TAIMEI TECHNOLOGY WHITE PAPER ON INFORMATION SECURITY

Version No.: 1.0

Date: Jun. 6, 2024

TABLE OF CONTENTS

I. DECLARATION

Company Introduction

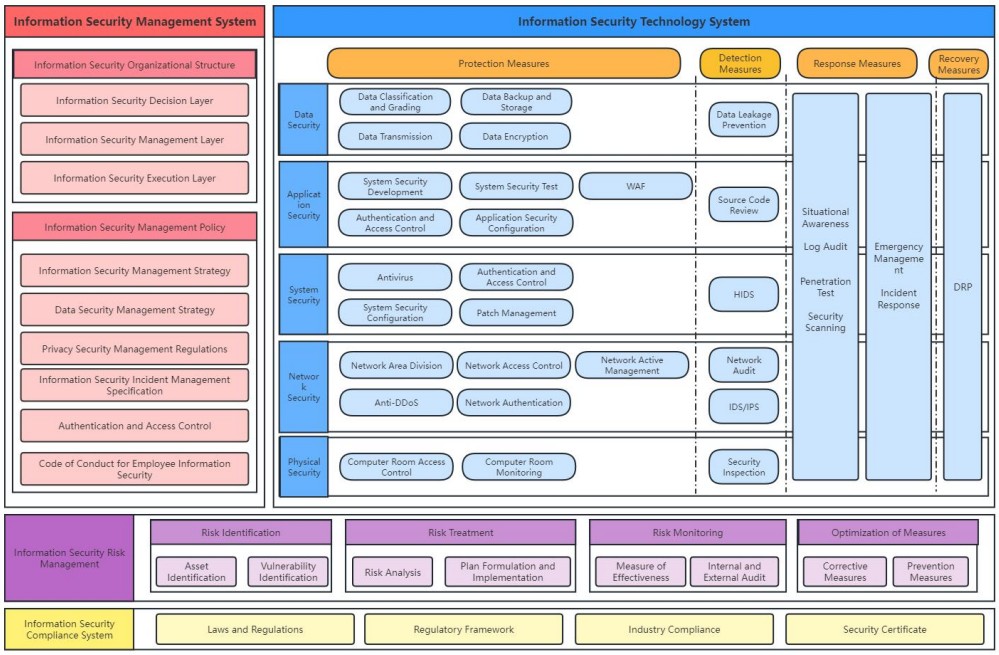
The mission of Taimei Technology is "Accelerating the Accessibility of Innovative Drugs". As a digital intelligence platform for the life science industry, Taimei Technology's business covers pharmaceutical R&D, pharmacovigilance, pharmaceutical marketing, and other fields. With collaboration as the core principle, our company leverages AI to innovatively develop the intelligent clinical study collaboration platform "Trials" and the medical-enterprise interactive academic exchange platform "Wujie". These platforms integrate a full suite of applications, connecting pharmaceutical companies, hospitals, third-party service providers (CROs, SMOs, etc.), regulatory agencies, and patients. By harnessing advanced technologies such as artificial intelligence, big data, and cloud computing, we have established standardized and data-driven processes that enhance workflow collaboration and resource integration. This facilitates the digital transformation of the industry, significantly boosting overall efficiency in pharmaceutical R&D and post-market commercial performance, thus achieving value upgrades and mutual benefits for all stakeholders.

Security Goals

Thank you for your trust and support. With Taimei Technology products, we will provide complete and sustainable guarantees to ensure the compliant, secure, and stable operation of our business system. The overall goals of information security of Taimei Technology are to continuously ensure the secure and stable operation of the business system within the controllable range and to continuously ensure that the business system meets the requirements of relevant laws and regulations, which are also the directions of our continuous efforts and continuous security operation.

Security System

Our security design philosophy is a multifaceted and integrated approach, drawing from ISO27001 standards, GDPR and HIPAA regulations, SOC2 practices, NIST frameworks, and OWASP vulnerabilities. It also incorporates the company's current situation to ultimately establish the optimal security system tailored to our present needs. The security system is not static. We will make dynamic adjustments to adapt to the ever-changing internal and external conditions. However, it is certain that we always believe a comprehensive security system must encompass both "management" and "technology". The following is our overall security design framework:



In terms of management, we have established a comprehensive security organizational structure and management policy. These involve multi-dimensional standard operating procedures (SOPs), covering security strategy, system security, physical and environmental security, network security, data security, application security, access control, incident management, disaster recovery, business continuity drill, etc., which are strictly implemented to ensure security and compliance throughout our production and operation processes.

