Meari Technology
Security White Paper v1.0

Catalog

1. Introduction of Meari Technology

We are a professional R&D company focusing on surveillance cameras, smart home and IoT smart products. We provide customers with one-stop video solution services, including OEM customization, private cloud deployment, AI analysis, SDK docking, SAAS layer services of smart home, and ODM customization of structural hardware. As of the end of December 2022, Meari Solutions' products are distributed in dozens of countries around the world, including Europe, North America and Australia. Meari products are available at retail chains such as Walmart, Bestbuy and Kingfisher throughout Europe and the United States. We have always been customer-focused, and determined to provide innovative products. services and solutions to meet our customers' growing product needs.

2. Security Responsibility

2.1 Security Responsibility for Meari cloud

Meari cloud ensures the security of management, infrastructure In operation and physical equipment by selecting the world-class cloud hosting providers such as Amazon, Alibaba Cloud and other first-class cloud computing platforms.
The cloud security covers data security and cloud service security. Meari promises to use its security team and the professional attack/protection technology experience of well-known security service vendors around the world to provide security operation and operation services for cloud platforms, to effectively protect the security operation of Meari Cloud, as well as to guarantee the security of customers, user privacy and data. Mainly covers but not limited to the following.

Data security: refers to the security management of the customer's business data in the cloud computing environment, including collection and identification, classification and grading, permissions and encryption, and privacy compliance.

Access control and management: The management of access rights to resources and data, including user management, permission management, authentication, etc.

Cloud Service Security: The security management of business-related application systems in the cloud computing environment, including aspects such as design, development, release, configuration and use of application and service interfaces.

2.2 Customer's Security Responsibility

When customers use Meari's cloud solutions, they need to strictly follow Meari's security configuration and access requirements. At the same time, customers need to ensure the security of their own cloud, client or hardware. For the APP developed based on Meari SDK, Meari only provides technical support, but cannot provide any security guarantee. based on Meari OEM (public version) APPs (without any customization scenarios), Meari will provide templates for customers' reference, like data security compliance, privacy policy and other related information, but the customer is responsible for the privacy policy statement and legal compliance of the upload, and when necessary, the security team of Meari is willing to provide help and consulting services for security solutions.

3. Compliance

Meari complies with the international authoritative security standards and industry requirements, and integrates them into the internal control framework, also strictly enforced during the realization process of cloud platform, APP, hardware products and other requirements. We also work with independent third-party security services, consulting and auditing organizations to verify and guarantee the compliance and security of our cloud platform.

Currently, Meari has been certified by multiple global consulting and auditing organizations for information security and privacy compliance, Meari is a IoT solution provider with multi-certified. Meari committed to ongoing certification and compliance credentials for multiple information security and privacy-related to protect our customers' data and privacy.

Currently, our certifications and compliance credentials are listed below.

3.1 ISO 27001

Meari Technology has obtained ISO 27001 certification.

ISO 27001 is an international standard for information security management systems (ISMS) that provides best practice guidance for all types of organizations to establish and operate an information security management system.

As required by the standard.

A business risk-based approach to establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security.

Establishes the appropriate organizational structure, establishes a systematic security management system, and provides resources safeguard in order to ensure the confidentiality, integrity, and availability of information.

follows the PDCA method to continuously improve information security management.

3.2 ISO 9001

Meari Technology has obtained ISO 9001 certification.

ISO 9001 is transformed from the world's first quality management system standard BS 5750 (written by BSI), ISO 9001 is by far the world's more mature quality framework, which is a systematic guiding principle and regulatory framework to ensure the quality and operation of a company's products and services around the products or services provided by the company. and is based on the planning and implementation of the entire process of product or service realization， and to ensure that the requirements of customers and related laws and regulations are met.

The quality management system is used to effectively and efficiently achieve the desired quality objectives through audits and management reviews of the quality management system, and use corrective actions and preventive actions, Continuous improvement of the effectiveness of the quality management system is fundamental

to the development and growth of the company.

4. Data Security

4.1 Meari Security System of cloud data

The Meari security System of cloud data start from the perspective of data security life cycle, use both management and technical to carry out comprehensive and systematic construction. Through the data security management and control of the data lifecycle (data collection, storage, processing, transmission, sharing and deletion), the data security goal is achieved in each stage of the data security lifecycle, with the corresponding security management system and security technology guarantee.

