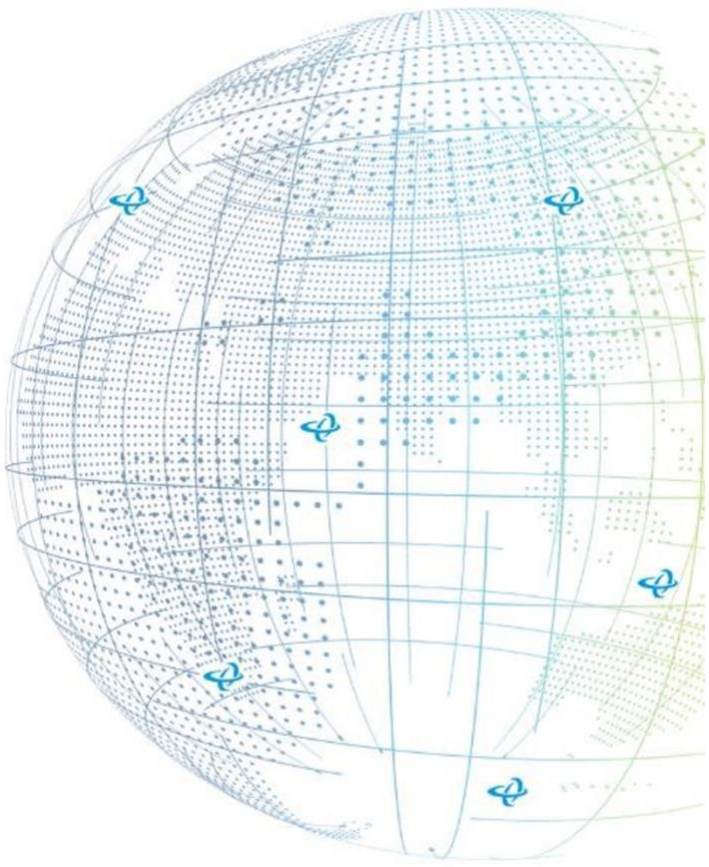
Hitrontech Security White Paper

Issue: 1.2
Date: 2023-11-09



Hitron Technologies (SIP) INC.

Content

1 Introduction

At Hitron Technologies (SIP) INC.(hereafter called “Hitrontech”), we are dedicated to delivering cutting-edge cloud application development and operation services that empower organizations to thrive in today's digital landscape. In this era of rapid technological advancement, we understand that ensuring the security of your digital assets and sensitive data is paramount. This document serves as a comprehensive overview of our commitment to security and the best practices we employ to safeguard your cloud-based operations.

2 Security Responsibilities

2.1 Shared Security Responsibility

Based on the service model of Hitrontech, the security responsibilities need to be shared between three participants：

- Hitrontech is responsible for the security configuration, management and operation of all cloud services, API services, SDK services and data interactions based on the basic cloud service, while also responsible for the security of data interaction on standardized access interface of the cloud solutions developed by Hitrontech.
- Customers are entrusted with the responsibility for safeguarding their own business security. This encompasses the security of hardware business logic, customized App business logic, and account security.

2.2 Hitrontech Security Responsibility

The main responsibility coverage including but not limited to:

- Network Security: Ensures the security and integrity of the cloud infrastructure, including network architecture, access control list and firewall configurations.
- Data Security: Safeguards client data through encryption, access controls, and data classification.
- Infrastructure Security: Maintains the physical and virtual infrastructure, including server security and data center protection.
- Human Resource Security: Ensures that employees are trained in security practices and follows security policies.

- Development Security: Incorporating security into the software development lifecycle (SDLC) to create secure applications. Conducting code reviews, vulnerability assessments, and penetration testing.
- Operation Security: Manages day-to-day cloud operations securely, covering patch management, system monitoring, and incident response.

2.3 Customer Security Responsibility

- Account Security: Customers are responsible for securing their own user accounts and access credentials. This includes maintaining strong, unique passwords and enabling multi-factor authentication (if available).
- Compliance: Customers are responsible for ensuring that their use of Hitrontech's cloud services complies with applicable laws and regulations.
- Incident Reporting: Customers should promptly report any suspicious activities or security incidents related to their cloud services to Hitrontech.
- Application Security (if applicable): Customers are responsible for securing any custom applications or code they deploy on the cloud platform.

3 Compliance and Regulation

In today's complex regulatory landscape, ensuring compliance with applicable legislation and contractual requirements is paramount. At Hitrontech, we take a proactive approach to compliance and regulation, consistently monitoring and adapting to meet evolving legal and contractual obligations.