In terms of technology, we leverage AWS's excellent security product and service capabilities, combined with management strategies, to implement security measures at every stage - before, during, and after any event - to ensure that the information system remains protected from both internal and external threats.

In the following text, we will focus on a comprehensive introduction to both aspects.

Shared Responsibility

For both parties or multiple parties in a partnership, we believe that the security responsibility does not rest solely on one party. The joint efforts of all parties involved are required to maintain the respective modules' security needs and ensure overall security and control. Given the different roles, we believe a distinction can be made between the "system user" and the "system provider". The system user is the customer (you) of Taimei Technology, who is responsible for using a specific information system and managing the corresponding use of the system; the system provider is Taimei Technology, who is responsible for providing the system and ensuring the underlying stability and security of the system.

The system user is responsible for account management (authorization and recovery, sharing, login, password complexity, etc.) and backend configuration, as these are user-defined and independently managed, with corresponding security configuration functions provided by Taimei Technology.
The system provider is responsible for the underlying security of the information system, such as application security, host security, network security, etc.

Compliance

We attach great importance to compliance construction, so as to meet the compliance requirements of industry standards and regional regulations. We have obtained ISO27001, ISO27701, and ISO27018 certifications for security, and completed the self-assessment reports as required by GDPR and HIPAA.
In terms of GDPR self-assessment, we selected the "Gartner GDPR Compliance Audit Checklist" provided by Gartner. Among the 83 assessment items in total, approximately 70% were "compliant", and 30% were "not applicable", with no instances of "non-compliant".
In terms of HIPAA self-assessment, we referenced the security risk assessment method provided by HealthIT. Among the 59 assessment items in total, only 1 item was "not applicable", and all the rest met the requirements.
The self-assessment conclusions for these 2 important bills demonstrate our outstanding compliance capabilities in international compliance projects.
If needed, please inform your sales representative or directly contact our security team via the public email provided in "Security Team Contact Information" below. After confirming your information, we will send you the corresponding materials in a timely manner.

Privacy

We have formulated and issued the "Information Security Management Strategy", "Personal Information Protection Management Regulations", and "Sensitive Data Usage Guidelines", which comprehensively standardize the privacy information identification, privacy information processing, privacy information monitoring, privacy information security incidents, privacy information recovery, complaint channels, and maintenance of personal privacy policies. In general, none of our employees (such as business personnel, R&D personnel) have access to data, only database and server administrators have corresponding operation and maintenance management authorities. All relevant personnel have signed special confidentiality

agreements. In addition, in order to ensure that we can effectively respond to security incidents related to privacy data leakage, we have established the "Information Security Risk Assessment and Disposal Process" to standardize the response handling process and related reporting process that Taimei Technology employees must follow after an information leakage event.

Security Team Contact Information

Security team public email: security@taimei.com

II. SECURITY MANAGEMENT

Security Organization Construction

The organizational structure of Taimei Technology's information security management includes: the Information Security Management Committee, the Information Security Management Department, and all employees.

For the Information Security Management Committee, the CEO of Taimei Technology serves as the chairman, the management representative serves as the vice chairman, and the heads of various departments of Taimei Technology are the members. The Information Security Management Committee leads the company's information security macro-management and is responsible for formulating the company's information security development strategy and coordinating and ensuring the resources required for information security activities. The Information Security Management Department of Taimei Technology is responsible for the daily management of the company's information security tasks, the preparation and maintenance of information security systems, and the optimization and adjustment of the company's information security control measures according to the company's development. All employees of Taimei Technology must follow the information security management requirements, implement various information security tasks, and cooperate in daily security supervision and various inspections.

