agora

# Security Whitepaper

agora.io

# Contents

# Introduction

Agora is committed to providing developers with a ubiquitous, real-time engagement (RTE) platform as a service (PaaS)—allowing everyone to interact with anyone, anytime, anywhere. Agora has designed a proprietary global network for audio and video transmission and interaction— we call it SD-RTN™ (Software Defined Real-time Network). In conjunction with our SD-RTN™, Agora provides unified, standardized API and SDK solutions for various industries and use cases across many popular operating systems and platforms. Developers can easily build safe, reliable, and high-quality RTE experiences by integrating the Agora SDK into their systems or applications to add functionality like video and voice call, real-time messaging, recording, and interactive live streaming.

As the industry pioneer, and the world's leading RTE service provider, information security, legal compliance and data privacy are top organizational priorities for Agora. Data privacy by design and by default are essential considerations when building RTE capabilities. The purpose of this paper is to outline Agora's efforts and the attributes of the platform that address security, compliance and privacy—so that developers can use the Agora RTE service with peace of mind.

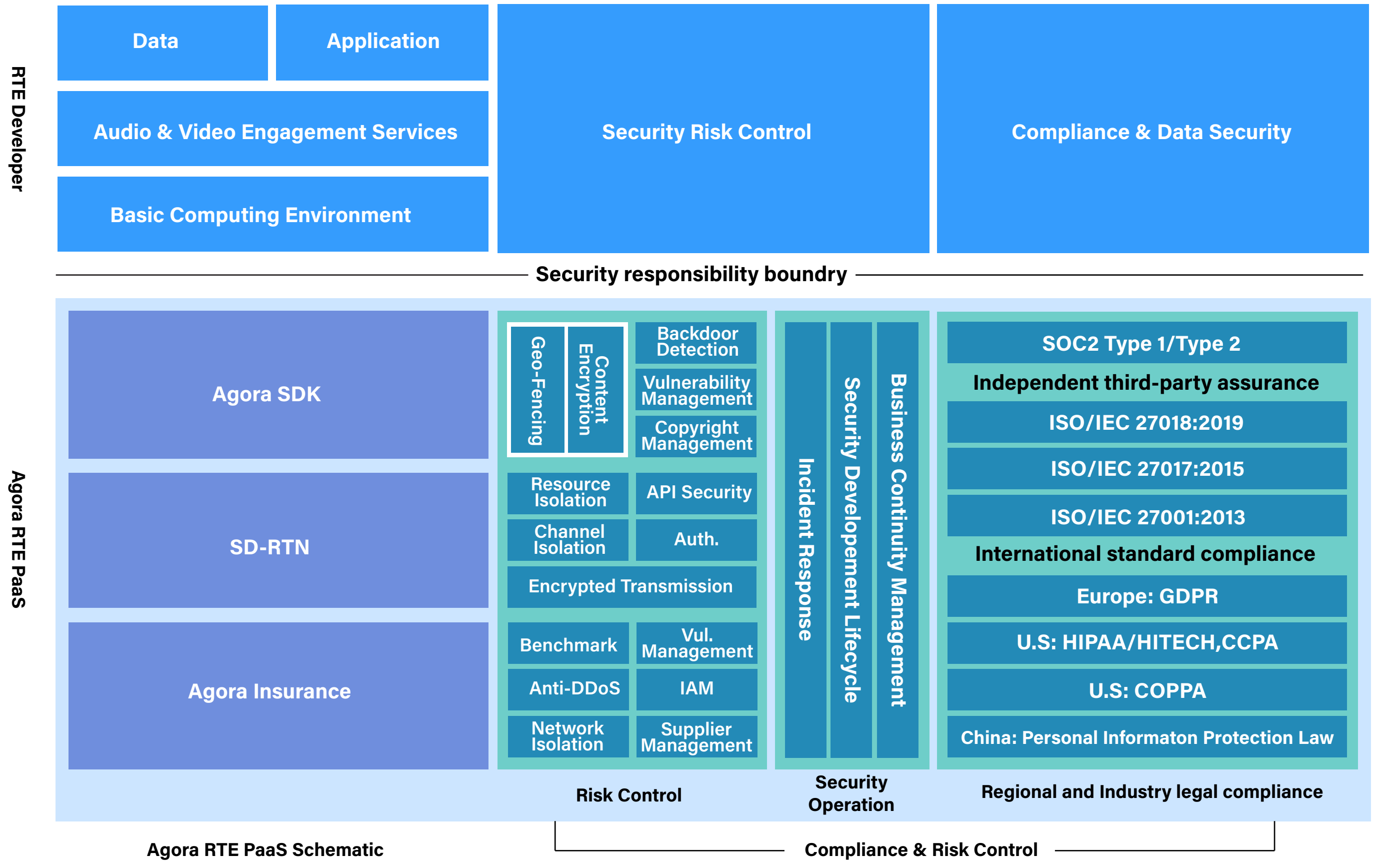
In this paper we will systematically explore the attributes of the Agora RTE platform, and the efforts of the company, related to security, compliance, privacy, and data processing.