3.1 Identification of Applicable Legislation and Contractual Requirements

We rigorously identify and document the legislation and contractual requirements relevant to our cloud application development and operation services. This includes but is not limited to:

- Data protection regulations such as GDPR or CCPA, depending on the client's geographic location and data types.
- Contractual agreements with clients that stipulate security and data protection requirements.

3.2 Intellectual Property Rights

We respect and protect intellectual property rights throughout our services. We ensure that client data, proprietary software, and any intellectual property created during the development process are safeguarded and used only in accordance with applicable laws and contractual agreements.

3.3 Protection of Records

Hitrontech maintains robust record-keeping practices. We securely store records related to security assessments, audits, incident reports, and compliance assessments. These records are protected against unauthorized access and alteration.

3.4 Regulation of Cryptographic Controls

Hitrontech complies with regulatory requirements related to cryptographic controls. We use industry-standard encryption algorithms and key management practices to protect sensitive data during transmission and at rest. Our cryptographic practices align with the guidelines set forth by relevant regulatory bodies.

3.5 Independent Review of Information Security

As part of our commitment to maintaining the highest security standards, Hitrontech conducts regular independent reviews of our information security practices. These reviews are performed by third-party auditors and assessors to ensure an impartial evaluation of our security controls. The results of these reviews are used to identify areas for improvement and demonstrate our dedication to transparency and accountability.

4 Human Resource Security

4.1 Personnel management

Hitron human resource management framework is consistent with global human resource management framework of the company. At the same time, the ruling Basic Policy of Human Resources regulates the whole human resource management processes, in recruitment, management of employee contracts, attendance and performance management, and procedural management of resignation to strengthen human resource security.

The role of the human resource department in ensuring security mainly includes ensuring that employee background and qualifications meet business requirements. All employees' acts are linked with a code of

conduct, with the requirements of all the laws, policies, processes set out by Hitrontech. All employees have the necessary knowledge, skills and experience to fulfill their duties. If the employee lacks experience, Hitrontech should provide employee training until they are competent before proceeding to work.

The employment agreement that between the employee and Hitrontech complies with the terms of the information security policies. At the same time, a confidentiality agreement must be supported to ensure the confidentiality and integrity of information, whether it's about Hitrontech or customers, that the employee may have access to, including commercial secrets, technical secrets, employee information and customer data.

4.2 Permissions management

Hitrontech uses JIRA for managing the development process and Gitlab for source code management. Both systems are configured with roles and access restrictions to ensure security of the development environment. All source code changes committed to the source code repository must be associated to a specific JIRA ticket or it will be rejected by the source code management system. This ensures a complete audit trial for all changes beginning with the original change request.

Based on employees' job positions and roles, Hitrontech follows the principle of minimum authority and separation of duties and grants employees limited access to resources. The company sets different Gitlab access permissions for each employee according to their work needs. If the employee is transferred or resigned, the permissions are immediately withdrawn. Hitrontech employees may not attempt to access any data or programs contained in the company's internal systems without authorization or explicit consent.

Hitrontech conducts technology training on the security of business, code, and products from time to time to improve the technical capabilities and safety awareness of Hitrontech employees, and each employee is directly responsible for their operations.

5 Data Security and Privacy

5.1 Data Security Framework

Hitrontech beholds the philosophy that "centralizing customer value" and pays particular attention to establishing long-term and lasting trust relationships with customers. From the perspective of data security life cycle, the cloud data security system adopts both organizational management and technical means to carry out comprehensive and systematic construction. Data security management is carried out at all phases

of the data life cycle (data collection, storage, processing, transmission, sharing, and deletion) to achieve data security goals.

Meanwhile, there is corresponding security management system and security technology guarantee at each stage of the lifecycle of data.

5.2 Data Ownership

Hitrontech is committed to the protection of data privacy, in compliance with all data protection laws, the individual user is the owner of the ownership and ownership of data belongs to individual users. Respectively, in the customized solution, the personal information generated shall be controlled by the respective customers, namely the data controllers. The customer has the discretion to determine the way and purpose of processing personal information, in the meanwhile, the customer has the primary liability in ensuring data security and conformity of privacy. Hitrontech acts as the data processor and the data processing activities are implemented under customers' written instruction, which is elaborately documented in the data processing contracts or addendum, on a lawful and transparent basis. Therefore, given compliance with the data protection regulations and Hitrontech privacy policy, Hitrontech is surely able to assist clients and users in protect data confidentiality, integrity, and security. Hitrontech, as the service provider, acts as a data processor that processes data per authorization of the customers. Hitrontech and the customers enter into stringent data processing agreements that provide for the scope and means of data processing, and relevant responsibilities and obligations. Hitrontech implements strict authorization and access control policies and corresponding technical safeguard structures to ensure that data is only accessed or processed under due authorization of the customers. Meanwhile, in order to guarantee data and privacy compliance, Hitrontech has deployed independent data node in North America to execute localized data storage and processing and implemented stringent data encryption mechanisms.

