Tencent LearnShare

Security and Policy

Product Documentation

Contents

Security and Policy
Security White Paper

Last updated：2024-12-27 09:28:26

[Copyright Notice]

[Trademark Statement]

All trademarks related to Tencent LearnShare services are owned by Tencent Technology (Shenzhen) Co., Ltd.

[Service Statement]

This document aims to provide customers with an overview of Tencent LearnShare's products and services, either in whole or in part, at the time of publication. Some aspects of the products and services may be subject to adjustment.

I. Foreword

Tencent LearnShare, launched by Tencent in 2008, is an enterprise community application designed with knowledge management at its core. It provides comprehensive services for knowledge sharing, communication, and collaboration within enterprises. Tencent LearnShare offers a wide range of applications, including the documentation, Q&A, event, forum, classroom, and examination. It supports multi-terminal access via PC browsers and mobile devices and is seamlessly integrated with WeCom, enabling users to access it anytime, anywhere.

II. Organizational Security

Tencent LearnShare, as an enterprise-level SaaS service provider, was incubated within Tencent and is built on Tencent Cloud. The security team comprises the Tencent Security Platform Department, Tencent Cloud Security

Assurance Team, and Tencent LearnShare Information Security Group, collectively ensuring the security and reliability of Tencent LearnShare.

1. Security Platform Department

Tencent Security Platform Department is responsible for building basic security infrastructure, including vulnerability scanning, anti-DDoS, secure connection gateways, and secure big data.

2. Tencent Cloud Security Assurance Team

Tencent LearnShare leverages Tencent Cloud's advanced security components and services, including the BGP Anti-DDoS system, Web Application Firewall (WAF), web vulnerability scanning, Virtual Private Cloud (VPC), and CVM firewall isolation. These are supported by the Tencent Cloud security team, which delivers professional and efficient security assurance services.

3. Tencent LearnShare Security Group

1. Responsible for the security design and development of Tencent LearnShare, establishing security policies, providing 24/7 security monitoring, and implementing dynamic defense measures.
2. Conduct business access audits and monitor suspicious operations.
3. Perform regular attack-defense experiments to assess product security risks and the reliability of security policies.
4. Provide 24/7 security incident response, identification, analysis, and resolution.
5. Collaborate with internal security experts and industry specialists to stay updated on cutting-edge security technologies.

III. Personnel Security

Before onboarding, Tencent conducts lawful background checks to ensure employees meet the company's code of conduct, confidentiality, business ethics, and information security requirements.
Upon onboarding, employees are required to sign a confidentiality protocol. Tencent places great emphasis on protecting customer information and user data. Any behavior involving the disclosure of such information is considered a serious violation of company policy and is strongly emphasized during onboarding training.
The Tencent LearnShare team strictly adheres to information security regulations such as the Regulations of the People's Republic of China for Safety Protection of Computer Information Systems and the Administrative Measures for Internet Information Services, ensuring that users' sensitive information and business data are not disclosed. In addition, Tencent LearnShare provides non-scheduled information security training for employees to ensure compliance with established security policies.
Furthermore, at no stage of Tencent LearnShare's design, development, Ops, or release processes does the team access or use production environment data in any form, thereby preventing the disclosure of user information and data.

IV. Compliance and Security

1. Tencent LearnShare strictly complies with relevant laws and regulations, including the following:
Laws:
Article 101 of the General Principles of the Civil Law of the People's Republic of China.
Article 253 (Paragraphs 3, 4, and 5) of the Criminal Law of the People's Republic of China.
Articles 2 and 3 of the Tort Liability Law of the People's Republic of China.
Article 39 of the Law of the People's Republic of China on the Protection of Minors.
Article 4 of the Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security.
Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks.
Regulations:
Regulations on Telecommunications of the People's Republic of China.
Administrative Rules:
Provisions on Protecting the Personal Information of Telecommunications and Internet Users (Promulgated by the Ministry of Industry and Information Technology of the People's Republic of China on July 16, 2013, Order No. 24).
Several Provisions on Regulating the Market Order of Internet Information Services (Promulgated by the Ministry of Industry and Information Technology of the People's Republic of China on December 7, 2011, Order No. 20) .
2. In accordance with relevant national laws, Tencent LearnShare is prohibited from using Personally Identifiable Information (PII) for any other purposes unless explicitly authorized by the customer.
3. In accordance with national laws and regulations, Tencent LearnShare will not disclose customers' PII to any third party without authorization from national judicial authorities.
4. Tencent LearnShare provides SaaS-like services to external clients.
5. Tencent LearnShare's security policy documents and operational procedure files are retained for a long time for customer reference.
6. Customers' PII is stored within mainland China.
7. Tencent LearnShare is ISO 27001 certified.