# 1. Shared Security Responsibility

Agora relies on the cooperation of customers in a joint effort to continuously improve security.

In order to help developers understand security responsibilities in complex RTE scenarios, we have created this sharing model:

### Security Responsibility Sharing Model



RTE Developer

Data

Application

Audio & Video Engagement Services

Basic Computing Environment

Security Risk Control

Compliance & Data Security

Security responsibility boundry

Agora RTE PaaS

Agora SDK

SD-RTN

Agora Insurance

Geo-Fencing

Content Encryption

Backdoor Detection

Vulnerability Management

Copyright Management

Resource Isolation

API Security

Channel Isolation

Auth.

Encrypted Transmission

Benchmark

Vul. Management

Anti-DDoS

IAM

Network Isolation

Supplier Management

Incident Response

Security Development Lifecycle

Business Continuity Management

SOC2 Type 1/Type 2

Independent third-party assurance

ISO/IEC 27018:2019

ISO/IEC 27017:2015

ISO/IEC 27001:2013

International standard compliance

Europe: GDPR

U.S: HIPAA/HITECH,CCPA

U.S: COPPA

China: Personal Informaton Protection Law

Risk Control

Security Operation

Regional and Industry legal compliance

Agora RTE PaaS Schematic

Compliance & Risk Control

🟦 RTE Developer's Security Responsibility

⬜ Agora Security Responsibility

Agora manages and controls the security of our RTE platform (PaaS) and SDK. Customers need to manage and control the security of their own applications and system environments. Also, based on their own needs, customers must properly configure the security settings of the Agora SDK to ensure the security of their own information, platform, program, system, and network.

# 2. Security Compliance and Privacy Protection

Compliance and privacy protection are top priorities of the Agora RTE service. Agora is dedicated to offering a platform that always complies with domestic and foreign privacy regulations, including the European Union GDPR, the United States CCPA, HIPAA, COPPA, and the Personal Information Protection Law of China.

In service of the above goals, we have established a dedicated Privacy, Compliance and Information Security teams that have constructed a series of policies, workflows, and systems used to protect customers' personal information. To ensure that privacy and security are implied by default, we adhere to privacy by design (PbD) principles and all products undergo rigorous security evaluation. We handle all personal data in strict accordance to the privacy protection laws of the country and/or region.

Agora also employs technical measures to protect customers' personal information and avoid unauthorized access, modification, disclosure, and/or abuse of personal information. Our voice and video SDK provides a built-in encryption algorithm, and the network communication with customers (over our SD-RTN™) is protected by an encrypted transmission protocol. Agora does not read any encrypted content or associate it with a specific customer.

We are committed to the employment of international standards and best practices in the continual evolution of our security management system. In addition to ensuring our own product security and compliance, we provide compliance support to our customers—to help them comply with applicable laws and regulatory requirements.