5.3 Data Security Lifecycle

5.3.1 The Fundamental Principles of Processing Personal Information

Any personal information processing activity by Hitrontech products and services adhere to the principles of lawfulness, legitimacy, and necessity. Specifically, such data processing principles require the data controller/processor to act according to the following:

- Consistency of rights and responsibilities (Accountability and Governance) – undertake liability for damages of the legitimate rights of the users caused by personal information processing activities.
- Purposes limitation – identify lawful, legitimate, necessary and specific purposes for personal information processing.

- Data subject authorization/consent – clearly state the purpose, means, scope and rules of personal information processing to the users, and obtain authorization/consent from such users.
- Data minimization – unless otherwise agreed with the user, only process the minimum types and amounts of personal information to satisfy the authorized purpose of the users; not process, store, request, provide or transmit any data unrelated to the services; and timely delete personal information pursuant to agreement after completion of the purposes.
- Transparency – publicly state the scope, purposes and rules of personal information processing in specific, understandable and reasonable manners, and accept external supervision of data processing activities.
- Security safeguards – have security competencies commensurate to the security risks it faces, and implement sufficient management means and technical measures to ensure confidentiality, completeness and availability of personal information.
- Subject engagement – provide means by which the users may access, rectify and delete personal information, and ways to withdraw consent or cancel the account.

5.3.2 Individual Privacy Rights

Data security and privacy protection laws and regulations emphasize the protection of personal privacy rights. Hitrontech has formed the Privacy Policy to help realize users' privacy rights based on the provision of services. At the same time, Hitrontech also helps customers in responding to user requests, including the following privacy rights:

- Right to be Informed
  - Privacy Policies for the Hitrontech Apps and websites.
  - The Privacy Policy elaborates all personal information, or the type of personal information being collected
  - The Privacy Policy elaborates the source of such personal information and the purposes of processing.
  - The Privacy Policy elaborates identities or types of third parties that may access the above personal information.
  - The Privacy Policy may notify the users from time to time via email or in-App prompted notices. When any significant change has been made to, e.g., the way or purposes of processing personal information, or to the new type of data collection, a separate consent shall be made by the user.

- Cookie Statement on the website
  - Displays all Cookies and their functions.
  - Users may turn off functional and advertising cookies with one click, which will not affect the functioning of the websites.
- Users' withdrawal of consent
  - Allows users to withdraw consent in using services of the App or the websites. After withdrawal, Hitrontech will not subsequently process any personal information of the user.
  - To analyze usage conditions of Hitrontech products and services and to enhance user experience, Hitrontech may conduct data analytics of data provided and reported by the users and timely examine issues that the users may encounter when using the products. Users may turn off data analytics in the Hitrontech App.
  - To provide customized products and tailored services for the users, Hitrontech may process account information, usage information and device information of the users. If a user does not consent to such processing, he/she may elect to turn off selection in the Privacy Settings in the App.
- Right of Access

Users can access personal information collected by Hitrontech through the App without additional technical support.

Users can make a privacy request to Hitrontech for any data processing activities and its related purposes, as well as all personal information associated with services and functions.

- Right to Erasure

As the owner of the data, the user can cancel the account and delete user data completely through the account deletion function on the APP or through submitting feedback/contact the official website customer service. The deleted data includes but is not limited to user identity information, the user's use of APP and smart device records, and the information generated and collected by the smart device during the user's use. The user may request deletion of specific personal information when one of the following conditions is met:

  - Personal information shall be removed per the user's request, when:
    - Hitrontech collects or uses personal information in violation of applicable law or regulation; or
    - Hitrontech collects or uses personal information in violation of relevant agreement with the user.
    - Hitrontech, in violation of applicable law or regulation or relevant agreement with the user, shares or transfers personal information to any third party; when the user requests deletion,

Hitrontech shall immediately cease such sharing or transfer, and notify relevant third party to timely delete the personal information.

- Hitrontech, in violation of applicable law or regulation or relevant agreement with the user, publicly discloses personal information; when the user requests deletion, Hitrontech shall immediately cease such public disclosure, and notify relevant recipient to timely delete the personal information.