Security Management Systems

Based on the requirements of laws and regulations, ISO practices, SOC2 practices, etc., and in combination with the company's current operating scenarios, we have established and implemented relevant systems such as the information security management strategy, privacy security management regulations, data whole life cycle security management system, risk assessment and disposal process, and incident management specification. The Information Security Management Department of

Taimei Technology is responsible for preparing, revising, and maintaining the information security management systems, and promoting the implementation of the systems.

III. SECURITY TECHNOLOGY

Office Security

We believe that the key factor in security assurance is the management of "personnel". Therefore, we have implemented strict controls on office security and employee code of conduct to ensure that neither intentional nor unintentional internal actions compromise business security and customer rights.

We have installed an access control system at the office entrance, monitored by security personnel, to prevent unauthorized individuals from tailgating. Access control software, data anti-leakage software, anti-virus software, USB reading and writing control, etc., are deployed in employees' computers for overall protection, ensuring that unauthorized computers are not allowed to connect to the company's internal network and that all the devices connected to the company's internal network are controllable. Besides, to manage both internet boundary traffic and internal traffic, we have deployed a "situational awareness" system in our office environment. This system can analyze and provide early warnings for potential security risks such as attacks and leaks.

Authentication and Access Control

We strictly control the accounts and permissions of employees in accordance with the principle of "minimization". In terms of product, R&D, and operation, there is no authorized approach or way to access the production environment. In terms of operation and maintenance, permissions are allocated according to the principle of minimization. Relevant personnel are only allowed to access servers and databases through bastion hosts. Access and operation behaviors are controlled to ensure security while meeting the needs of basic work.

At the same time, we believe that only with the recovery and audit mechanisms in place can there be an effective closed loop for the permission management cycle. Taimei Technology's Information Security Center, in conjunction with each business department, carries out an annual review of the account permissions of existing application systems, internal supporting systems, and databases to confirm whether the existing account permissions match the job responsibilities of each employee and whether there is redundant authorization.

Risk Assessment

In our opinion, risk assessment is an important part of proactively discovering potential risks. Therefore, we specially formulated the "Information Security Risk Assessment and Disposal Process", which standardizes the risk assessment process and requirements that Taimei Technology must follow, including risk identification, risk grading, risk analysis, and response and disposal measures for risks beyond the acceptable level.

We carry out a risk assessment annually. Based on different risk scenarios and considerations of changes in the company's internal and external environment, we identify and evaluate the significance level of the risk exposure of the company's personnel, data, software, etc. Based on the assessment results, a risk assessment control matrix will be established and rectification measures will be developed, and the rectification follow-up will be completed through the risk assessment control matrix.

Vulnerability Management

By referring to the CVSS scoring mechanism, we classify vulnerabilities into 4 levels: critical, high-risk, medium-risk, and low-risk based on the system's importance, destructiveness, and availability, and specify the corresponding time limit for repair. Vulnerabilities identified during penetration testing or reported via dedicated channels will be followed up by submitting a work order. After preliminary analysis and grading, the submitted vulnerability repair work order will be transferred to the relevant R&D personnel for subsequent follow-up and repair. The personnel of the Information Security Center will then verify the vulnerability repair and issue a retest report, and close the work order after confirming that the vulnerability or failure has been successfully repaired.

Security Incident Management

We have formulated the "Information Security Incident Management Specification" to clarify the procedures for handling information security incidents. Taimei Technology conducts multi-channel real-time monitoring of information security incidents and sets up a reporting mechanism. The Information Security Department promptly responds to and handles reported incidents. We have also established a classification and grading system for information security incidents, which analyzes and grades incidents according to the nature of the incident, the degree of harm, and the scope of impact, and forwards the incidents to relevant responsible personnel for disposal and

traceability. During the incident handling process, based on the different scenarios and levels, we will provide necessary notifications to regulatory authorities and affected parties, and conduct a review and summary after the resolution.

Availability Management

Data backup management

By combining the advantages of various backup methods, we implement a strategy incorporating full backup, incremental backup, and transaction log backup according to the backup cycle.

A full backup is a complete backup of all data, performed once a day.

Incremental backup refers to backing up only the newly added and modified data relative to the most recent backup. It uses the previous full backup as a baseline, backing up data files, log files, and other modified content in the database after the full backup, performed once a day.

