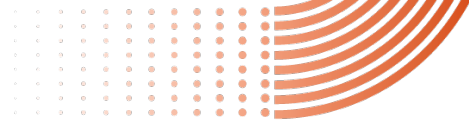


ThroughTek Information Security White Paper



Revision

Version	Amendment	Author	Issued Date
1.0	Initial Issue	Kate Huang	2023/6/30
1.1	Content optimization and security description adjustments	Kate Huang	2025/8/12

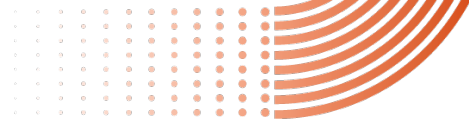


TABLE OF CONTENTS

1. THROUGHTTEK (TUTK) INTRODUCTION.....	3
1.1 INTRODUCTION OF KALAY CLOUD PLATFORM.....	4
1.2 KEY FEATURES OF KALAY CLOUD PLATFORM.....	5
2. SECURITY RESPONSIBILITY ATTRIBUTION.....	6
2.1 RESPONSIBILITY ATTRIBUTION.....	6
2.2 TUTK SECURITY RESPONSIBILITY.....	7
2.3 CUSTOMER SECURITY RESPONSIBILITY.....	7
3. TUTK INTERNATIONAL COMPLIANCE AND CERTIFICATION	8
3.1 ISO/IEC 27001	8
3.1.1 ISO/IEC 27017	9
3.1.2 ISO/IEC 27018	10
3.2 GDPR (GENERAL DATA PROTECTION REGULATION).....	11
3.3 CCPA (CALIFORNIA CONSUMER PRIVACY ACT)	12
3.4 Other Information Security and Privacy Protection Measures	13
4. TUTK TECHNICAL SAFETY COMPLIANCE	15
4.1 SECURE DEVELOPMENT PRACTICE :	15
4.2 AUTHENTICATION MECHANISMS AND ACCESS CONTROL :	16
4.3 CLOUD SERVICE STORAGE :	16
4.4 APPLICATIONS :	17
4.5 DATA TRANSMISSION :	17
5. PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT)	19

1. THROUGHTTEK (TUTK) INTRODUCTION

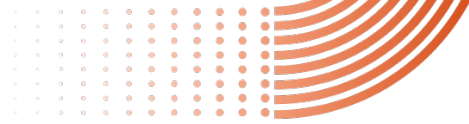
ThroughTek Co., Ltd. (6565.TW, hereinafter referred to as TUTK or the Company) was established in Taipei, Taiwan in 2008 as an IoT cloud service platform solution provider, actively committed to the development of device connectivity technology and cloud service platforms. Initially, the Company focused on developing easy-to-setup and user-friendly point-to-point connectivity technology, primarily applied to consumer-grade video surveillance products. With the rise of the IoT trend, the demand for software connectivity solutions applicable to diverse hardware products has continued to grow. Leveraging its extensive experience in software-hardware integration, TUTK further launched the Kalay Cloud Platform to expand service offerings for enterprise customers seeking to venture into IoT development.



Picture: The Ecosystem of Kalay Cloud Platform

Kalay Cloud Platform is built on superior peer-to-peer (P2P) connectivity technology, enabling it to operate across various operating systems. It offers flexible and scalable modular services to help brand manufacturers or hardware manufacturers extend the value of their products through cloud applications.

TUTK has established close partnerships with global OEM/ODM manufacturers, brand manufacturers, system integrators, and chip manufacturers through its core Kalay Cloud Platform. This enables the Company to address the diverse needs of different clients, accelerate product development, expedite time-to-market, and effectively reduce



operational costs. The Kalay Cloud Platform offers open APIs and third-party service integration, enabling customers to adopt more diverse business service models. Currently, it provides over ten functional modules, including video transmission, cloud recording, data collection and analysis, remote control and management of hardware devices, and push notifications. These modules can be flexibly combined to meet the needs of different markets and customers.

Additionally, Kalay Cloud Platform prioritizes information security and privacy protection from its design inception. All functional modules adhere to international cybersecurity standards and encryption technologies to ensure the security and compliance of data transmission between devices, the cloud, and applications.