- Right to Rectification

Users can manually and proactively rectify the personal information on the App if there is any incorrect or out-of-date information about the individual. In case the App does not provide the function to rectify certain information, the user may provide feedback in the Hitrontech App or contact customer service by email.

- Right to Data Portability

If a user wishes to export all personal information and transfer it to another data recipient for data processing, Hitrontech can assist data extraction for the user.

5.3.3 Security Management during Data Lifecycle

- Data Collection

Hitrontech adheres to the principles of data protection and personal privacy rights. The user's consent for data collection constitutes the legal basis for further data processing. Data collection is performed by protecting the user's Right to be Informed and the necessary principles of the service. All data collection will undergo stringent risk and compliance review by the compliance team during demand assessment or planning design phase before officially initiating R&D process. Meanwhile, the compliance team will conduct DPIA from time to time to perform analytics on sensitive data, ensuring compliance of data collection with applicable laws

- Data Storage
  - Data and File Storage
    - Hitrontech provides different data storage services under various business scenarios. Personal information is encrypted and stored using AES256, and personal sensitive data will be subject to extra AES encryption. Also, certain sensitive data will be desensitized when necessary. At the same time, the key is uniformly secured through the key management system (KMS) and further managed and distributed through the KMS.
  - Data Storage Location
    - Currently Hitrontech implemented 1 data center located at AWS West USA, providing data services for the North America Customers. More server rooms will be made available in the future.

- Multi-copy Redundant Storage

Under the distributed architecture, all servers are deployed simultaneously among three server rooms in different areas of the same city. Databases and other data storage services follow a multiple backup model (keeping a minimum of two real-time copies) that performs real-time backup. It allows high reliability and availability of data and services from the physical perspective.

Hitrontech uses cloud databases for data storage, the default master-subordinate reproduction, the master and subordinate databases are distributed in different availability zones. All disks use local SSD hard disks and support automatic disk expansion. The full and incremental backups of data are all stored on cloud.

For data backup and synchronization across computer rooms, strict data integrity checks will be performed to ensure the integrity of synchronized or backup data.

- Secured Data Processing
  - Data Classification

    Hitrontech implements strict data classification and handling policy internally to specify the scope of data property, identifying principles for classification and relevant persons in charge, and relevant requirements of data governance.

    Hitrontech classifies data according to the source, content and purpose of data, and divides data into different sensitivity levels according to value of data, sensitivity of content, impact and scope of distribution.

  - Access Control Mechanism
    - Hitrontech adopts an access control mechanism relying on the Access Control Platform. Including the unified control of the application and assigning the minimum and least necessary permissions according to the user roles and responsibility.
    - Implement internal approval process for sensitive data operations.
    - Separate the roles of security managers, data operators, and auditors.
  - Data Filtering

    Hitrontech enforces strict verification of the type, length, format, etc. of the data of all entrances to ensure the integrity of the data and not be tampered with.

  - Data Auditing

    Complete data usage records, including auditing records of applications or user operations.

  - Data Desensitization

After collecting personal information, Hitrontech will perform de-identification processing, and adopt technical and management measures to store the de-identified data separately from the data that can be used to restore the identification of the individual and ensure that the subsequent processing of personal information does not re-identify the individual.

- Data Retention Policy

The retention period of personal information is the minimum time necessary to achieve the purpose of providing product and service. Hitrontech will delete or anonymize user data at the request of the customer and return the data to the customer when the data retention policy is triggered. Therefore, Hitrontech has adopted the principle of minimum data retention:

- The retention of user's personal information is limited to the user's express consent so that the personal information can be used for service-related purposes and shall not be used for any additional purposes without the user's consent.
- Data that needs to be retained in accordance with the law, or the company has the ability to prove that it is necessary for business purposes, can be retained within the time specified by a clear data retention schedule.
- Data retained for realizing the legitimate interests of customers or third parties can only be retained when the company has clear contractual agreements or instructions with customers or third parties, such as when providing services to customers or providing services for other purposes.
- According to the principle of minimum data retention, customers have the right to determine data retention strategies and inform Hitrontech in time for service purposes. When customers request to delete data or return data, Hitrontech will follow this clear instruction to execute.