V. Data Security

Tencent LearnShare's production environment operates on a unified Tencent Cloud operating system. All service installations, upgrades, and migrations are performed by authorized Ops personnel with restricted access, using downloads exclusively from designated trusted sources. Configuration files for system-level services such as Nginx, MySQL, and Redis are centrally managed in the code repository and are uniformly maintained and distributed through deployment, release, and job platforms. Additionally, high-risk APIs and functions of system-level services are strictly prohibited to minimize the potential for vulnerabilities.

All servers hosted on Tencent Cloud are standardized with the TLinux operating system, and maintained by a dedicated Tencent team. These servers are also equipped with Tencent Cloud security components, providing superior security performance.

1. Hierarchical Storage With Sharded Databases by Enterprise

On the Tencent LearnShare platform, all enterprises' business data is stored in independent data instances, each with unique database passwords. This ensures complete data isolation and prevents the risk of database scraping. Furthermore, database accounts are exclusively assigned for specific purposes, with permissions strictly managed based on the principle of least privilege to prevent privilege escalation vulnerabilities and safeguard against data breaches.

2. Data Masking

All sensitive database information, including user-sensitive data and database passwords, is encrypted using symmetric algorithms. Encryption keys are regularly updated.

3. File Storage

All attachments, documents, public resources, and other files are stored using Tencent Cloud's Cloud Object Storage (COS) service. This ensures convenient scale-out, high security, and exceptional reliability. All COS service access policies are exclusively restricted to Tencent LearnShare. Permissions are controlled on a per-enterprise basis and verified through a bypass system.

4. Production Environment Data Access

Unless explicitly authorized by users, no member of the Tencent LearnShare team, including Ops personnel, is permitted to access production environment data in any form. This includes, but is not limited to, database access, text, screenshots, videos, or other means. Additionally, data is never modified without authorization, ensuring user information remains secure and protected from any potential breaches. Additionally, Tencent LearnShare commits not to share user data in any form with third parties, including Tencent Cloud.

5. Data Termination Management

For enterprise data with no access records over a long period, Tencent LearnShare ensures it will be retained for a specific duration. However, beyond this period, the data may be subject to cleanup.
The Tencent LearnShare platform provides an option for enterprises to directly cancel their accounts. Once such an operation is confirmed by the user, the terminated data will be irrecoverable.
All storage media containing data (such as hard disks) should be unmounted before undergoing any maintenance. For network and storage devices scheduled for decommissioning or removal from the data center, data is cleared, disks are demagnetized, and physical termination is performed in accordance with relevant security standards.

VI. Network Security

Tencent LearnShare's network security integrates the advanced capabilities of BGP Anti-DDoS and Web Application Firewall (WAF). This ensures timely detection and response to various abnormal network behaviors.

1. Transmission Protocol

To prevent man-in-the-middle attacks, Tencent LearnShare employs HTTPS/SSL for encrypted data transmission. The RSA algorithm is used for key encryption, while the signature algorithm utilizes the high-bit SHA-256 secure hashing algorithm to ensure the encryption keys remain unbreakable. The enterprise-grade SSL certificate is issued by GlobalSign.

2. Security Domain Segmentation

Tencent LearnShare's deployment on Tencent Cloud uses Virtual Private Cloud (VPC) to achieve network isolation for user data, public data, Redis, job services, and other foundational services. Each service block is confined to its respective security domain, ensuring maximum protection against data breaches.

3. BGP Anti-DDoS

Tencent LearnShare leverages Tencent Cloud's BGP Anti-DDoS service, which effectively prevents various types of DDoS attacks. It also uses the alarm mechanism provided by BGP Anti-DDoS to promptly detect attack activities.

4. WAF

Tencent LearnShare integrates Tencent Cloud's WAF, which blocks malicious requests at the access layer, effectively preventing injection attacks as well as XSS and CSRF attack attempts.

5. Network Access Control

In the production environment, network access control is enforced through mechanisms such as firewalls and security policy groups, ensuring adherence to the principle of least privilege. External upstream gateways are also managed in a unified manner.

VII. Application and Business Security

1. Business Permissions

The Tencent LearnShare platform uses a self-developed access control component. Authorized users can only access data for specific projects. Within a project, the Tencent LearnShare platform provides group-based permission control, enabling multi-dimensional access control over business objects, operation types, and more.