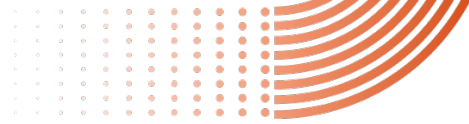
1.1 INTRODUCTION OF KALAY CLOUD PLATFORM

Based on peer-to-peer (P2P) connectivity technology, Kalay Cloud Platform offers a range of modular functions to assist customers in developing diverse IoT products with seamless software and firmware integration. Kalay Cloud Platform ensures that the products are user-friendly, reliable, and secure.

Kalay Cloud Platform is widely used in various applications, offering customizable services, project management, and application development to cater and meet specific customer requirements. This comprehensive support empowers customers to introduce their smart products or services to the market quickly.

Furthermore, customers have the option to adopt TUTK's products, including Kalay Cloud VMS (Video Management System), Hausetopia APP, Kalay Mobile APP or DMP (Data/Device Management Platform), which are developed using the core technology of the Kalay Cloud Platform. By doing so, customers can expand and enhance their own products and services.

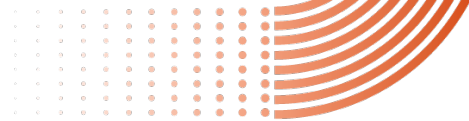
In terms of platform architecture design, TUTK incorporates cybersecurity and privacy protection into its core principles. All modules use end-to-end encryption, strict identity verification, and permission control, and undergo regular security testing and version updates to ensure the security and compliance of data transmission across devices and cloud services.



1.2 KEY FEATURES OF KALAY CLOUD PLATFORM

Through Kalay Cloud Platform, users have the ability to develop a reliable, secure, and scalable IoT solution. The platform encompasses essential functions, including device connectivity, data management, application development, and security protection. These features empower users to effectively harness IoT technology and achieve intelligent and efficient IoT applications. The following are the key features of the platform:

- **Device Connectivity and Management:** Kalay Cloud Platform offers device connectivity and management features that facilitate seamless communication between devices and the platform. It supports diverse communication protocols and connection methods, including Wi-Fi, Bluetooth, Ethernet, Z-Wave, ZigBee, to cater to various device types.
- **Data Collection and Analysis:** Kalay Cloud Platform enables real-time data collection from connected devices and offers data storage and analysis capabilities. This empowers users to capture and analyze data generated by devices, providing valuable insights and decision support.
- **Application Development and Deployment:** Kalay Cloud Platform provides tools and environments for application development, allowing developers to build and deploy IoT applications quickly. It supports various programming languages and frameworks, while offering a rich set of APIs and SDKs for easy integration and extension of functionalities.
- **Security and Privacy Protection:** Kalay Cloud Platform prioritizes security and privacy protection by implementing multiple security measures to safeguard device and data security. It provides features such as identity authentication, data encryption, and access control to ensure that only authorized users can access and operate devices and data.



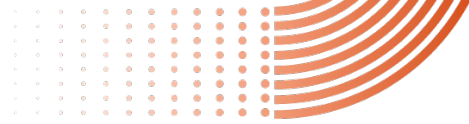
2. SECURITY RESPONSIBILITY ATTRIBUTION

The protection of data security on the user side and device side is fundamental to all cloud services. Users control devices using their cell phones, and important data is transmitted end-to-end through the network. As a pioneer in the IoT cloud platform service field, TUTK prioritizes being a stringent gatekeeper for its customers. The Company implements multiple protections, including cloud servers, software and firmware technologies, encryption verification mechanisms, etc. Data security protection is held to the highest standard within the Company. TUTK continually pays attention and adopts the latest security technologies and measures to ensure the utmost protection of its customers' data.