5.3.4 Technical Measures for Data Security and Privacy

- Secured Transmission of Data
  - The integrity of the data transmission

  When the application program processes the data transmission process, including without limitation, device-cloud communications, App-cloud communications, it will perform integrity check, usually using the HMAC-SHA256 algorithm
  - The desensitization and encryption of the data content

AES-256 encryption is utilized in the communication between the APP and the cloud, the communication between the device and the cloud, the communication between the APP and the device, as well as the communication between the device and the device, the sensitive data, including passwords, biometric data, etc., are transmitted after being desensitized by an irreversible algorithm

- Encryption of the Transmission Channel

Hitrontech uses the TLS1.2 protocol for communication channel, the communication between the APP and the cloud, the communication between the device and the cloud, whether it is HTTP or MQTT, and implements strict certificate verification

5.3.5 Organizational Measure for Data Security and Privacy

- The International Data Transfer

With the ever-changing requirements for data security and privacy protection in the international environment, Hitrontech pays close attention to the international dynamics of cross-border data transmission in real time.

In general, Hitrontech strictly follows the general principles of "data localization requirements", and user personal information is stored on the local server to the greatest extent and would not be synchronized to other regions.

- The Access Control for Data Processing Activities

In accordance with the principle of "minimizing data processing access", Hitrontech strictly manages the personnel who have access to customers' personal information, clarifies the division of responsibilities, standardizes data processing procedures, regularly reviews access, and strengthens data security training.

6 Development Security

6.1 Security Demand Analysis and Product Design

During the demand analysis, Hitrontech's security team will analyze the security demands based on the functional requirement, create communications regarding the business content, the business process and the technical framework to form the security demand analysis proposal, and reach a consensus with the business side and the developer regarding such proposal.

During the product design, Hitrontech security team will analyze the system attack surface, establish a threat model and security and privacy risk assessment, analyze the security of technologies to be used in the product design to form the product design security proposal, and reach a consensus with the developer regarding such security proposal.

6.2 Development Stage

6.2.1 Safe Development Standards

During the coding phase, Hitrontech's security team will design a safe development kit for the developer and require the developer to undergo training related to secure coding standard, provide R&D engineers with automatic detection tools and test cases to minimize security risks before submission for testing. Meanwhile, upon completion of each code submission by R&D, automated code audit and open-source component audit will be carried out, and in case of risks, the corresponding developer will be notified immediately to do safe recovery.

Hitrontech security coding standard follows the international coding standards, including the relevant standards of the USA National Standards and Technology Association NIST, the relevant standards of the European Telecommunications Standards Institute ETSI, and the relevant standards of OWASP.

6.2.2 Code Auditing

The code auditing independently developed by Hitrontech is able to accurately locate the high-risk function entry by means of the syntax tree analysis, and do retrograde analysis before use of the function, in order to discover the unsecure uses. Meanwhile, prevailing vulnerability information will be tracked in an automated real-time manner, any third-party component library that is considered unsecure will be automatically updated, and rules will be generated for a vulnerability warning.

At the same time, Hitrontech also integrates the international mainstream third-party code audit tool, which supports Hitrontech's main languages (including without limitation, Golang, TypeScript, C, Python, NodeJS) through this tool, which can effectively help the business to find vulnerabilities.

6.2.3 WEB Vulnerability Scanning

Hitrontech uses a passive scanning proxy server. As long as the proxy is activated and tested, the black box scanner can automatically get the project interface (port) for automated security auditing.

6.2.4 Mobile Scanner

Hitrontech App packaging platform, after completing the new app package, Hitrontech will automatically send the app package to the mobile scanning platform for scanning, which supports both Android and IOS Apps.

6.2.5 IAST (Interactive Application Security Testing)

IAST (Interactive Scan) technology is a real-time dynamic interactive vulnerability detection technology. By combining all RASP node clients in Hitrontech developed services, it collects and monitors the runtime function execution and data transmission of the Web application, and conducts real-time communication with the scanner. Interactively, efficiently and accurately identify security vulnerabilities.

6.2.6 Security Scanning on the Deployment Environment

For the application deployment environment, including ports, domain names, servers, and corresponding images, Hitrontech will conduct baseline security audits and use tools for continuous baseline security monitoring, including unsafe configurations, version vulnerabilities, baselines under compliance requirements, etc., and project-aligned at the same time, the release not only ensures the quality of the code itself, but also ensures the security of the deployment environment.

6.3 Security Test, Fixing and Verification

6.3.1 Security Test

Security testing will be conducted on the running environment, including root detection, jailbreak detection, debugging detection, injection detection, etc. The purpose of testing is to ensure that the client runs in a trustworthy environment to prevent the program from being cracked or exploited by malicious software

During the test phase, the security team of Hitrontech will carry out security penetration to discover vulnerabilities by means of the vulnerability scanning platform and the code audit platform in combination with manual tests. If any vulnerability is found, it will be fixed and specifically tracked through the work order system.