4.2 Data ownership

In the services customized by Meari, the customer is the data controller, and the customer needs to ensure the compliance of data use, and Meari is the data processor, will handle the customer's personal data in accordance with the customer's written instructions and contractual agreement on the basis of compliance with laws and regulations, and all data processing behaviors are transparent to the customer. Therefore, on the basis of compliance with laws, regulations and the Privacy Policy, Meari helps customers and users to safeguard the confidentiality, integrity and security of data.

4.3 Multi-copy Redundant Storage

Using a distributed architecture, all business servers are deployed simultaneously in three server rooms in different regions of the same city, and data storage services such as data repositories use a multi-copy model (at least two real-time copies are guaranteed) and real-time data backup. The high reliability and high availability of

data and services are guaranteed from the physical level.

4.4 User device data security

In terms of device interaction with the cloud.

Data encryption: Encrypt data content using AES128.

identification: Meari's own algorithm guarantees multiple interaction authentication, access control and effective authorization, such as device connection authentication, request authorization, command issuance and etc.

Dynamic Key: One machine with two codes, including dynamic key and dynamic password, to ensure device security.

Channel Encryption: Use TLS1.2 encrypted transmission protocol.

Security Chip: Some chips support the option to use the version with security chip for secure storage of hardware. authorization information and encryption key, etc.

In terms of interactions within the device LAN.

data encryption: using AES128 to encrypt data content for transmission within the LAN.

Dynamic key: algorithm is dynamically assigned during network allocation.

4.5 Enterprise Data Security

Meari cloud will isolate enterprise data to ensure the security of customer data. At the same time, will provides different data storage services for different business scenarios.

and uses AES128 to encrypt and store sensitive data of customers or users, and some sensitive data will be desensitized.

and the key will be unified security managed and distributed through the key management center.

4.6 Residual Data Protection

Memory and disks that have once stored customer data are automatically zero-valued

overwritten with all information once they are released and reclaimed. At the same time, any replacement or obsolete storage devices will be degaussed and physically destroyed by the cloud server infrastructure provider before being shipped out of the data center.

4.7 Privacy Protection

Meari Cloud Platform practices the business philosophy of "everything is based on user value" and pays particular attention to establishing a long and sustainable trust relationship with customers.

With a solid technical foundation and a complete operation and management mechanism, Meari ensures that user and customer data are fully protected. Meari Cloud will strictly implement Meari Cloud's publicly released 《Privacy Policy》 to effectively protect user privacy.

Laws and norms give users rights related to personal information (from the 《Network Security Law of the People's Republic of China》, 《Information Security Technology - Personal Information Security Specification》 (GB/T 35273:2017), GDPR).

1. the right to be informed: the user has the right to know the information about the purpose, basis, source, process, the rights enjoyed of Processing data

2. the right of access: the user has the right to access and confirm the personal information related to him/her.

3. Right of correction: The user has the right to correct and improve the personal information related to him/her.

4. Right to delete (right to be forgotten): The user has the right to request the deletion of personal information related to him/her.

5. Right to restrict processing: The user has the right to restrict the processing activities of the personal information related to him/her.

6. Right of portability: the user has the right to receive all personal information related to him/her in a structured, common and machine-readable format.

7. right to refuse: the user has the right to refuse the processing of personal information related to him/her for direct marketing purposes.

8. right to self-determination: the user has the right to refuse the processing of personal information related to him/her for direct marketing purposes.

8. the right to self-determination: the user has the right not to be bound by decisions based on automatic processing.

To ensure that the legal rights of the user correspond to the functionality of the product.

N	Right	Show on product
1	Right to be informed	To inform the user of the data collected and to obtain explicit authorization from the user when acquiring the user's data (to strongly remind the user to read and authorize the Service Agreement, Privacy Policy, and Permissions Statement at the time of registration, to strongly remind the user to read and authorize again after changes to our agreement, when need acquiring additional data for value-added services, to strongly remind the user of the data situation which need to collected and to obtain authorization)
2	Right of access	Users can access their own relevant data, whether through the product or through an after-sales service.
3	Right of correction	Users can modify all of their own data including cell phone numbers, email addresses, etc. (including but not limited to, identity information, address, avatar, nickname)
4	Right to delete (right to be forgotten)	Be sure to implement the function of "logging out" and deleting usage data.
5	Right to restrict processing	Users can choose the scenarios in which their personal data will be used
6	Right of portability	users can get to all their own data on the platform, whether through APP self-service acquisition, or through customer service and technical support.