Agora has not only obtained a series of internationally recognized information security and privacy management system certifications (including ISO/IEC 27001, ISO/IEC ISO27017, and ISO/IEC 27018) but we have also earned SOC2 TYPE II certifications issued by an independent third-party auditor. The following tables summarized these certifications:

# Table1 ISO Certifications

| Certification | Issued by | What This Means to Customers | Scope of Application |
|---|---|---|---|
| ISO/IEC 27001:2013, Information Security Management System | DNV | Agora has sufficient information security risk identification and control capabilities, and we can provide safe and reliable products and services to customers around the world. | ▪ Regions of Agora's RTE nodes: Europe, North America, Asia, Africa, Oceania, and South America.<br>▪ Customers of industries: online education, social pan-entertainment, interactive games, Internet healthcare, online finance, e-commerce, live broadcast, video conferencing, smart hardware, etc.<br>▪ Components of Agora's RTE: real-time engagement products, modules, systems and services (e.g., SD-RTN™, video and voice call SDK, real-time messaging SDK, recording SDK, interactive live streaming SDK, and Argus).<br>▪ Process and life cycle of the Agora RTE solution and operation: Research and Development, Quality Assurance, Operation, Customer Support, Technical Maintenance, Data Processing, etc. |
| ISO/IEC 27017:2015, Information security controls applicable to the provision and use of cloud services | DNV | Agora RTE PaaS services have adequate information security management and support capabilities. | |
| ISO/IEC 27018:2019, Based on ISO/IEC 27002, provides a set of personally identifiable information (PII) protection guidelines and security control measures applicable to public clouds | DNV | Agora has established a personal information protection system to protect users' personal information in terms of privacy and the data life cycle. And we protect corporate data and users' personal information to meet industry-recognized standards of practice. | |

## Table2 SOC2 Reports from Third-Party Compliance Auditor

| Certification | Status | What This Means to Customers |
|---|---|---|
| Type II | Obtained | ▪ Agora has established and implemented effective internal control, which can continuously and effectively guarantee the security, availability, confidentiality, and privacy of various products and services.<br>▪ Agora is regularly audited by third-parties to verify the products and services meet the audit standards. |

# 3. Agora RTE Platform Security

Real-time interaction depends on strict assurances of security across the RTE platform. In the Internet environment, these security assurances are necessary to keep the services available and protect customer data.

As we continue to evolve our RTE service offering, we are committed to the ongoing assessment of technical risks related to platform architecture and have fully integrated security risk control and standards compliance into all aspects of platform construction, implementation and operation.

The Agora RTE platform is principally comprised of the infrastructure later, the SD-RTN™, and the Agora SDK. In this section we discuss the security risk control measures associated with each layer of technology and operations.

## 3.1 Infrastructure Layer Security

Agora infrastructure is composed of more than two hundred private, strategically located, internet data centers (IDCs), working in combination with virtual public cloud (VPC) services from leading pubic cloud providers, to provide a unified computing environment that is highly vailable, scalable, efficient, and secure.

### 3.1.1 Security Management of Devices in Private IDCs

The daily management of the devices in our private IDCs are coordinated and supported by the entrusted data center operators. In accordance with the RTE service requirements, Agora has formulated a complete set of data center supplier management specifications. The specifications define the management methods and service implementation standards that the suppliers must comply with. In brief, the suppliers are responsible for the physical environment security, power protection, daily inspection, physical redundancy switching, abnormal monitoring and reporting, etc.

We only select suppliers that have obtained ISO27001 or equivalent/higher certification and we confirm that they meet all Agora security requirements in these areas:

- Access management
- Risk management
- Incident response
- Network security
- Alert monitoring
- Disaster Recovery

Before putting our IDC devices into service, we perform a unified initialization process. When running these devices, we collect real-time operating status-related data, such as OS load, and network flow.  We also configure service incident alerts on our monitoring platform. In the case of an alert, a 24/7 Agora operations team will respond to it, handle exceptions, and quickly recover the service. Before any devices are taken offline we implement data encryption processing and then suppliers are instructed ship them to Agora's centralized processing environment. As the final step, we will either seal or perform physical destruction after erasing data and configurations.