2.1 RESPONSIBILITY ATTRIBUTION

TUTK is responsible for the operation and security management of the cloud platform and data exchange, ensuring the protection of the cloud platform and servers. However, if customers develop their own APPs, set up or maintain their own servers, or integrate their own hardware with TUTK technology (including the use of TUTK's SDK), the security of those applications and data—including protective measures for hardware, servers, and APPs—remains the customer's responsibility. Except for the items listed in the table below, which fall under TUTK's responsibility, all other aspects of security and privacy are the responsibility of the customer.

Type	Hosted or co-located by TUTK			
Server	Alibaba Cloud/ JD Cloud	Google Cloud	Amazon	IDC/ Telecoms
Responsibility	TUTK and the cloud platform service provider share joint responsibility			
Application (APP), Cloud Platform	Both TUTK standard edition and full customization options			
Responsibility	TUTK takes on the responsibility			



2.2 TUTK SECURITY RESPONSIBILITY

TUTK collaborates with various cloud hosting service providers, including Amazon, Google, JD Cloud, etc., and deploys hosted server/co-located server service areas according to customer requirements to ensure the quality of customer service and the security of device connections.

Additionally, TUTK collaborates with cloud hosting service providers to ensure that the connections provided to customers maintain a high level of security. This primarily involves safeguarding the security of customer data, preventing vulnerabilities, and hacking attacks, and ensuring the security of equipment management and upgrades.

Furthermore, when it comes to user privacy information, the Company acknowledges the importance customers and users place on their privacy rights. TUTK upholds its commitment to privacy protection, as outlined in the [privacy protection policy document](#).

2.3 CUSTOMER SECURITY RESPONSIBILITY

When using TUTK's solutions, customers must strictly adhere to the Company's documentation and correctly configure security and integration requirements. Additionally, customers must ensure the security of their servers, clients, or hardware products themselves. For APPs/platforms developed by customers using TUTK's SDK, the Company can provide technical support; however, it cannot guarantee the overall security of their operation. Instead, it can offer security implementation recommendations and testing tools upon request to help mitigate potential risks. Regarding data security, privacy policy statements, and legal requirements related to APPs/platforms modified or customized by TUTK, customers are solely responsible for ensuring compliance with all relevant regulations.

3. TUTK INTERNATIONAL COMPLIANCE AND CERTIFICATION

As a global IoT cloud solution provider, TUTK has long been committed to complying with international information security compliance, privacy standards, and certification requirements. Our products and services follow global regulations, and we continue to introduce and pass multiple international information security and privacy protection standards to ensure that our cloud services achieve the highest levels of security and privacy.

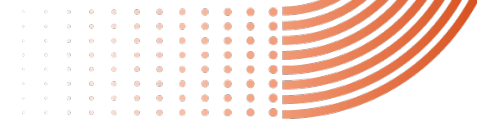
3.1 ISO/IEC 27001



ISO 27001 is the Information Security Management System (ISMS) standard developed by the International Organization for Standardization (ISO). By obtaining this certification, TUTK confirms that it has established and implemented a comprehensive information security management system capable of ensuring the security, availability, and integrity of its information.

The ISO 27001 certification encompasses the following areas:

- **Risk Management:** Ensuring the security of data, systems, and services by assessing and managing risks.
- **Security Controls:** Meeting the latest security control requirements to protect against unauthorized access and use.
- **Audit and Control:** Ensuring the ongoing effectiveness of the information security management system through dedicated audit and control mechanisms.



By obtaining ISO 27001 certification, TUTK demonstrates its commitment and expertise in information security for its customers and partners. It also reflects the Company's dedication to continuous optimization and improvement in security management and the recognition and acceptance by international.

3.1.1 ISO/IEC 27017



ISO/IEC 27017

ISO/IEC 27017 is a guideline for information security controls specifically designed for cloud services, aimed at enhancing security practices in cloud environments, including the division of information security responsibilities between cloud service providers and users.

Through this certification, we demonstrate that the Company has implemented security controls compliant with international standards in the operation and management of our cloud platform.

The requirements of ISO/IEC 27017 cover multiple aspects, such as:

- **Cloud Service Roles and Responsibilities:** Clearly define the responsibilities of suppliers and customers in terms of information security to ensure that both parties comply with regulations and implement management measures, thereby avoiding risks caused by unclear responsibilities.