7	Right to refuse	The user has the right to refuse to provide information that is not necessary for the provision of the user's services
8	Right to self-determination	All locations that require user confirmation of authorization cannot be confirmed by default in the checking box, and must be confirmed by user initiative.

Data classification: distinguish between personal data and platform information data, and classify personal data using sensitivity and confidentiality level.

4.8 Data Storage Area

Five data centers: China server room, North America server room, South America server room, Europe server room, and Singapore server room (each data center is physically isolated from each other and does not interoperate). The data service is provided according to the user's location.

China: Data is stored in Hangzhou, China, with Alibaba Cloud providing basic cloud computing support.

North America: Data is stored in Northern Virginia, USA, with Amazon AWS providing the underlying cloud computing support.

EU countries: Data is stored in Frankfurt with Amazon AWS providing the underlying cloud computing support.

Singapore: Data is stored in the Singapore server room, powered by Amazon AWS.

Other countries: choose the server room for storage according to the principle of proximity, and will gradually open more regional server rooms, which are currently under construction in many regions.

5. Security organization and personnel

In order to let all employees continuously improve security awareness, better protect customer (tenant) data, especially the user's private data, and better protect customer interests and product and service reputation, Meari has established management policy

"information security, full participation; key data, strict control; active prevention, continuous improvement; customer trust, stable operation. " improve the information security awareness of all staff, integrate the information security culture into the corporate culture, and implement the work of information security to every person.

5.1 Security and Privacy Protection Team and Personnel

At the security technology level, Meari has a professional security technology team to support the security architecture, security design, security assessment and security operation and maintenance of Meari Cloud. At the level of privacy compliance, Meari has set up a Privacy Protection Officer (PPO), who is responsible for privacy impact assessment, rule-making of privacy requirement design and promoting the execution of privacy protection management.

At the same time, we have established an internal information security management and compliance group, which covers information security and privacy protection, and its members are divided into decision-making, management and execution levels, corresponding to the information security leadership team, information security working group and members of each team in Meari. The top-down security organization ensures the alignment of security goals, security strategies and Meari's business strategic planning, and provides Meari (including operational and business stakeholders) with the resources needed for risk avoidance and compliance.

5.2 Human Resource Management

Meari's HR security management framework is consistent with the company's overall HR management framework, which sets security requirements for employees, key positions and third-party personnel, including four aspects of appraisal management, entry job management, on the job management, off-job management and personnel security assessment management, so as to effectively prevent or reduce information security incidents caused by human factors through active prevention.

5.3 Security Awareness Education

In order to enhance the network security awareness of all employees, avoid the risk of network security violations and ensure the normal operation of business, Meari has issued an internal "Employee Information Security Manual" and regularly carries out network security awareness education and learning based on this, requiring employees to continuously learn network security knowledge and understand the policies and systems on the manual. Knowing which behaviors are acceptable and which are not, realizing that even if there is no subjective malice, they must be responsible for their own actions and committing to perform as required.

5.4 Security management system related training

In order to enable all company staff to accurately understand the company's information security management policies and effectively promote and implement security policies, the

Meari's security team regularly conducts training related to privacy protection compliance and data protection for business personnel.

5.5 Information Security Capability Enhancement

Meari regularly holds security development training and exchanges the information security internally, aiming to improve employees' security skills and ensure that they are capable of delivering secure and compliant products, solutions and services.

6. Cloud Platform Security Assurance

6.1 Physical Security

As an IoT cloud computing service provider, Meari Cloud Platform strives to provide a secure, stable, continuous and reliable physical facility foundation for each customer. Based on the international standards and regulatory requirements related to data centers,

a comprehensive security management system has been established, from system strategy, to process management, and with strict monitoring and auditing, to ensure the physical and environmental security of the cloud platform data center through continuous improvement.

6.1.1 Highly available infrastructure

Meari Cloud Platform integrates the world's most famous cloud hosting providers, such as AWS, Alibaba Cloud, to build global service nodes. It provides customers with a secure, stable, continuous and reliable physical facility foundation. According to the domestic and foreign sales regions of Chinese enterprises, Based on the distribution of submarine fiber optic cables and the results of actual measurements in cities around the world, we have deployed five availability zones covering China, Europe, North America and Singapore.

