymization.

All data deletion and anonymization technical means comply with the prevailing industry standards and the requirements of laws and regulations.

## 7.5 Data Security Inspection

The login behaviour, operation behaviour, server security baseline file changes, access rights changes, and data access behaviours of all servers in Simplamo's online environment will be recorded. By establishing user behaviour portraits and abnormal behaviour models, the security team realizes the identification, analysis and correlation of abnormal behaviours, and automatically detects various abnormal data access behaviours in real time, such as illegal access to data, malicious data crawling and risky operations, log in abnormalities, privilege escalation, etc., and issues alarms or block them.

## 8. Physical Infrastructure Security

Simplamo uses AWS cloud services, and AWS is responsible for operating, managing and controlling its hardware and software facilities. As the world's leading cloud service provider, AWS has the industry's top security capabilities to protect users' infrastructure security. See [https://d0.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Whitepaper.pdf](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) for more information on cloud service infrastructure protection provided by AWS.

## 9. Disaster Recovery and Business Continuity

### 9.1 Backup and Disaster Recovery

Simplamo has formulated relevant regulations to standardize database backup strategies, backup data storage, and backup recovery testing. The business databases have regular snapshots and backups, and the data is stored in two places and three backups. At the same time, Simplamo has deployed a backup execution monitoring mechanism to ensure the integrity of data backups, and regularly conducts backup data recovery tests.

Full data backup is performed once a day. Simplamo has deployed a backup execution monitoring mechanism. If the database backup task fails, an alarm will be automatically sent to the database administrator through the Simplamo push function, and the database administrator will check the cause of the failure and handle it.

Simplamo extracts backup data every day for recovery testing. The R&D personnel put forward the demand for backup data recovery through the database operation and maintenance platform. After being reviewed by the person in charge of R&D, the database administrator will restore the data, and the R&D personnel will verify whether the backup data is available.

### 9.2 Business Continuity Guarantee

The access layer of the business system is accessed in a high-availability manner through the public gateway service provided by the basic service provider. The backend adopts multi-instance access to ensure service reliability. Carry out meticulous monitoring of traffic and faults, and adopt degraded operation mode to ensure business availability when traffic bursts or faults occur.

Simplamo has the emergency response and recovery measures in place for scenarios that could result in business disruption. Perform business impact analysis and risk assessment once a year to identify important business processes and threats that may disrupt Simplamo's business and resources; define indicators such as maximum tolerable interruption time, recovery time objectives, and minimum service levels; formulate responses to different business interruption scenarios strategy.

### 9.3 Emergency drills

Simplamo has a complete emergency drill mechanism, and regularly conducts failure drills. Participants include business teams, security teams, and operation and maintenance teams. Conduct disaster recovery drills at least once a year for situations that may cause business interruptions to ensure data availability.

## 10. Change Control

### 10.1 Program Changes

Simplamo has formulated comprehensive program change management regulations, and clarified the change management requirements and process, including changing plan formulation, changing approval, and changing the implementation. Operations that have known or potential impacts on the stability, availability, and security of online services fall within the scope of online changes. Simplamo product development strictly controls the change operation to prevent the change operation from affecting the stability of the service. Online operations must have an operation sheet, which can only be carried out after approval. Simplamo has deployed independent development, testing, and production environments for each product-related application. The change operation follows the grayscale release and goes online. A small traffic test is required before the official release, so as to ensure the stability and security of the service.

### 10.2 Source Code Control

Simplamo has established a strict source code management process, and research personnel can only access and manage the code warehouse corresponding to their team. Each project code warehouse in the code warehouse has a person in charge of the code warehouse. If the R&D personnel need to apply for access to the code warehouse other than their team, they must submit the application in the code warehouse, and after the approval of the department head and the person in charge of the applied code warehouse, the corresponding permissions can be added.

### 10.3 Infrastructure Changes

Simplamo deploys an access control list at the border of the public network to control network access. If it is necessary to change the ACL configuration baseline and network access control list, the operation and maintenance personnel submit an application through the platform, and professional engineers will perform the operation after judging the rationality of the change. Only authorized engineers have the authority to perform changes to the network access configuration.

### 10.4 Change Monitoring

Simplamo conducts internal audits every year to check the operation of Simplamo's internal control system, which covers the implementation effectiveness of control related to change management, and summarizes the results in the internal audit report. If abnormalities are found, the internal audit department and the relevant responsible team will communicate and follow up on the rectification results. Incompatible segregation of duties exists in the change management process, including change development, testing, approval, release, and monitoring.

Simplamo is committed to creating a rich and diverse, safe and reliable application ecosystem platform to provide customers with a more diverse SaaS service experience and meet the individual needs of different companies. In this model, the Simplamo platform, application developers, customers and users form a multi-party responsibility system. Simplamo protects the security of applications, the health of the ecosystem, and the privacy



of users from the aspects of service provider registration, application development review, permission classification and approval, and regular security inspections.