6.3.2 Security Vulnerability and Security Assessment Report

For the release phase, a system can only be released to the online environment after it passes the security test, fix all medium and high risk vulnerabilities, and acquires the security test report, in order to prevent the product from running in the production environment with security vulnerability; the whole system will be reinforced as per the safe online specification during the release process.

7 Operations Security

7.1 Security Risk Management

Hitrontech has an in-house security team taking charge of vulnerability management and discovery, which is able to discover, track, trace and fix security vulnerabilities.

Hitrontech's security team conducts security penetration tests before any business code is online; meanwhile, and periodically conducts black-box testing for online business.

Each year Hitrontech also cooperates with third-party security organizations to complete penetration testing on cloud services, mobile clients and hardware products.

7.1.1 Security Asset management

At Hitrontech, we recognize the critical importance of securely managing the equipment and infrastructure that underpin our cloud application development and operation services. Proper asset management ensures the confidentiality and integrity of our clients' data, even at the end of its useful life.

- Equipment Lifecycle Management

We follow a rigorous process throughout the lifecycle of physical equipment used in our cloud operations, which includes procurement, deployment, and retirement phases. This process ensures that equipment is used effectively and securely.

- Secure Disposal Practices

When equipment reaches the end of its operational life or is no longer in use, we employ industry-standard secure disposal practices. This involves the responsible decommissioning of equipment to prevent data breaches. We ensure that all data stored on the equipment is thoroughly sanitized or destroyed to prevent unauthorized access.

- Reuse and Recycling

We are committed to reducing our environmental impact. Whenever possible, equipment that is no longer suitable for our production environment is assessed for potential reuse. We may refurbish or repurpose equipment, following stringent security protocols to ensure data erasure before reuse.

- Inventory and Tracking

Our asset management program includes robust inventory and tracking procedures. We maintain a comprehensive inventory of all equipment used in our cloud services, allowing us to track its status throughout its lifecycle. This inventory serves as a crucial component of our security and compliance efforts.

- Data Erasure and Destruction

We employ certified data erasure methods to ensure that sensitive data is effectively removed from equipment before disposal or reuse. Our procedures adhere to data protection regulations and industry best practices, providing clients with peace of mind regarding data security.

7.1.2 Security Scan

Perform a full network security scan every month, including WEB site vulnerability scanning, application and service vulnerability scanning, host vulnerability scanning, code component vulnerability scanning, and IAST real-time scanning.

7.1.3 Penetration Test

Penetration testing is a practical demonstration of possible attack scenarios, simulating hackers trying to bypass the security control in Hitrontech network and being able to obtain the highest authority in the system.

Hitrontech conducts at least one internal penetration test every year for Hitrontech staff, organizational structure and IT structure. The test content includes external network penetration, internal network penetration, social engineering, etc.

Meanwhile, the penetration test from the third party may conduct at least once a year.

7.1.4 Security Incident Response

Hitrontech has established and improved its internal network security incident emergency work mechanism to improve its ability to respond to emergent network security incidents, prevent and reduce the loss and harm caused by network security incidents, improve emergency response capabilities, and ensure the safe operation of the company's business.

The security incident response process at Hitrontech aligns with our policy of "proactive prevention, timely detection, swift response, and comprehensive recovery." This process adopts strict classification of security incidents and vulnerabilities. In response to incidents, the corresponding processing and execution procedures are carried out according to the classification, including incident discovery, detection, suppression and eradication recovery, and follow-up summary of the entire incident life cycle.

7.1.5 Security Risk Assessment

In order to maintain the appropriate control objectives and methods under the premise of considering the balance of control costs and risks, and to remediate information security risks at an acceptable level, Hitrontech conducts a risk assessment at least once a year.

The evaluation process is to establish a global modeling view for Hitrontech's existing services, analyze the risk factors in the internal mechanism of the system itself, and discover abnormal and malicious behaviors in the interaction between the system and the external environment, so as to complete the system weakness analysis and security threats, and reduce and control potential or existing risks.

7.1.6 Security Audit

Hitrontech's security team will conduct audits on all security system platforms, tool access, configuration changes, and permission granting processes, and keep all audit records.

At the same time, a set of internal security auditing platform is built, which is connected to the primary internal management system, which can conduct unified audit of all employee access and operation logs, and guarantee the accuracy, completeness and non-repudiation of audit logs.

