

智连云端 坚守隐私

This is How SUBMAIL protects your privacy and data security.

—— SUBMAIL如何保护您的隐私和数据安全





隐私数据泄露形势严峻

The privacy data leak situation is grim

近几年隐私泄露的情况愈演愈烈，给个人带来了非常多的困扰和安全隐患。而对于企业来说，一旦没有做好信息保护，不仅会产生经济损失，还会损害用户的信任和企业形象，造成负面的社会影响。甚至还会面对法律诉讼、刑事调查。SUBAMIL赛邮作为服务于广大企业和用户的云通信平台，必须全力做好信息数据的安全防护。

In recent years, the situation of privacy disclosure has become more and more important, which has brought many security risks to individuals.

For enterprises, once they fail to do a good job of information protection, it will not only cause economic losses, but also damage the trust of clients and corporate image, resulting in negative social impact. Some may even face legal proceedings and criminal investigations.

As a cloud communication platform for enterprises and users, SUBAMIL must do its best to protect clients information and data.

SUBMAIL 数据加密及安全

SUBMAIL Data encryption and security

—— 严格把关 保护用户隐私



ISO 27001信息管理体系认证

ISO 27001 Information Security Management System Certification



SUBMAIL已获得认证

ISO 27001是世界上应用广泛与典型的信息安全管理标准。认证表明遵守了相关的法律法规，建立了妥善的信息数据保护体系，确保了云计算服务的管理标准，能够保护企业和相关方的信息系统安全、知识产权、商业秘密等。

ISO 27001 is a widely used and typical information security management standard in the world. The certification shows that it has complied with relevant laws and regulations, established a proper information and data protection system, ensured the management standards of cloud computing services, and can protect the information system security, intellectual property rights, business secrets of enterprises and related parties.



网络防护 层层加密

Network Protection Layer Encryption

威胁来源

在网络传输过程中，信息数据可能会被窃取、劫持。甚至网页能直接被篡改，被假冒的钓鱼网站替代。

Sources of threat

In the process of network transmission, information and data may be stolen and hijacked. Even web pages can be tampered with directly and replaced by fake phishing websites.

解决方案

SUBMAIL全站采用先进的HTTPS和SSL/TLS 安全加密传输协议(包含网站、API、以及内网传输)，层层加密，确保用户使用时的安全与稳定。

Solution

In the process of network transmission, information and data may be stolen and hijacked. Even web pages can be tampered with directly and replaced by fake phishing websites.

系统防护 环环相扣

System protection

威胁来源

系统漏洞、API接口漏洞、缺乏完善的账户管理系统等问题，都可能给不法分子可乘之机。

Sources of threat

System loophole, API interface loopholes, the lack of a complete account management system and other issues may give hackers an opportunity.

解决方案

SUBMAIL 通过接入保护、密钥管理、补丁升级、漏洞防护、多账户管理等多维度解决方案来防止用户数据泄露，真正做到安全稳定、环环相扣。

Solution

SUBMAIL prevents user data leakage through access protection, key management, patch upgrade, loophole protection, multi-account management and other multi-dimensional solutions, and truly achieves security, stability.

数据监控 了如指掌

Real-time monitoring

威胁来源

对于云通信中数据管理的不透明、不详尽，就会存在暗箱操作、数据泄露的风险，也会造成用户的疑虑。

Sources of threat

If the data management in cloud communication is not transparent and detailed, there will be the risk of data leakage, which will also cause users'doubts.

解决方案

SUBMAIL 支持用户可以随时查看账户的登录日志以及账户内数据的导出日志，并且精确到IP、时间、浏览器和操作系统。

Solution

SUBMAIL supports users to view account logs and export logs of data in the account at any time, and accurately to IP, time, browser and operating system.

数据储存 万无一失

Data Storage

威胁来源

数据的处理和存储往往会被忽视，一旦发生丢失、泄露、备份不足等问题，则会造成大范围的影响。

Sources of threat

Data processing and storage are often neglected. Once problems such as loss, leakage and insufficient backup occur, will often lead irreversible consequences.

解决方案

在SUBMAIL，您的所有信息数据将保留90天。90天后到180天内，将进入灰度区域，准备清除。180天后您的隐私数据将全部永久删除，只保留分析报告备用。

Solution

In SUBMAIL, all your information and data will be kept for 90 days. From 90 days to 180 days, it will enter the gray area and be ready for removal. After 180 days, all your privacy data will be permanently deleted and only the analysis report will be reserved.

SUBMAIL 未来数据安全企划

SUBMAIL Future Data Security Planning



A. 构建数据保护体系

继续扩大数据保护范围，及时找出和解决数据在流程控制中的安全隐患，完善风险分析和预警系统。

Data Protection System

Continue to expand the scope of data protection, timely identify and solve data security risks in process control, improve risk analysis and early warning system.



B. 构建权限分级体系

减小授权管理的复杂性，在优化体验的同时提高防护能力。层层把关环环相扣,更加完善多账户管理系统。

Hierarchical system of authority

Reduce the complexity of authorization management, optimize the experience and improve the protection capability. Layers of checkpoints are linked to improve the multi-account management system.



C. 信息安全管理日志

不断优化、完善日志的精确性、实时性，详尽地监控数据的动态，形成更加系统化，清晰透明的安全管理体系。

Information Security Management

Continuously optimize and improve the accuracy and real-time of the log, monitor the dynamic data in detail, and form a more systematic, clear and transparent security management system.