Meegle Security & Compliance Whitepaper v2.0 (EN)

As an enterprise-level SaaS service, Meegle prioritizes the security of customer data. This security statement provides a detailed description of Meegle information security control mechanisms, including internal security mechanisms, data security, and the organization of security plans at the network and server levels.

Compliance and Certification

Meegle places a high emphasis on compliance certification. Since its launch, as part of the Lark suite, it has participated in and obtained multiple national and international compliance certifications alongside Lark. These include the Ministry of Public Security's Network Security Level Protection Grade 3, ISO27001, ISO27018, ISO27701, ISO22301, ISO9001, ISO20000, Trusted Cloud, STAR Cloud Security Certification, CMMI (Capability Maturity Model Integration) Level 3, ITSS-Cloud Service Assessment (SaaS), etc. Additionally, it has completed SOC 1 Type II, SOC 2 Type II, and SOC 3 service attestation reports. This signifies our achievement of a more standardized and regulated level in aspects such as information security, privacy protection, business continuity, service quality, and IT services.

Data Security

Data Transmission

Meegle provides tenants with data transmission channels that support strong encryption protocols and has established various specifications for data transmission, including but not limited to:

- Data transmission is encrypted using HTTPS (with TLS version 1.2 and above) and 2048-bit RSA keys.
- Message push uses the WSS protocol to encrypt and protect transmitted data.
- Sensitive data such as phone numbers and user identity tokens are prohibited from being passed through URL GET parameters to prevent data leakage.
- The server is configured to enforce HTTPS 301 redirection on the CDN or TLB side.

- For highly sensitive information such as account passwords, parameters are encrypted during transmission.
- Parameters such as IDs that can be traversed in queries are encrypted or non-sequentially ordered to prevent bulk data scraping through ID traversal.
- When implementing cross-origin requests, CORS whitelist mechanisms and CSRF protection plugins are used to restrict the sources of cross-origin requests.

Data Storage

Meegle has a comprehensive classification and grading management system for data. It strictly classifies and grades user information collected by Meegle and tenant information in the backend management system, encrypting sensitive information to effectively safeguard user data security.

For structured data, all newly added fields are designed with their data grades specified from the outset to determine if encryption is necessary. If a field's grade is not specified, DDL cannot be executed to add the field.

For unstructured data, such as attachments in work items, they are treated as user content data and are encrypted by default.

Regarding encryption, Meegle utilizes Lark unified encryption and decryption capabilities. Keys are generated by the Key Management System (KMS) and are called upon by various applications. The KMS service manages the lifecycle of keys and sensitive configuration information, including creation, storage, distribution, usage, update, and deletion. The main keys for encrypting Lark user data and various other sensitive information (such as database accounts, passwords, etc.) are stored in the KMS system maintained by Lark, and access requires KMS access. The root key of the KMS system is maintained using a Hardware Security Module (HSM), which requires multiple keys to cooperate for management. These keys are distributed to different functional roles for management. The KMS system uses envelope encryption to encrypt and decrypt data. The main keys used by different tenants are isolated from each other.

Data Access

- Data Isolation between tenants
  - Meegle enforces strict permission isolation for user data access. Users cannot access each other's data without authorization. Access to data must be explicitly authorized by the data owner, such as through the “enterprise interconnection” feature or any other ways alike.

Sensitive Logs

Meegle also has clear specifications for logging. Printing sensitive content such as user-generated data is strictly prohibited. The logging plugin automatically identifies and anonymizes corresponding content (printed as *), preventing this data from mistakenly appearing in the logging system.

Data Destruction

When an employee's account is deactivated due to resignation or proactive actions by an administrator, their personal data will be deleted or anonymized to ensure that no identifiable personal information is explicitly retained.

Product Security Capabilities

Permission Control

Meegle provides powerful permission control capabilities, ensuring that data is not accessed beyond authorization, thus protecting enterprise data security and mitigating the risk of data leakage.

- Multi-dimensional control capabilities to meet various permission control scenarios in enterprises, such as tenant management, space management/access, viewing/creating/deleting work item instances, field management/viewing, node management/circulation, view management/viewing, etc.
- Data row permissions that support fine-grained permission control scenarios: Customized range rules based on the attributes of work item instances, ensuring that employees can only view specified ranges of work item instances and can only delete specified ranges of work item instances.
    - Robust preset permissions, such as automatic viewing permissions for creators of work item instances and node leaders.
    - Authorization can be granted directly to individual employees or to roles such as departments/teams/user groups in which employees belong.
- Flexible authorization configuration, supporting differentiated permission control scenarios: for example, default permission configurations for "Space Member Groups" and differentiated permission configurations provided for "Custom User Groups."

Operation Record

Meegle maintains detailed operation records for all changes made to work items, spaces, and other objects, facilitating traceability and detection of malicious modifications. Detailed records are also kept for changes made by administrators in the management backend, enabling timely

detection and mitigation of unintentional or malicious permission errors. These records also meet audit requirements post-event.

Watermark

Watermarking is a highly effective security measure. Its presence can deter employees from sharing screenshots beforehand, and even if shared, watermarks can effectively trace the source of information leakage.

Meegle supports three types of watermarks: visible watermarks, image-based invisible watermarks, and text-based invisible watermarks.

- Visible Watermarks: These are user identifiers faintly tiled at the bottom of Meegle interface, typically consisting of partial content summaries such as usernames or phone numbers.
- Image-based Invisible Watermarks: These are invisible to the naked eye and are transparent images containing user identifiers. They are used as tiled backgrounds in the frontend. In the event of data leakage, user identifiers can be extracted by extracting the invisible watermark from the image.
- Text-based Invisible Watermarks: Similar to image-based invisible watermarks, these are also invisible to the naked eye. They are font resources containing user identifiers, with each user having a unique set. These resources are used for text rendering in the frontend. In the event of data leakage, user identifiers can be extracted by extracting the invisible watermark from the text font.