- **Customer Data and Asset Protection:** Ensure that customer data in the cloud environment is properly deleted after service termination or contract expiration to avoid data residue or leakage.
- **Virtualization and Cloud Environment Security:** Through environmental isolation and enhanced measures, ensure that operations between different customers (server tenants) do not interfere with each other, and reduce the possibility of unauthorized access or cross-server attacks on customers.
- **Operational and Monitoring Transparency:** All management operations must be recorded and supervised, and supported by continuous monitoring mechanisms to ensure the transparency and auditability of cloud service operations.

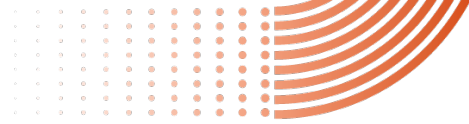
Certified by ISO/IEC 27017, the Company demonstrates its commitment to cloud service security governance and continuously improves its cloud information security management capabilities to ensure the security and reliability of customer data when operating in the cloud.

3.1.2 ISO/IEC 27018



ISO/IEC 27018

ISO/IEC 27018 is the world's first code of practice specifically designed for cloud service providers handling personal data, with the primary objective of protecting personally identifiable information (PII) in cloud environments. This certification demonstrates that the Company has



implemented personal privacy protection measures that comply with international standards in our cloud service architecture.

ISO/IEC 27018 certification covers the following key points:

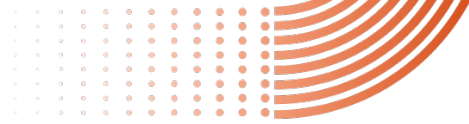
- **Personal Data Processing Regulations:** Ensures that personal data in cloud services complies with privacy protection principles and regulatory requirements throughout its entire lifecycle, from collection to use, storage, and deletion, and establishes clear internal policies to regulate the processing procedures at each stage.
- **Transparency and Consent Mechanisms:** Ensuring users clearly understand how their data is collected and used, and providing users with a verifiable authorization consent process to ensure all personal data is used only in a lawful, explicit, and authorized manner.
- **Personal Data Security Controls:** Enhance personal data security in the cloud environment through encryption technology, prevention of unauthorized access, real-time incident reporting, and response procedures, and reduce the risks associated with data breaches or misuse to ensure that user privacy is protected by multiple layers of security.

Through ISO/IEC 27018 certification, the Company demonstrates a strong commitment to protecting personal data in cloud services, ensuring that customers' privacy and rights are protected to international standards when using our platform.

3.2 GDPR (GENERAL DATA PROTECTION REGULATION)

GDPR (General Data Protection Regulation) is a data protection regulation implemented by the European Union on May 25, 2018. It aims to protect the privacy and rights of personal data while requiring organizations to comply with specific legal requirements for processing and protecting personal data. The following are key regulations under GDPR:

- **Data Protection:** As a company providing IoT and connected device solutions, TUTK may process and store large amounts of personal data. According to GDPR, the processing of personal data must meet specific legal requirements, including legality, transparency, purpose limitation,



data minimization, accuracy, and security. By complying with GDPR, TUTK ensures the proper protection of personal data, reducing the risk of data leakage and privacy violations.

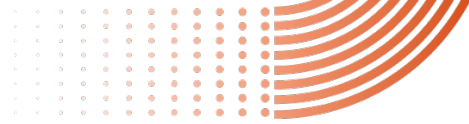
- **Protection of User Rights:** GDPR grants individual data subjects specific rights, such as access, correction, deletion, restriction of processing, and data portability. As a data processor, TUTK can implement processes and controls to ensure users can effectively exercise their rights. This fosters trust in TUTK and demonstrates the Company's commitment to privacy and data protection compliance.
- **Risk Management:** Compliance with GDPR enables TUTK to assess and manage risks and implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, or corruption.