### 3.1.2 Network Isolation

One of the prerequisites for network security is efficient network isolation. Based on differences in RTE platform functions, we divide the network into several security groups, including Core, Edge, and IT. In each of these groups, different routing and strict access rules are implemented according to service requirements and security levels. To achieve a unified network isolation capability, we program the network security rules directly into our network hardware switch in our private IDCs to give an extra layer of security. We complete these rules on the switch in our private IDCs based on the virtual private cloud (VPC) security group while in the public cloud

## 3.1.3 Anti-DDoS

Distributed denial-of-service (DDoS) attacks can have a significant impact on RTE services including quality degradation or in some cases service interruption. To ensure the availability of the Agora RTE platform, we have deployed a DDoS defense solution for our core services via the capabilities of public cloud vendors. The solution can automatically detect an attack and then schedule and call the DDoS mitigation function, which can be completed within a few seconds. The 24/7 Agora security team is notified of any DDoS attacks so that they can monitor and make the best response decision.

## 3.1.4 Host, Database and Middleware Security

Services in operation depend on the guarantee of computing resources—background programs, caches, databases, and other middle ware. This guarantee is satisfied by rational scheduling and allocation of CPU, memory, disk, etc., via the system operation or container.

### 3.1.4.1 Security Hardening

We have formulated a series of security baselines for our private IDCs and VPCs that cover operating systems, containers, databases, storage, web services, etc. These baselines address account security, identity, authentication, minimum authorization, log audit, and clock synchronization. In practice, we implement security hardening on these baselines based on a number of factors including the type of device or service, asset level, and use, in order to ensure that our computing resources meet our security requirements. We also conduct regular configuration inspections of the resources and compare with the baselines to identify any potential vulnerabilities. If any vulnerabilities are detected, the security operations team notifies the associated business, technical, or operation teams to implement necessary changes.

### 3.1.4.2 Vulnerabilities Management

All Agora computing resources are carefully analyzed for security vulnerabilities. We collect the version information of  components into the security operation system for centralized analysis to identify whether a package or service is affected by any known vulnerabilities. As for the hosts on the public cloud, security agents are also deployed to for real-time vulnerability detection. In addition, the security team regularly scans the assets both in our IDCs and in our VPCs on public clouds, reviews the reports, and logs issues into the security incidents and events management system. If a vulnerability is identified, the security team provides a comprehensive assessment of the risk—offering treatment measures and fix suggestion. The security team works with business, technical and operations teams to conduct the necessary repair, security hardening, and image updating.

#### 3.1.4.3 Security Operation of Infrastructure

**Operation Account Security**
In daily operation and maintenance, we have put in place an identity and access management (IAM) mechanism. The identity of all operators must be verified and authorized before they can perform any system changes. Additionally, these accounts are correlated to the employee identities of operation teams, and multi factor authentication (MFA) is enabled by default.

We have also created a set of strict controls for the use of public cloud service APIs. Programs can only be accessed via an authorized access key or assumed role credentials. Passwords or access keys associated with the root account are not permitted.

**Operating System Account Security**
Operating system account security includes the use of strong passwords with regular rotation and the security team carries out regular inspections.

**Operation Auditing**
We record and archive all operation and maintenance processes in real-time. Policies and metrics are in place that trigger an alarm the moment a risk operation is detected.

## 3.2 SD-RTN™ Security

Agora's SD-RTN™, the world's largest software-defined real-time network, is specialized for real-time, audio and video interaction. Its main benefits are ultra-low latency, high-quality transmission, and support for millions of users—interacting in real-time. As one of the Agora RTE platform's core services, SD-RTN™ supports RTE terminal source access, authentication, authorization, intelligent routing, real-time scheduling, and real-time transmission.