The deployment covers five availability zones in China, Europe, North America, and Singapore. This includes, but is not limited to, the Virginia server room in the United States;the Frankfurt server room in Europe; and the Alibaba Cloud server room in Singapore. Meari cloud flexibly deploys data and systems in different data centers or different regions to ensure the disaster-tolerant requirements of the business.

6.1.2 Security inspection and audit

Security event management: Meari and the cloud server provisioning platform reach a physical security contingency plan and organize regular security drills for data center staff. In the event of a physical security incident, the plan will be able to take effect immediately and guide relevant personnel to protect customer assets to the greatest extent possible.

6.2 Network Security

6.2.1 Security Architecture

Meari has a mature network security architecture, including firewall, WEB application firewall, intrusion detection, RASP, host protection system, and other multiple protection mechanisms to deal with various threats from the Internet.

6.2.2 Network Communication Security

The communication on the Meari cloud platform all adopts TLS1.2 security protocol and implements mandatory encryption protection with certificate authentication, including the communication between devices with APPs and the cloud, and the API interface provided also has perfect security capabilities such as TLS, which can provide port-level security to customers. At the same time, the content of communication is additionally encrypted with AES128. Double-layer encryption protects the security of the communication process.

6.2.3 Network Isolation and Access Control

Meari has established strict internal network isolation rules. Access control and boundary protection of internal office network, development network, test network, production network, etc. are realized through physical and logical isolation. Meari cloud ensures that non-authorized personnel are prohibited from accessing any internal network resources. All employees who need to go from the company network to the production network to carry out daily operation and maintenance must go through strict approval and permission control of the Bastionhost before they can use the restricted permission to log into the production system, and the whole use is audited.

6.2.4 Network Redundancy

Cloud hosts of Meari Cloud Data Services are located in many regions around the world,

building the disaster recovery capability of network cross-territory, which can minimize the business impact of network failures caused by non-human factors. At the same time, the redundant network construction method is adopted, while the same city also adopts multi-physical room deployment, which realize the convenience network and flow echo of engineering scheduling to ensure that the network service will not be interrupted by a single point of failure, and realize co-location and cross-city disaster recovery.

6.2.5 DDOS Protection

Meari uses self-developed WAF and third-party security tools to detect, block and deal with DDOS attacks, and formulates different perfect measures for the scale of DDOS attacks to ensure the stability of the cloud platform network. For CC attacks, the internal firewall and WAF are used to block them. At the same time, through the internally analysis of all the request logs, the abnormal IP are detected and the suspicious source addresses are dynamically blocked.

6.2.6 Intrusion Prevention

Intrusion prevention: Intrusion blocking is carried out through firewalls and WAF devices.
Host Intrusion Detection System: Meari uses a combination of self-developed HIDS and third-party HIDS to defend against many external attacks, with features including WebShell detection module, where the server deploys a WebShell real-time detection engine that can detect, delete and report WebShell in real time.
A host anomaly login detection module that identifies machines that are logged in by non-bastion machines.
-Insecure baseline configuration detection module, which identifies whether a machine is online according to the security baseline configuration. Brute -force cracking detection module, which identifies whether a server has been remotely blasted, and host vulnerability detection module, which identifies application vulnerabilities and system vulnerabilities in the host. etc.
Database audit: Strictly unified management and restriction of database permissions,

and complete log audit of all database additions, deletions, and changes, search.

7. Cloud platform security assurance

The cloud platform and cloud products are developed in strict accordance with the security development lifecycle approach, with the goal of integrating information security into the entire software development lifecycle.

Meari's development lifecycle security cycle comprehensively covers all phases of the system development lifecycle. Through the security management platform unified project SDL implementation monitoring and management, and basically realizes fully automated process tracking and automated security rating.

7.1 Security Training

The Meari security team establishes a regular security training management mechanism for developers, and according to the security vulnerabilities found during the testing, release and vulnerability operation stages, we continuously improve security training.

7.2 Security Requirements and Review

Requirements analysis phase.

The product manager will use the baseline requirements set by the security team as criteria, including password security, authentication, encryption and decryption, service and port security, file upload, configuration security, privacy protection, etc., to collect the security requirements that need to be met, and When necessary, the security team will assist in developing security requirements, and when new applications, old applications, systems, or products are created or have change requirements, If privacy risks are involved, the product manager will follow the "privacy design management requirements" to ensure that the privacy protection measures are designed to penetrate into the project plan. The product manager will follow the "Privacy Design Management Requirements" to ensure that the design of privacy protection measures will penetrate into the project solution.