3.3 CCPA (CALIFORNIA CONSUMER PRIVACY ACT)

CCPA (California Consumer Privacy Act), effective January 1, 2020, is designed to protect the personal information privacy rights of California residents. The Act grants consumers several rights, including:

- **Access to Personal Information:** Consumers have the right to request access to the personal information collected by organizations.
- **Deletion of Personal Information:** Consumers can request that an organization delete their personal information.
- **Disclosure:** Organizations are obligated to provide transparent information regarding the purposes for collecting and using personal information when it is collected.
- **No Sale of Personal Information:** Consumers have the option to restrict organizations from selling their personal information to third parties.

TUTK is CCPA certified and is dedicated to complying with the law. This entails taking several measures to ensure complete protection and respect for the privacy of its customers' personal information. By obtaining CCPA certification, TUTK demonstrates its commitment to safeguarding the privacy of its



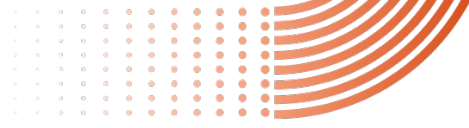
customers' personal information, providing you with added confidence and reassurance.

3.4 OTHER INFORMATION SECURITY AND PRIVACY PROTECTION MEASURES

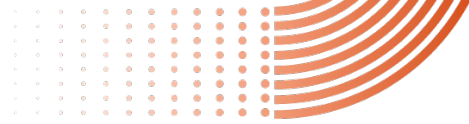
The Company places a high priority on information security compliance and takes multiple measures to ensure the security of customer data and information:

- **Compliance with Applicable Laws and Regulations:** The Company complies with applicable information security laws and regulations, including but not limited to the GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act) and other applicable privacy protection laws.
- **Data Encryption:** The Company employs robust data encryption technology to ensure the security of customer data during transmission and storage. By utilizing encryption protocols and secure algorithms, TUTK guarantees the confidentiality and integrity of sensitive data.
- **Access Control:** TUTK has implemented stringent access control measures to ensure that only authorized employees can access and process customer data. TUTK restricts data access to only necessary personnel, ensuring that only individuals with a legitimate need-to-know can handle the relevant data.
- **Security Audits and Monitoring:** The Company conducts regular security audits and monitoring to promptly identify and protect its systems and networks. TUTK closely monitors for potential security threats and unusual activities, taking appropriate measures to address and prevent them.
- **Employee Training and Awareness:** The Company provides comprehensive employee training to enhance awareness and understanding of information security compliance. TUTK encourages employees to follow best safety practices and regularly update their knowledge and skills.

Through these information security compliance measures, the Company is dedicated to safeguarding the security and privacy of its customers' data. TUTK



will continue to allocate resources and efforts to continually improve its information security practices, addressing emerging threats and risks.



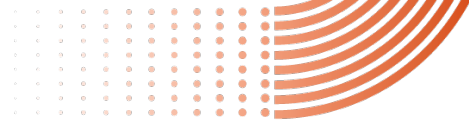
4. TUTK TECHNICAL SAFETY COMPLIANCE

Technical Safety Compliance entails ensuring that the Company adheres to applicable safety regulations and standards during the implementation and operation of its technology. The following outlines its approach to technical safety compliance.

4.1 SECURE DEVELOPMENT PRACTICE :

The Company adheres to the Secure Development Lifecycle (SDL) and best practices to integrate security measures into software and system development processes. TUTK conducts code reviews and vulnerability scans to identify and mitigate potential security vulnerabilities and weaknesses. The following practices are followed:

- **Secure Coding Guidelines:** The Company has established secure coding guidelines that outline best practices and specifications to be followed during the development process. These guidelines cover areas such as input validation, output coding, security configuration, and error handling to mitigate common security vulnerabilities.
- **Security Audits:** The Company conducts code audits to identify potential security vulnerabilities and weaknesses. Regular code reviews allow TUTK to identify and address security issues at an early stage, ensuring code quality and security.
- **Security Testing:** The Company performs system-level and application-level security testing, including black-box and white-box testing. By conducting simulated attacks and vulnerability testing, TUTK can evaluate the security of the system, identify potential vulnerabilities, and take appropriate measures to address them.
- **Security Training:** The Company provides security training to its development teams, enabling them to understand common security threats and attack techniques, and equip them with defensive measures. This helps enhance the security awareness and skills of its developers, ensuring that security is considered throughout the development process.