In order to ensure the compliance and security of RTE services, we built the architecture of SD-RTN™ in full consideration of internet threats. SD-RTN™ provides customers with secure and stable services through the following control measures:

### 3.2.1 Resource Isolation

SD-RTN™ allocates dedicated resources for each RTE project to ensure that it is independent of other project resources, and SD-RTN™ provides secure and reliable resources for access, computing, and transmission. Customers need only to perform simple configuration on the Agora customer console. When an RTE project is created by a customer, we will automatically assign a unique App ID to the project, and allocate the related resources. Simultaneously, the SD-RTN™ performs resource isolation based on the App ID.

### 3.2.2 Channel Isolation

We create an independent, isolated, channel for each type of audio, video, or message data transmission. All channels are logically separated; only users with the same App ID for audio and video interactive applications, and the same channel name, can join a given channel. When a user starts up a session, the channel is created. When the session ends (the last user leaves), the channel is destroyed.

### 3.2.3 Encrypted Transmission

In order to ensure the confidentiality of the transmission process, the SD-RTN™ uses Agora Universal Transport (AUT). (a custom transmission protocol based on TLS 1.3) to provide encryption guarantees for the RTE transmission links. AUT is globally enabled, by default, on the Agora RTE platform.

### 3.2.4 Authentication

When RTE application users access the Agora RTE platform, we provide a service of generating dynamic tokens based on the App ID. with the App Certificate for authentication, in order to help customers  perform strong authentication on their users when needed. To use the dynamic authentication service, customers need to first configure it in the console.
For more detailed information, see "Security Best Practices" at
https://docs.agora.io/en/Agora%20Platform/security_practice?platform=All%20Platforms.

## 3.3 SDK Security

Agora provides RTE SDK support for platforms such as iOS, Android, macOS, Windows, Linux, applets, and the web, to meet the real-time engagement needs of customers under a variety of circumstances. The Agora RTE SDK not only provides customers with a simple, easy-to-use, unified, credible, and secure development kit, but it also  provides customers with compliant and secure configuration options. The aim is to optimize customers' real-time engagement scenarios in a compliant manner with the ability to quickly identify and completely respond to any threats against source data.

### 3.3.1 SDK Security Features

When Agora provides SDKs to customers, security is one of our primary guarantees. When adding features or iterating versions of an SDK, Agora fully evaluates the risk points of functional requirements, in terms of compliance, privacy, and security. All code is carefully audited rigorously tested for quality assurance. Where quoted or integrated third-party code is integrated, Agora thoroughly evaluates penetration testing reports looking for malicious code or back doors. We also ensure copyright and use agreement compliance. If any risks are detected, the publishing process is suspended until all vulnerabilities have been patched and any bugs fixed.

### 3.3.2 Content Encryption and Geo-Fencing

In order to assist our customers improving data security, compliance, and privacy in RTE scenarios, Agora provides data source encryption and geo-fencing options.

#### 3.3.2.1 Content Encryption

The Agora SDK supports data-level encryption of all audio streams, video streams, and messaging using AES 128/256 symmetric encryption algorithms. The encrypted data is transmitted to other nodes in the channel via the Agora SD-RTN™. At the receiving end, it is decrypted by the application and then forwarded to the media stream renderer. The encryption key is known only to the application developer and is not sent to the Agora server.

#### 3.3.2.2 Network Geo-Fencing

In order to meet the legal and regulatory requirements of different countries or regions, the Agora platform supports network geo-fencing so that customers have complete control over the countries and regions where their data might pass through. Customers can configure and enable geo-fencing in the SDK according to their needs.

Refer to the development documentation here to enable these functions in their configurations.

## 3.4 Web API Security

Customers manage their projects and channels by calling the RESTful APIs of the console on the Agora RTE platform, This documentation can be found at https://docs.agora.io/en/rtc/restfulapi/

To protect the APIs, we not only use WAF solutions, but also implement the following control measures:

### 3.4.1 Identity Authentication

Before using the Agora RESTful API, customers need to log in to the Agora console (https://console.agora.io/) and create a key and secret pair. Subsequent API calls require the corresponding key-and-secret-pair. This ensures secure separation of different projects and applications.