Infrastructure Security

Meegle is built on ByteDance Cloud, benefiting from the stability and security brought by ByteDance's powerful infrastructure capabilities. Additionally, based on this foundation, further optimizations and reinforcements have been made to align with the specific characteristics of Meegle.

Physical Disaster Recovery

The supporting data centers of Meegle are located in three different facilities, ensuring redundancy across multiple locations.

The data centers are maintained by professional personnel on a daily basis and are equipped with 24/7 monitoring. Visitors need to apply to Lark for access to the data center and are accompanied by Lark personnel throughout the entire visit. Access to the data center and server rooms is subject to review by Lark personnel.

Additionally, Lark conducts at least one data center inspection per year, reviewing the hosting service provider, monitoring the security and operational standards of the hosting service, such as infrastructure environment management, personnel access and permission management,

and asset security management. Inspection reports are issued, and any anomalies discovered are promptly addressed by the service provider. Lark arranges on-site personnel to monitor hardware status and determine if destruction is necessary. Upon receiving notification from relevant personnel, operators proceed with hardware destruction and provide destruction results via email for documentation.

Network Security

ByteDance Cloud provides network access for customers through CDN and dynamic acceleration, and accesses backend services through company load balancing. In the event of DDoS attacks targeting the data center, attack defense is conducted through cleaning services provided by network access service providers.

Production Process Security

New Requirement Security Assessment

Meegle has a comprehensive technical solution template, which includes dedicated security-related sections. Technical leads are required to conduct detailed assessments and checks of the security-related aspects of the requirements. Additionally, it is required to involve colleagues from security risk control and legal departments to conduct security technology assessments and compliance evaluations.

- Security Technology Review: Security team members conduct security assessments of the implementation logic of the requirement's technical solution to determine if further manual security testing is needed.
- Compliance Evaluation: Legal and corporate compliance colleagues assess the requirement's design scheme to determine compliance with laws and regulations. If the requirements are not met, corrections are made during the design phase.

Before the product is launched, the security team also conducts penetration testing and deployment security assessments on the requirements to ensure the security of the service.

Testing Security

During the testing process, to avoid security risks caused by testing activities, Meegle has established comprehensive testing security specifications. For example, when logging into company accounts on test machines, it is restricted for personal use only and cannot be loaned out; without customer authorization, it is prohibited to use SaaS customer content data for testing, with testing purposes including but not limited to algorithms, product feature optimization, and functionality verification. These specifications effectively prevent potential information leakage or other security risks caused by testing.

Change Control

Meegle has well-defined procedures for change management, outlining change management requirements and processes, including change proposal formulation, change approval, and change implementation. Operations that are known or potentially impact the stability, availability, or security of online services fall within the scope of online changes. Meegle product development strictly controls change operations to prevent them from affecting service stability. Online operations must be accompanied by an operation form and can only proceed after approval. The company has deployed independent development, testing, and production environments for each product-related application. Change operations follow a gradual release process, with small-scale testing conducted before official release to ensure service stability and security.

Development Environment Security

Employees of Meegle are required to follow the company's environmental controls during the production process. The company internally divides different network areas such as visitor networks, office networks, development testing networks, and production networks. All employees accessing internal company resources from outside the company's network boundary must do so through a VPN connection. The internal auditing department conducts audits on access logs, identifying and tracing records of non-compliant operations, and imposing appropriate penalties.

Internal Security Mechanisms

Vulnerability Operation

Meegle monitors internal and external security vulnerabilities and threat intelligence through various means. The security team utilizes automated security scanning tools to scan their own services and operating systems and conducts regular penetration testing to inspect application systems for security issues. Once vulnerabilities and threat intelligence are confirmed by the security team, they are categorized based on their severity, and notifications are promptly sent to relevant departments for remediation. The company has a comprehensive vulnerability lifecycle management strategy, with a dedicated security team following up on all security issues.

Additionally, the Lark Security Team maintains close cooperation and communication with top third-party assessment companies and white-hat communities in the industry. External companies and white-hat hackers are periodically invited to conduct penetration testing on various services, including Meegle, and are rewarded for discovering as many security vulnerabilities as possible.

Security Incident Operation

Meegle has a well-defined process for handling security-related incidents, from discovery to resolution to post-incident analysis. This ensures that security incidents are detected and mitigated as quickly as possible.

For on-call issue feedback, on-duty personnel are required to promptly determine whether the issue is related to security factors. If a security incident is discovered or occurs, it must be escalated to leadership immediately, reported to the security business partner, and a security on-call initiated.

Third-Party Library Detection

Meegle has a very strict third-party library admission mechanism. Even for approved third-party libraries, their usage is regularly checked to avoid security and compliance issues.

- The license of third-party libraries may change, posing compliance risks in usage.
- New potential security issues may arise with third-party libraries. If vulnerabilities are discovered, it is necessary to determine whether they need to be followed up with upgrades or replacements.

Employee Training

Meegle always places a high emphasis on improving employees' security awareness. Multiple online security-related courses have been developed, which employees are required to complete and pass exams upon launch. These courses are also included as mandatory training for new employees.

In addition to online courses, Meegle provides tools such as IDE security plugins, which are required to be installed by all developers. These tools can effectively identify potential vulnerabilities locally in the IDE, thereby nipping security risks in the bud.