Requirements Review Phase.

Requirements review follows the overall information security requirements of Meari, including but not limited to the following.

a) Data security: Data collection, transmission, use, storage, and erasure need to follow the requirements of《Meari's Data Protection Management Specification》, to ensure the lifecycle security of application-related data; In addition, routine integrity checks should be performed on the application interfaces, interfaces across multiple systems, and data input and output of the database.
b) Key security: key generation, transmission, storage, update, destruction and audit need to follow 《 the requirements of Meari Key Security Management Control Procedures》 to ensure the lifecycle security of application-related keys.
c) Network security: The service protocols, ports and IP that need to be opened due to business requirements should be safety assessment.
d) Permission security: Role-based access control (RBAC) is used for authorization, and the minimum permission policy is implemented between topics and objects to ensure that the access control list covers all possible schemes.
e) Business security: The business rules, processes, and product functional security involved in the application after it goes online are evaluated and need to comply with the relevant national laws and regulations, website related rules and other specific requirements. Products should plan to take the necessary means or measures to strengthen the control of security risks, such as docking security products, filtering security risk list, take the necessary prevention and control means.
f) Technical security: technical security review of the application technology framework, code vulnerabilities, system security and other assessments, need to meet the specific requirements of product security. Products should plan to take the necessary means or measures to strengthen the control of security risks, such as the use of security components, consciously conduct security code scanning, etc., and timely response and prevention of risks when security risks and vulnerabilities arise.

7.3 Security Design

Security management and technical means matching security requirements will be fully considered in the design phase. Based on the results of requirements analysis and review, when new systems are developed or existing system versions are iterated, the development team will conduct security architecture design and threat modeling with the assistance of the security team, fully considering business system confidentiality, integrity, authenticity, reliability, availability, and non-repudiation, identifying counterfeiting, tampering, denial, elevation of privileges, denial of service, information leakage, and risks related to business security and compliance.

7.4 Secure Development

7.4.1 Code Specification

Throughout the development cycle, application development/testing activities are isolated from the production environment information resources to ensure high availability of the online environment. Develop secure development specifications and guidelines and use secure methods for development work.

7.4.2 Code Audit

The code audit developed independently by Meari is bound to Meari's project release system, and the code audit test is automated before the project reaches the testing stage. It automates real-time tracking of mainstream vulnerability intelligence, automatically updates the library of insecure third-party components, and can generate rules for vulnerability alerting in the first place.

7.4.3 Mobile scanning

Meari APP packaging platform, after completing the packaging of new APP, it will automatically send APP packages to the mobile scanning platform for scanning, supporting APPs of Android and IOS.

7.5 Security Testing and Fix Verification

Meari security team refers to OWASP Top10, third-party vulnerability platforms and industry security practices to continuously improve the product and rules, and formulate 《Meari Security Test Cases》 for testers to test. Only after passing the security test and passing the security release review, the system can be released to the production environment, which can effectively prevent the product from running in the production environment with security vulnerabilities, and prohibit the use of unauthorized or sensitive data in the production environment without desensitization during the testing process. The release process is strictly in accordance with the security go-live specification for overall system hardening.

8. Cloud platform security guarantee

Through Meari's security operation and maintenance platform for unified management, strict access control and monitoring and auditing are adopted to ensure the security of operation and maintenance.

8.1 Access Control

8.1.1 Principles

Meari access control follows the following principles.

Isolated operation: For networks and information systems of different importance levels and different purposes, specific isolation measures (logical isolation or physical isolation measures) should be taken to ensure that various types of systems operate

independently.

Minimum Permissions: Users should have only the minimum access rights required to complete a certain job, and user rights should be closely related to job responsibilities and updated in a timely manner.

Approval on demand: When granting access rights to users, the person responsible for the system should authorize on demand to avoid excessive user access rights.

Separation of duties: A user cannot assume multiple roles with conflicting duties at the same time to prevent obtaining excessive privileges. The requesting party, authorizing party, and managing party of important access actions should realize the separation of duties.

Default denial: Users without explicit authorization shall be denied access by default.

8.1.2 Account Management and Identity Authentication

Meari uses domain accounts for unified identity authentication and account management for employees. During employees' employment, domain accounts are unique and unchangeable, so that users are combined with their actions and are responsible for their actions to ensure accountability. Centrally issue password policies, enforce password strength, and require regular password changes. Two-factor authentication is turned on for the core system, and dynamic verification codes are obtained for secondary verification.