2. Code Security Scanning

Tencent LearnShare incorporates dynamic code scanning tools from Tencent's professional security team across testing, integration, and production environments. These tools provide comprehensive code reinforcement to prevent

potential security vulnerabilities, including SQL injection, XSS, and CSRF attacks. Additionally, security components like CSP are implemented to mitigate vulnerabilities from unauthorized sources, particularly in mobile browsers.

3. Access Security

Tencent LearnShare integrates Tencent Cloud's WAF, which blocks malicious requests at the access layer, effectively preventing injection attacks as well as XSS and CSRF attack attempts.

4. Business Logic Security

The Tencent LearnShare security team incorporates mechanisms such as parameter filtering and secondary data verification at the code framework level to prevent vulnerabilities in the business logic layer. Additionally, the team ensures strict implementation of these security measures by the development team. In addition, the team conducts regular inspections to identify and address potential business logic vulnerabilities within the system.

5. Data API Security

The Tencent LearnShare platform provides API services through a dedicated subsystem with an independent domain name. This subsystem is decoupled from the primary platform using methods such as database read-write separation and microservices architecture. At the same time, the API system enforces strict restrictions on IP addresses, accounts, and data operation permissions, ensuring the prevention of data leaks or unauthorized modifications. Additionally, the API system imposes strict regulations on access frequency.

VIII. Information Security

As an enterprise service provider, Tencent LearnShare is committed to delivering a secure, stable, continuous, and reliable information security foundation for every customer.

1. Access Control

The Tencent LearnShare platform uses a self-developed access control component. Authorized users can only access data for specific projects. Within a project, the Tencent LearnShare platform provides group-based permission control, enabling multi-dimensional access control over business objects, operation types, and more.

2. Anti-Fraud for Activities

Using Tencent Cloud's anti-fraud engine, every request is assessed and validated in real time. The real-time model for activity anti-fraud is trained and refined through extensive business scenarios, serving as the intelligent core of the service to ensure high availability and broad coverage.

3. Captcha

Tencent's security big data system, backed by over a decade of experience in security protection and combating malicious activities, enables real-time and precise analysis of malicious access attempts. It allows trusted users to

bypass verification or undergo lightweight Captcha checks while presenting high-difficulty Captchas to malicious users. This approach ensures a seamless experience for trusted users while effectively countering malicious activities.

4. Image Recognition

Tencent LearnShare leverages Tencent's advanced image data mining technology, covering various informational dimensions of everyday photos to efficiently identify image content. The platform employs an innovative deep learning-based image pornography detection technology, fully replacing manual review and reducing costs by over 90%.

IX. Business Availability and Continuity Security

Leveraging Tencent's extensive service capabilities, Tencent LearnShare uses an automated monitoring platform and OSP to detect faults in real time and enable automatic switches. With multi-site active-active architecture, it ensures continuous business operations.

Tencent LearnShare is deployed on Tencent Cloud, inherently benefiting from Tencent Cloud's high availability capabilities. Furthermore, Tencent LearnShare has been adapted and enhanced to further optimize its performance on this foundation.

Tencent LearnShare uses Tencent Cloud servers powered by high-performance and highly stable virtualization technology, offering reliable services such as web hosting, data storage, and file storage. Additionally, Tencent LearnShare has established comprehensive disaster recovery procedures, which are regularly experimented and maintained. Servers are deployed across multiple regions to minimize the impact of disasters, such as physical damage to IDCs caused by force majeure events, on the system.

PRIVACY POLICY MODULE

Last updated：2024-12-26 17:07:50

1. INTRODUCTION

This Module applies if you use Tencent LearnShare ("**Feature**"). This Module is incorporated into the privacy policy located at （"Privacy Policy"). Terms used but not defined in this Module shall have the meaning given to them in the Privacy Policy. In the event of any conflict between the Privacy Policy and this Module, this Module shall apply to the extent of the inconsistency.

2. CONTROLLERSHIP

The controller of the personal information described in this Module is as specified in the Privacy Policy.

3. AVAILABILITY

This Feature is available to users in Singapore, Thailand and Indonesia.