### 3.4.2 Transmission Security

Restful APIs support only the HTTPS protocol ensuring that all communication is encrypted with SSL/TLS—protecting both the API credentials and transmitted data. This also works to prevent man-in-the-middle and other attacks.

### 3.4.3 API Call QPS Limit

The queries per second (QPS) of API calls are limited in order to ensure that normal user requests can be responded to—and to refuse malicious users.

### 3.4.4 Input Verification

To avoid common vulnerability flaws (SQL injection, remote code execution, etc.), Parameters requested by user calls are verified and filtered by the server.

### 3.4.5 Output Encoding

The server adds security options (Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, etc.) to the headers of responses to increase protection.

# 4. Data Security

It is important to process data legally, compliantly, and securely—and this is one of our chief concerns. This section outlines our policies on data security and management, and the technical control measures in place to support them.

## 4.1 Organization of Data Security

We have established a Data Security and Privacy Committee (DSPC) to focus on the data security and privacy protection policies in our platform and services. This committee supervises the implementation of policies, procedures, and precautions, and is charged with promptly addressing any data security technology and privacy compliance issues. The DSPC consists of personnel from teams and departments of Security, Legal Affairs, data platform, and management. In addition, we have a Data Protection Officer (DPO) to be responsible for data classification, privacy compliance, and protection.

## 4.2 Policy of Data Security

Ωn response to the increasing severity of network security threats and the gradual tightening of regulatory requirements, we have integrated data security into the process of security system construction, focusing on:

- Confidentiality: To prevent unauthorized access and eavesdropping
- Integrity: To prevent malicious tampering and forgery of data
- Availability: SD-RTN™ supports the high data availability

In addition, all Agora employees:

- Sign confidentiality agreements
- Undergo regular information protection, privacy compliance and confidentiality awareness training

Additionally, all employees with access to any platform systems or data receive advanced security training arranged by the Information System Support Center, which is responsible for the normal operation and maintenance of the operating platform and services.

## 4.3 Data Gathering

We adopt the principle of minimal data collection and only collect  data fields that are 1) necessary in order to conduct business and 2) authorized and agreed to by the customer. User data collected by Agora customers, such as login credentials and payment information, is managed entirely by Agora customers themselves. This user information is not stored on the Agora platform.

## 4.4 Data Masking

In order to protect data privacy, we display only desensitized corporate and personal information in the Agora console. This strategy is also applicable across the platform internally, including Agora's internal management platform, log printing, monitoring alarms, and all other places where data is displayed.

## 4.5 Data Protection and Encryption of Transmission

Data protection is at the core of the Agora RTE security strategy. Within our RTE platform, SD-RTN™ offers additional data security, you can find more detailed information in "3.2 SD-RTN™ Security." For solutions that do not rely on SD-RTN™  (such as like Web SDK, cloud recording, content approval, and transcoding), we offer a different encryption method.
In these cases, encryption is dealt with by the WebRTC standard and interoperability with Agora is completed using our encryption engine (the key has been safely transferred to the Web SDK server via API). For more information about WebRTC security, see

https://webrtc-security.github.io.

## 4.6 Data Usage and Storage

We strictly separate the Production, Testing, and Development environments. Real data is not used for development or testing. In production, if a customer makes use of recording features provided by the Agora platform, those recordings are always stored on the customer's servers and never stored on Agora servers.

As for the stored information, we establish data backup and storage policies in accordance with relevant regulatory requirements. When processing applications from customers, we will cooperate with the implementation of data cleaning or transfer according to the corresponding regulatory requirements authorized by customers. For more details about Agora's data collection and usage, see our privacy policy (https://www.agora.io/en/privacy-policy/) and information security instructions (https://docs.agora.io/en/Agora%20Platform/security?platform=All%20Platforms).