8.1.3 Special access rights management

Restrict and strictly control the allocation and use of special access privileges, and do not allow the use of privileged accounts for daily business activities. Special access privileges are assigned to users in accordance with the principles of "use on demand" and "one matter at a time", i.e., the minimum requirements are assigned to their functional roles only when needed; the validity period of special access privileges is defined, and special privileges are immediately recalled upon expiration. Regularly audit

the authorization status of special access privileges and user accounts and keep records to ensure that there are no unauthorized special privileges.

8.2 Operation security management

8.2.1 Operation Procedures

Meari establishes appropriate operational responsibilities and standard operating procedures (SOPs) for operation activities related to information processing facilities and develops security policies to ensure that employees operate information processing facilities correctly and safely. Effective access control policies are also established to prohibit unauthorized access and disclosure.

8.2.2 Change Management

All change operations follow the requirements of 《Meari Change Management Procedures》 to ensure that the change process does not affect the stability and continuity of the business, and the person in charge of the change process issues monthly change management reports, analyzes the quality of changes, and analyzes and evaluates failed changes, and regularly reviews and optimizes the process, including key measurement indicators, process execution efficiency and the effectiveness of process support tools, etc. Ensure continuous improvement of the change management process.

8.2.3 Capacity Management

When monitoring, forecasting and planning for capacity, the following aspects are considered.

Based on SLA, business backup and recovery requirements, and the results of capacity monitoring and business forecasting, develop monitoring scope and indicators for resource service objects, as well as monitoring cycles, thresholds, methods and techniques.

Conducting capacity analysis based on capacity monitoring data, analyzing the gap

between existing capacity and current SLAs and projected requirements, and making recommendations for improvement.

should conduct continuous and effective capacity monitoring of the information system, and should provide timely warning once abnormalities are detected, and achieve dynamic adjustment and management.

Capacity planning will be managed anew when new service level agreements are initiated, when changes affecting system capacity are implemented or when new technical, operational, legal and business process and other external changes affect system capacity

8.2.4 Backup Management

In data backup activities, data backup policies are formulated and data is backed up regularly in accordance with RPO requirements; strict permission control is also set for backup data to prohibit unauthorized access and use; recovery tests and drills are conducted regularly to ensure data confidentiality, integrity and availability.

8.2.5 Log Management

All operations and maintenance operations by employees on the production system must and can only be performed through the Bastionhost. All operation processes are completely recorded and taped, and the log server is deployed for unified and centralized storage. Regular log check audits are conducted for privileged use, unauthorized access attempts, system failures and abnormalities. All suspicious or confirmed illegal access behaviors and attempts are reported to the information security working group in a timely manner and corresponding measures are taken.

8.2.6 Security baseline management

Set up standard baseline specifications for the network, system, middleware, database and other components involved in the information system; and constantly update and maintain them according to the actual situation, detect and monitor the baseline

configuration of the information system by automated means before the system is put on line and during the operation process, and conduct early warning, tracking and management.

8.2.7 Test Management

Meari develops strict environmental isolation measures, separates the online environment from the test environment, prohibits the use of online data containing personal information or other sensitive data for testing, and strictly prohibits stress testing in the online environment.

8.2.8 Security Threat Prevention

Security scan: We perform weekly security scan of the whole network, including WEB site vulnerability scan, application and service vulnerability scan, host vulnerability scan, etc.

Security crowd testing: Meari inspires security experts in the whole society to test and discover vulnerabilities in the enterprise's own website or business system by issuing rewards, timely discovering high-risk vulnerabilities that exist online, and ensuring that security risks can be quickly responded to and repaired to prevent greater security losses.

Virus prevention.

1) The office terminals of Meari are uniformly installed with anti-malware programs, and terminals without anti-malware programs are strictly prohibited from accessing the company network, while the automatic update function is turned on.

2) The server side of Meari deploys anti-malware software, and ensures that all relevant components of the anti-malware software can run normally, and the functions of real-time scanning and automatic update of components are opened normally.

9. Business Security and Risk Control

9.1 Account security

Meari Cloud Service is designed to attach great importance to user account security, so strict security control and log audit are carried out for account registration, login and password retrieval, etc. Verification codes are used to guarantee the ability of human-machine identification and avoid attacks such as account violence cracking, and SMS verification codes are used to bind users' common devices to ensure the security of user accounts through secondary SMS verification.