4. HOW WE USE PERSONAL INFORMATION

We will use the information in the following ways and in accordance with the following legal bases:

Personal Information	Use	Legal Basis
Account Information: Your enterprise name, organizational structure, enterprise logo (to the extent such data qualifies or contains any personal data).	We only process this data for the purposes of providing the Feature to you and your end users.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
User Device Information: User Device Information: device-related information (such as device model, operating system version, operating system name), device	We only process this data for the purposes of providing the Feature to you, including to ensure the normal operation and functioning of the Feature.	We process this information as it is necessary for us to perform our contract with you to provide the Feature, and it is in our legitimate interests to improve and optimize our services.

location-related information (including IP address).	This data is also processed by our Application Performance Management and Cloud Log Service features.	
Log Data: Method, type and status of access to the network, network quality data, operation logs (such as functional operations during the use of the Feature), service log information (such as website information you view on the Feature and service failure information).	We use this information to ensure the Feature functions as required, and to improve and optimize our services. This data is also processed by our Cloud Log Service feature.	We process this information as it is necessary for us to perform our contract with you to provide the Feature, and it is in our legitimate interests to improve and optimize our services.

5. HOW WE DISCLOSE AND STORE YOUR PERSONAL INFORMATION

As specified in the Privacy Policy.

6. DATA RETENTION

We will retain personal information in accordance with the following:

Personal Information	Retention Policy
Account Information	Stored for up to 180 days after the Use we describe in the above is fulfilled; or within 30 days if you request to delete the data.
User Device Information	Stored for up to 180 days after the Use we describe in the above is fulfilled; or within 30 days if you request to delete the data.
Log Data	Stored for up to 180 days after the Use as we describe in the above is fulfilled; or within 30 days if you request to delete the data.

DATA PROCESSING AND SECURITY AGREEMENT MODULE

Last updated：2024-12-27 09:17:49

1. BACKGROUND

This Module applies if you use Tencent LearnShare ("Feature"). This Module is incorporated into the Data Processing and Security Agreement located at Data Processing and Security Agreement("DPSA"). Terms used but not defined in this Module shall have the meaning given to them in the DPSA. In the event of any conflict between the DPSA and this Module, this Module shall apply to the extent of the inconsistency.

2. PROCESSING

We will process the following data in connection with the Feature:

Personal Information	Use
End-user (employee) information: Company, Employee user ID, Department. (Optional) Any personal data relating to your end users that you and/or your end users choose to provide/upload to the Feature (optional), such as nickname avatar, interests, hometown, personal signature, birthday, gender, job position, email address, phone number. Please note that any data categories marked "optional" are not required to be provided to or processed by this Feature, and rather are data that you may choose to provide to us (or require your end user to provide to us) as part of the Feature. We process such data only in accordance with your instructions.	We only process this data for the purposes of providing the Feature to you and your end users, including to display end user information as part of the Feature and to enable you to manage your users. The data is also processed by our TencentDB for MySQL feature.
User Operations Data: Data relating to your employee's and administrator's operations and records on the Feature, such as browsing records, document access records, file download records.	We only process this data for the purposes of providing the Feature to you. Please note that data is also processed by our Cloud Log Service and TencentDB for MySQL features.
Uploaded content: Any documents, files, videos, and audio content uploaded by you or your end users	We only process this data for the purposes of providing the Feature to you.

to the Feature.	Please note that uploaded documents will be integrated with our Cloud Infinite feature, and uploaded videos will be integrated with our Video On Demand feature. Please not that your uploaded content is stored and backed up in our Cloud Object Storage feature.

3. SERVICE REGION

As specified in the DPSA. The main and backup servers for this Feature are in Singapore.

4. SUB-PROCESSORS

As specified in the DPSA.

5. DATA RETENTION

We will store personal data processed in connection with the Feature as follows:

Personal Information	Retention Policy
End User (Employee) information	We retain such data until you terminate your use of the Feature or manually delete such data, in which we will delete this data within 30 days after such termination or deletion.
User Operation Data	We retain such data for up to 180 days. Otherwise, when you request deletion of such data, we will delete such data within 30 days thereafter.
Uploaded Content	We retain such data until you terminate your use of the Feature. If you manually delete such data, we will archive this data after 30 days and permanently delete after 180 days, unless you instruct us to permanently delete in a shorter period of time.

You can request deletion of such personal data in accordance with the DPSA.

6. SPECIAL CONDITIONS

You must ensure that this Feature is only used by end users who are of at least the minimum age at which an individual can consent to the processing of their personal data. This may be different depending on the jurisdiction in

which an end user is located.

You represent, warrant and undertake that you shall provide all notices to, and obtain and maintain all necessary consents from, data subjects in respect of the processing of their personal data (as applicable) in respect of the Feature (including for the purposes of providing the Feature), in accordance with applicable laws and so as to enable us to comply with applicable laws. You agree you will indemnify and hold Tencent harmless from and against all claims, liabilities, costs, expenses, loss or damage (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) incurred by Tencent arising directly or indirectly from a breach of this requirement.