## 4.7 High Availability of Data Service

Customers who use Agora's network (SD-RTN) are provided with highly available RTE data services that include these features:

- Mass data centers: Multiple data centers are deployed around the world to provide services, and any data center attack will not affect the normal operation of other data nodes, thus ensuring the stability of the overall service.

- Fault self-healing: If the server fails due to malicious attacks, such as denial of service (DoS), we automatically isolate the faulty machine to ensure that the service is not affected.

- DDoS prevention: We have configured anti-DDoS services in each core cloud data center, and we have deployed more than 200 distributed data centers around the world to prevent and control DDoS security risks.

# 5. Security Operation

Security is a continuous process. In consideration of the characteristics of the RTE platform, we have developed security operations through these dimensions:

## 5.1 Security Development Life Cycle

Security and privacy related requirements are a must in our software development life cycle.

Based on the security development life cycle (SDLC), we combine the concept of DevSecOps with more automatic methods and tools to efficiently perform security and privacy checks.

### 5.1.1 Threat Modeling

At the stages of Design and Architecture, we use threat modeling to identify potential security issues and then implement response measures designed in to detect these risks earlier. To effectively identify and solve the risks, we refer to the STRIDE threat modeling method, and focus on minimizing the attack surface, basic privacy, minimizing permissions, default security, and data encryption.

### 5.1.2 CI/CD Black Box and White Box Detection

In the Testing stage, we pay close attention to the built-in security protection mechanisms advocated by DevSecOps. To improve our risk detection capability, we have integrated both black box and white box testing tools at the CI/CD steps—including SonarQube (an open-source code scanning tool), Black Duck (a commercial components and compliance scanning tool), and MobSF (and open-source mobile security framework).

## 5.2 Anti-Intrusion and Security Monitor

In order to implement defense in depth to respond to threats, we collect logs for security analysis (within the scope of minimum authority). These logs are used by our real-time security monitoring and analysis platform. When an abnormal event is detected, we alert the Security Operations team and instruct them to expand the correlation and traceability analysis. If an incident is confirmed, it is dealt with according to the emergency response mechanism. The team continues to monitor to ensure the security and availability of business systems.

## 5.3 Emergency Planning and Response

In accordance with the characteristics of RTE services, we have classified and graded service types and formulated different incident classification standards by systematically identifying threats and assessing risks. At the same time, matched response timeliness and handling procedures are implemented to ensure that incidents are dealt with in a timely and effective manner. In brief, our response process is as follows:

Anomaly Detection → Incident Confirmation → Event Suppression → Event Handling → Root Cause Analysis → Final Report

## 5.4 Business Continuity Management

Low latency and high quality require high availability of the Agora RTE platform. To ensure that we can provide continuous (24/7) RTE services to customers, we have established a professional and efficient team responsible for continuity support and management.

### 5.4.1 Real-Time Monitoring

We have built a set of unified monitoring tools to inspect the status and resource level of system components, including middleware, computing load, databases, and network devices, for each service. Once an exception occurs, automatic alarms trigger message robots to inform the on-duty teams to restore services and ensure availability.

We also maintain a centralized and quantitative display of core service indicators that allows us to monitor the overall service situation in real-time. This enhances our ability to make timely and reasonable expansion decision on the use of business resources.

### 5.4.2 Disaster Recovery and Redundancy

When designing the RTE platform infrastructure, we considered extreme computing load scenarios and built the appropriate redundancy into our internet data centers. To guarantee the availability of our basic resources in emergencies, we have combined our IDCs with the leading public cloud services. The hybrid cloud model is an important measure for the high availability of the Agora RTE PaaS.

### 5.4.3 Continuity Drills

To ensure the continuity and effective operation of the most important RTE services, we regularly carry out emergency drills on the network, computing loads, middleware, business systems, etc. We review and analyze the results and data of every drill to aid in the optimization of technical architectures, processes, and emergency plans.