7.2 Network Security

7.2.1 Network Communication Security

All communications with Hitrontech cloud platform are encrypted with the TLS security protocol including the communication between Device and Cloud, the API interface is also equipped with a full range of TLS. In the meantime, the AES 128 is applied to its content, the key is randomly generated based on each device and a user, ensuring the uniqueness and security of the key, two-layer encryption ensures the communication channel.

7.2.2 Network Isolation and Access Control

Hitrontech has established an internal network isolation rules to realize access control and boundary protection for internal office network, development network, staging network and production network through physical and logic isolation; Hitrontech cloud platform ensures that unauthorized personnel will be prohibited from access to any internal network resource; and all the employees need to pass strict approval and permission control by the Jumpserver before logging in part of the production system and develop routine operation & maintenance, with the entire process being audited.

With regards to the network access isolation for cloud users, Hitrontech provides multiple security mechanisms including virtual-control-level resource access control policy, inter-private network isolation policy in cloud platform, Web console permission distribution and authentication, interface conversation ID and access key, thus to ensure that customers can only have the access to the relevant data generated by their users, and realize access isolation among customers effectively.

7.3 Access Control

Hitrontech implements unified management of system permissions, machine permissions, data permissions and other permissions of the IT system, and realizes a zero-trust permission management model. Based on the types of user identities, application identities, and application functions, it achieves minimal permission control.

7.3.1 User Account Management

- User Account Creation

Customers who require user accounts for our cloud services are requested to initiate an account creation request. This request should include the user's email address and specify the necessary permissions associated with the account. Within 24 hours of receiving the request, we will create the user account, configure the associated permissions, and set up the required access controls. Once the user account has been successfully created, we will promptly notify the customer. This notification will include the necessary account credentials and any additional information required for accessing our cloud services securely.

- User Account Deletion

When a customer determines that a user account is no longer required, they can submit a request for account deletion. This request should include the email address associated with the account to be deleted. Upon receiving a user account deletion request, our team is dedicated to initiating the deletion process within 24 hours. In the event of user account removal, we manage associated data in compliance with applicable regulations. This may include secure archiving or permanent deletion, depending on the customer's specific requirements and legal obligations. Once the account has been successfully deleted, we will notify the customer to confirm that the requested account removal has been completed.

7.3.2 Authentication, Authorization, Accounting

The system permissions mainly include internal system platform permissions, application permissions, and machine permissions. The authorization of system permissions follows the "principle of minimum privilege", that is, to assign each authority role and only assign the "essential" authority needed to complete the task or operation. At the same time, the system strictly records all audit records for changes in permissions.

- MFA: Hitrontech has implemented Multi-Factor Authentication (MFA) to further enhance the security of privileged accounts. This ensures that even if credentials are compromised, unauthorized access is significantly more challenging.
- SSO: Regarding the identity authentication of the internal system, Hitrontech has implemented single sign-on (SSO) for all internal applications. Additionally, this SSO mechanism is extended to integrate seamlessly with the authentication systems of our customers and third-party cloud services. This unified authentication approach simplifies access control and enhances user convenience by allowing users to authenticate once and access multiple systems and services without the need for repeated login credentials.
- ACL: Hitrontech has a unified authority management system (ACL) for the access verification of the internal system, which realizes the authorization of applications, application functions and data. There is a complete approval process management on the platform.

7.3.3 Access Control on Machines

Hitrontech employees are required to obtain authorization before accessing the cloud machines. Once authorized, they can log in to the Jumpserver to control limited access to the machines. Throughout the authorization approval process, machine login sessions, executed commands, file transfers, and other activities, there is a comprehensive audit trail in place to ensure accountability and security.

7.3.4 Access Control on Applications

Hitrontech enforces unified management and control of permissions through Role-Based Access Control (RBAC) for each individual application and interactions among applications. This approach ensures that access to resources and functionalities is systematically regulated based on user roles, streamlining security and access management throughout the ecosystem.

7.3.5 Access Control on Database

Hitrontech's database authority management mainly includes: application accounts, database platform accounts, etc. The application account refers to the account provided for the application to access the database, and the identity authentication is realized by identifying the machine where the application is located.

The accounts used by the database platform are specially created by the DBA, including read-write permission used to execute work orders and read-only accounts used by query modules. The database platform accounts are rotated every 3 months.

7.3.6 Access Granting

Hitrontech employees have a unified management platform for access permission application and approval. The approval of the corresponding supervisor, operation and maintenance, security and application person in charge is required to complete the authorization. Approval is granted based on below criteria:

- Job Role Relevance: Employees are granted access aligned with their job responsibilities. Access privileges are strictly based on the principle of least privilege, ensuring that individuals have access only to the data required to perform their duties.
- Customer Authorization: In cases where data access involves customer information, access is granted only after receiving explicit authorization from the respective customer.