Transaction log backup involves backing up the database log records, capturing the changes in logs from the last backup to the current backup time, performed once every 5 minutes.

Amazon S3 offers a range of storage classes, with backup slices stored in S3, which spans across three availability zones, ensuring backup redundancy. Backup jobs are automatically executed through the cloud configuration.

Based on the established "Data Backup and Recovery Procedure", we have adopted a strategy of performing local full backup every week and local incremental backup every day for business data. To ensure security, backup files are protected by symmetric encryption to prevent data compromise. At the same time, in order to ensure the availability of the stored backup data, we have established a data recovery test mechanism. The Operations and Maintenance engineers will test and recover the backup files every month to test the data availability.

Business continuity

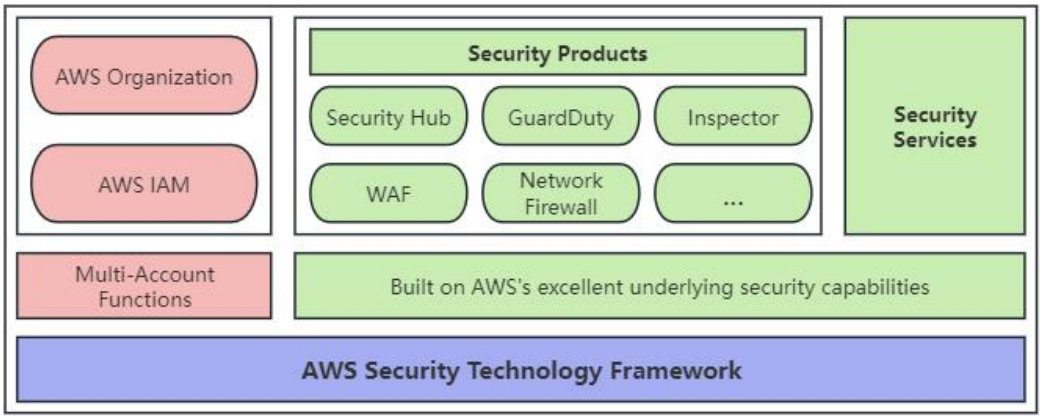
We have defined disaster recovery goals and business continuity plan processes in accordance with the established "Business Continuity Plan for Business Systems". We conduct a business impact analysis and risk assessment annually to evaluate indicators such as the maximum tolerable interruption duration, recovery time objective, and minimum service level for various potential threats and formulate response strategies accordingly. Based on the results of risk assessment, the Operations and Maintenance Department will organize relevant business departments to conduct business

continuity drills for different business scenarios every year. After the drills are completed, the personnel participating in the drills will review the issues found in the process and record the drill results in the "Business Continuity Drill Report".

Environmental Security

Based on security and compliance considerations, all of our virtual environments are deployed in AWS, namely AWS Singapore data center and AWS California data center.

For the establishment of cloud security, we mainly rely on the security product and service capabilities of AWS to carry out security activities. The following is the technology framework, which will be introduced in detail in the following sections.



Penetration and Scanning

We hold the opinion that penetration testing and vulnerability scanning are essential to ensuring system security. They enable us to proactively detect security vulnerabilities and repair them as soon as possible, which is most beneficial to our maintenance costs and customer protection. Therefore, we have been conducting and inviting third-party teams to conduct penetration testing and vulnerability scanning.

We choose the black box approach for penetration testing. A complete and effective penetration test must be conducted mainly with manual penetration and supplemented by tools. Manual participation can discover more logical vulnerabilities and unauthorized vulnerabilities, while tools can help humans conduct more detailed, extensive, and in-depth detection. This is our understanding of penetration testing.

S-SDLC

The National Institute of Standards and Technology (NIST) estimates that if a code fix is performed after release, the fix will cost 30 times more than that performed during the design stage. One thing that is certain is that taking action to avoid vulnerabilities

from the early stages of software development will greatly reduce the cost of fixing software vulnerabilities. Therefore, we developed the S-SDLC (Secure Software Development Lifecycle) based on the SDL ideas proposed by Microsoft and in combination with the company's current situation. We have integrated security factors into the entire process from before project initiation to after project operation, such as early employee training on security technology and security awareness, security risk assessment in the requirements and design stages, security coding specifications and security testing in the coding and testing stages, and security monitoring and vulnerability handling in the release and operation stages, forming an overall security closed loop.