# 6. Security Culture

Information security is a systematic project that not only requires the support of the company's strategic level, but also the participation of all employees. Ultimately, information security is dependent upon the cooperation of customers, third-party organizations, and individuals in the industry ecosystem. Agora fully integrates this understanding into daily operations and management processes.

## 6.1 Security Organization

We have fully recognized the strategic position of information security and its supporting role in the company's long-term business development, and we have built an independent information security team to be responsible for the construction and improvement of Agora's security capabilities. We have also established these virtual internal organizations:

- Information Security Management Team
- Security Compliance and Privacy Team
- Security Internal Control Team
- Data Security Team

These teams work across technical, management, and legal to ensure that information security can be coordinated globally (from the strategic level) and that security policies can be effectively transmitted, step-by-step, to ensure that security measures are implemented.

## 6.2 Employee Security

Agora attaches great importance to contributions of employees to our product, culture, and success—and as an essential part of our security efforts. To ensure that employees share Agora's values and ethics while meeting information security requirements, we have integrated security and ethics to every part of the employee life cycle—from recruitment and onboarding through training and resignation.

### 6.2.1 Recruitment

Candidates are professionally vetted by a background check organization before being hired. We check education, previous employment, external references, criminal records, credit rating, immigration status and other information where local labor laws or statutory regulations permit.

### 6.2.2 Onboarding

Our new employee onboarding process places emphasis on the Employee Code of Conduct and understanding the requirements of our information security management. Depending on job requirements, we may execute confidentiality agreements. Employees in positions involving important data or consumer information, are required to sign the highest level of confidentiality agreement and we ensure that they fully understand the security responsibilities.

### 6.2.3 On the Job

Employees on the job are required to participate in online security and privacy protection awareness training. This training includes GDPR, HIPAA and other laws and regulations as well as daily office security awareness. Employees must pass exams. Additionally, Agora periodically organizes security and privacy related educational events.

### 6.2.4 Resignation

Employees who have resigned must hand over or close their physical and logical access rights in accordance with the established resignation process. We will audit the execution of the confidentiality period in accordance with the confidentiality agreement signed by the employees, and we will clearly inform them of their post-employment responsibility for information security and confidentiality. Employees in key positions need to sign non-competition agreements as appropriate upon hire. The resignation process requires work handover, data cleaning, and passing an audit.

## 6.3 Security Collaboration with Outside Resources

Our goal is to provide customers and developers with a secure and reliable RTE service platform. To this end, we also work with third-party security vendors, such as Trustwave and BishopFox, to conduct outside penetration tests, code reviews, and reverse engineering. These resources enhance our ability to identify vulnerabilities and risks—thereby improving Agora's overall service security and system robustness.

We also attach great importance to input from customers, security research communities, white hat teams, etc.. We have created the Agora Bug Bounty Program to receive input on potential security vulnerabilities and/or security risks. To learn more about the Bug Bounty Program, visit this page: https://docs.agora.io/en/Agora%20Platform/bug_bounty

Any security-related vulnerabilities, suggestions, etc., can also be submitted to us through this address: security@agora.io

# Summary

Agora's goal to provide customers and developers with a compliant, highly secure, and highly reliable RTE platform, is foundational to our company culture and underpins all decision making related to our architecture, product, and service offering. To this end, Agora:

- Systematically promotes the implementation of information security policies related to personnel, technology, and management processes.
- Fulfils all regulatory compliance obligations including ISO/IEC 27001, 27017, 27018 and SOC 2 security standards and privacy regulations like GDPR, CCPA, and HIPAA.
- Works closely with partners, customers, and other parties to stay on the cutting edge of intelligent, highly-efficient, security protection capabilities.

In the increasingly complex Internet environment, with new threats emerging every day, it is essential to choose an RTE platform that can ensure security and privacy for your company and your users. Agora is dedicated to its duties of ensuring the continuity of RTE services while defending the legitimate rights and privacy of all RTE end users.