Upon approval, access is provisioned based on the principle of least privilege, granting the necessary permissions and restricting unnecessary privileges.

7.3.7 Access Revocation

At Hitrontech, we conduct regular access reviews to verify that existing access aligns with current job roles and business requirements. Any discrepancies or redundant access privileges are promptly identified.

When an employee changes roles, leaves the company, or when access is no longer necessary for their responsibilities, access revocation procedures are initiated immediately. Revocation is swift and comprehensive, ensuring that former employees or individuals no longer requiring access are removed promptly from all relevant systems and data repositories.

Continuous monitoring and auditing mechanisms are in place to detect any unauthorized access attempts or anomalous activities. This enables proactive identification and swift action in case of any breaches or unauthorized access.

7.4 Security Management of Service Provider

7.4.1 Risk Assessment of Service Provider

Hitrontech has formulated a screening mechanism and regular evaluation mechanism for platform software vendors. In addition to the security indicators of hardware products and the security standards of software services, Hitrontech needs to have a deeper understanding of the practices of various service providers in information security assessment and privacy compliance. The information security assessment involves security penetration testing and supplier security capability assessment.

With the help of privacy compliance assessment tool, we first adopt the standard version of the security and privacy compliance questionnaire to conduct a standardized assessment of third party. When a third party has a non-compliance item which impact the service, it without any doubt shall be resolved before the service commences, otherwise they will not be allowed to enter the third party's list.

7.4.2 Monitoring of Service Provider

Real-time monitoring over the service quality, paying attention to the third parties security management, etc., so that Hitrontech can respond quickly when abnormalities occur.

7.4.3 Customer Security Service Support

The complete operation security capability of Hitrontech cloud platform is able to provide customers with 24x7 technical support on cloud services.

7.5 Change Management

Hitrontech follows a well-defined change management process to ensure that all changes, whether they involve updates, modifications, or configurations, are executed in a controlled and secure manner to minimize risks and disruptions to our clients' cloud environments.

Our change management process begins with the identification of the proposed change, followed by a thorough assessment of its potential impact on security and service continuity. Changes are subject to a rigorous review and approval process, involving key stakeholders and subject matter experts. Once approved, changes are systematically tested in a controlled environment to identify and mitigate any unforeseen issues. Throughout the process, comprehensive documentation is maintained to track the change's progression from inception to implementation. Regular reviews and post-implementation assessments are conducted to ensure continuous improvement and adherence to our stringent security standards

7.6 Business Sustainability

To eliminate the interruption to key production and operation activities, and protect them from the impact of major failure or disaster, Hitrontech monitors all hosts, applications, services, networks and the like of the cloud platform through the O&M platform, and has a complete set of automatic process systems and guarantees for business failure; and a hot switch of multiple services guarantees that the service will not be interrupted.

A complete set of counter-measures has been developed for risks incurred by the software and hardware failure of the business system or even force majeure such as natural disasters, in order to guarantee the business sustainability under predictable conditions.

7.6.1 Disaster Recovery

Security, reliability and sustainable availability of business data are guaranteed by means of master-slave data real-time hot backup, redundant storage and multi-place backup. The backup is monitored and verified in real time manner.

7.6.2 Emergency Plan

Hitrontech has developed internal emergency plans and measures for various assets and security risks, in order to guarantee the correct, orderly and efficient afterward emergency handling, and guarantee the normal operation of works. The emergency plans include prior pre-plan procedure, monitoring and a series of fault secure measures. During the incident, providing sufficient data for subsequent handling by means of detailed system monitoring review records is helpful to quick understanding and analysis, as well as corresponding interface personnel. After the incident, there is a complete set of handling procedures and emergency pre-plans to guarantee the rapid handling and analysis of problems as well as the responsibility investigation.

7.6.3 Emergency Exercise

Hitrontech regularly carries out internal technical emergency tests and drills regarding large hardware failure, network DDoS, security incident and the like.

7.7 Clock synchronization

An incorrect time setting can lead to significant adverse effects in various domains, such as data processing, scientific computing, and transaction processing. Inaccurate system time can result in unreliable timestamps, security token issues, synchronization failures, and application errors further up the pipeline. At Hitrontech, we employ a time synchronization service delivered through the Network Time Protocol (NTP). This service leverages a network of redundant satellite-connected and atomic clocks in each region to provide highly precise time derived from these accurate reference clocks.