Network Security

We always adhere to the principle of "minimization of authorization" to implement information security strategies, which is also the same at the network level. At the boundaries of the internet, we minimize control over incoming and outgoing traffic and services through firewalls. Any network access, except for ports/services essential to business operations, requires approval from the security department and is only permitted within controlled limits. Within the VPC, we divide different subnets according to different business attributes, and separate each subnet by security groups. Only when communication is required and after security assessment, the minimum access permission will be enabled.

Transmission and Storage Security

Data encryption technology is a technical means to re-code information to hide information content, making it impossible for illegal users to obtain real content. We attach great importance to the confidentiality and integrity of the data, and implement encryption control during data transmission, database storage, and file storage. Our system employs HTTPS encryption for all site-wide data transmissions, using TLS version 1.2 or higher without any insecure cipher suites. For data storage, we use AES256 encryption for sensitive personal information and apply complex hashing combinations to passwords, ensuring one-way encryption that is completely irreversible. For file storage, we use AWS S3 object storage service, employing encryption and access management tools to protect data from unauthorized access. It encrypts all objects uploaded to all storage buckets.

AWS Security

As described in Section "Environmental Security", we have deployed critical security products on AWS to address a variety of security needs. The following is an introduction to the security products that form our core operations.

WAF, short for Web Application Firewall, protects our web applications from common vulnerabilities, such as SQL injection attacks, cross-site request forgery, uploading vulnerabilities, and cross-site scripting attacks. It is widely recognized as an effective web defense solution.

Network Firewall enables us to create firewall rules to inspect inbound and outbound internet traffic, deploy outbound traffic filtering to prevent data loss, help meet compliance requirements, and block known malicious communications. It offers comprehensive management of all incoming and outgoing traffic of the internet across all protocol layers, providing sophisticated control over network traffic to meet compliance and security requirements.

Inspector, an automated vulnerability management tool, continuously scans for software vulnerabilities and dangerous network exposures in AWS such as EC2 instances and containers. It can detect common operating system vulnerabilities as well as burst 0-day vulnerabilities. Risk scores are available to prioritize vulnerability fixes and reduce the average time to remediation. Meanwhile, Inspector's scanning rules support compliance requirements and best practices, including NIST CSF and other regulations, ensuring not only the detection and remediation of vulnerabilities but also compliance adherence.

Security Hub automates security best practice checks and consolidates and displays security alerts, thus serving as an operation center for overseeing the overall security status on AWS.

GuardDuty combines machine learning with threat intelligence from AWS and third parties, helping protect our accounts, hosts, and data from threats. It offers robust and comprehensive threat detection analysis, such as identifying suspicious activities in S3 data access events, analyzing malicious activities and unauthorized behaviors during EC2 runtime, and examining for malware when suspicious operations are detected.

Monitoring and Emergency Response

Every day, our professional technical engineers monitor and analyze the security data generated, with rigorous alert strategies implemented. Depending on the category and level, we can receive timely alerts for various anomalies via SMS or email.

When a 0-day vulnerability or an APT attack is discovered, we conduct a thorough self-inspection using Inspector, custom scripts, manual checks, and log analysis. We take immediate action based on the severity and scope of the issue. After resolving the incident, we perform a comprehensive review and generate a self-inspection report, which is available for customers to obtain and verify as needed.

IV. CONCLUSION

At Taimei Technology, we firmly believe that security and compliance are the lifelines of our operations. We have obtained comprehensive certifications including ISO27001, ISO27701, ISO27018, ISO20000, and ISO9001. Additionally, to meet regulatory requirements, we have conducted gap analyses and continuous improvements to develop GDPR and HIPAA self-assessment reports. Adhering to the principle of "security and compliance are ongoing processes", we have been continuously improving the security system to ensure the secure, compliant, and stable operation of the information system.

*Disclaimer

This document describes Taimei Technology's methods and understanding of security in the process of information security construction. However, since security is dynamic, any security assessment in project cooperation should not be based solely on this. We recommend communicating with us through audits or questionnaires to obtain the most comprehensive security updates.