The storage of user accounts and other private data is protected by high-grade encryption. There are real-time detection and alarm mechanisms for security response to common account attacks such as crashing and API abuse.

10. Terminal Security

10.1 Hardware and firmware security

10.1.1 Communication security

According to the performance of different hardware chips, Meari provides different levels of encryption mechanisms to maximize the security capacity of the chips, and the communication security of data is guaranteed regardless of which encryption mechanism. Currently, the main communication protocols of Meari modules are MQTT over TLS and HTTPS, which use TLS1.2 and AES encryption algorithms to ensure communication security, and additional AES encryption protection for data and control instructions during interaction. The AES encryption key uses a dynamically generated device-based, unique random key.

At the same time, Meari critical communication data is protected using various data protection mechanisms such as data replay prevention verification, authenticity and

integrity verification, device identity verification, access control and permission verification.

10.1.2 Firmware Protection

Meari carries out multiple protections for firmware: 1.

1. Firmware anti-counterfeit verification, Meari firmware will be signed by Meari's certificate, and the legitimacy of the firmware will be verified by the certificate before Meari device upgrade.

10.1.3 OTA Security

Meari adopts multiple protection means to protect the firmware upgrade process.

1. When generating a firmware package, the packaging tool will generate a firmware integrity check information, which consists of several variables.

When the client requests firmware, the server will send a firmware download information and firmware verification information. The firmware checksum information is uses a secure RSA + SHA256 signature algorithm and adds the device's unique identity key information as a factor to ensure that the firmware cannot be tampered with during transmission.

3. After the device gets the firmware, it needs to calculate the firmware verification information and compare it with the firmware verification information provided by the server, and it also needs to check the integrity verification information calculated by the packaging tool in the firmware when decompression. Only when the firmware double-checking is completed, the firmware is allowed to be written.

4. If the firmware fails to be written or does not work properly after writing, it will automatically revert to the original firmware.

10.1.4 Data Protection

In the secure chip version, we store authorization information and encryption key, which are used to ensure the security and legality of communication between Meari module

and the cloud, and can effectively prevent the authorization data and encryption key from being stolen or tampered by illegal persons. There is a secure data area inside the security chip, and during the use, the Meari module will read the encrypted sensitive information into the RAM and lose it when power is lost. At the same time, when the module and the security chip communicate, there is a temporary key for encryption protection. Encryption protection.

For the non-secure chip version, in order to secure the core data, the important information stored locally will be AES encrypted After that, it is stored.

10.1.5 Network security

Before network distribution, the device discovers that the broadcast information sent by APP and hardware is transmitted with AES encryption.

In the process of network distribution, the device opens WIFI hotspot protected by WPA2, and the information of network distribution is encrypted by WPA2 and then transmitted to the device, which ensures the security of user network and reduces the risk of network distribution process.

11. Business Sustainability

11.1 Business Continuity

In order to eliminate disruptions in critical production and operation activities and avoid them from suffering from major failures or disasters, Meari develops business continuity management strategies, documents business continuity plans, organizes and conducts business continuity plan exercises, and continuously improves business continuity strategies and plans. Through the operation and maintenance platform, all hosts, applications, services and networks of the cloud platform are monitored in real time, and there is a complete set of automated process system and guarantee for business failures, and the services are guaranteed to be uninterrupted through multi-service hot-swap.

11.2 Disaster Recovery

Real-time hot backup of master and slave data, redundant storage and multi-location backup are adopted to ensure that business data is safe, reliable and continuously available. The backup situation is monitored and verified in real time.
At the same time, for business systems, multi-link backup systems are used to ensure rapid emergency switchover.

11.3 Contingency Planning

We establish internal contingency plans and measures for various types of assets and security risks, and implement them based on the 《Meari Business Continuity Control Procedures》. The implementation is based on the Meari Business Continuity Control Procedures, which can guarantee the correct, orderly and efficient emergency treatment after the incident and the normal operation of work. Contingency The emergency response plan includes the pre-planning process, monitoring and a series of failure response measures. A detailed review of the system monitoring during the event records, to provide sufficient information for quick understanding and analysis afterwards, as well as the corresponding interface personnel. Afterwards, there is a set of perfect The process of handling methods and contingency plans to ensure that the problem can be dealt with quickly, analysis and accountability.

11.4 Emergency Drills

Regularly implement large scale hardware failure, network DDoS, security events and other internal technical emergency drill tests and practical exercises.