4.2 AUTHENTICATION MECHANISMS AND ACCESS

CONTROL :

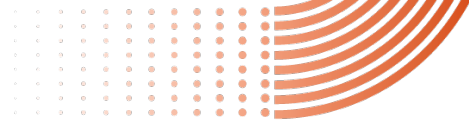
TUTK employs multiple authentication mechanisms to ensure that only authorized users can access the system and data. It has implemented stringent access control policies, including role and permission management, to grant only the necessary permissions. All servers require PKI key access, which is issued only to a limited number of personnel or authorized administrators.

- 24-hour automatic/manual monitoring to detect abnormal visits and behaviors on servers.
- Servers are distributed across multiple locations worldwide to eliminate any single point of failure.
- Regular system updates to address potential security vulnerabilities.
- Continuous testing and scanning for any unexpected vulnerabilities.

4.3 CLOUD SERVICE STORAGE :

TUTK's global servers are hosted at trusted cloud service providers, such as AWS, Google, and Alibaba Cloud, among others. By leveraging these data centers, TUTK gains access to their advanced security measures and stringent access policies, guaranteeing the confidentiality and security of its customers' data.

TUTK is fully committed to implementing best security practices, which include continuous monitoring and updating of systems and servers to ensure the highest level of protection for customer data. TUTK regularly assesses and enhances its security measures, employs encryption technology to safeguard data during transmission and storage, implements stringent authentication and access control measures, and takes proactive and contingency measures to address potential security threats.



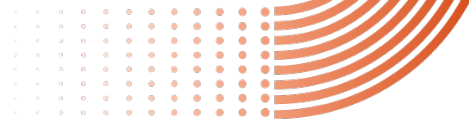
4.4 APPLICATIONS :

- TUTK utilizes advanced AWS or Softlayer security services, which offer advanced attack detection, prevention, and analysis capabilities.
- TUTK implements strict rules-based firewall blocking, which ensures that only necessary ports are open and accessible via specific access protocols.
- TUTK performs large-scale log analysis to strengthen server security and optimize resource allocation.
- Additionally, TUTK collaborates with Trend Micro Inc. for enhancing security.

4.5 DATA TRANSMISSION :

The Company implements multi-layered encryption and protection measures for data transmission and security to ensure the security of connections and data transmission between devices and cloud services, as well as between cloud services. The main measures are as follows:

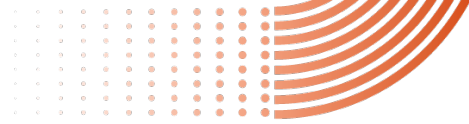
- **HTTPS Connection:** The Company utilizes the HTTPS protocol to establish secure communication between devices and cloud services. By encrypting the SSL/TLS protocol layer over HTTP communication, data confidentiality and integrity are ensured during transmission. This measure enhances the security of data exchange between devices and the cloud service.
- **Data Encryption:** Depending on the characteristics and performance requirements of different products, the Company uses AES128 or AES256 (Advanced Encryption Standard) symmetric encryption algorithms for data encryption and decryption.
 - AES128 uses a 128-bit key, providing a good balance between performance and security, making it suitable for low-latency or resource-constrained devices.
 - AES256 uses a 256-bit key, offering longer key length and higher security, making it suitable for applications with extremely high data protection requirements.



Whether using AES128 or AES256, data confidentiality and integrity are ensured through multiple rounds of encryption operations during transmission and storage, and decryption can only be performed using the correct key.

- **Secure Communication:** Depending on the device's capability and configuration, customers can choose to utilize TLS 1.2 or DTLS 1.2 for secure communication. TLS 1.2 and DTLS 1.2 are protocols designed to ensure the protection of network communication by providing encryption, integrity verification, and authentication. TLS 1.2 is suitable for reliable transmission protocols, such as TCP, while DTLS 1.2 is suitable for real-time communication and data transmission based on unreliable transport protocols, such as UDP. TUTK also has plans to periodically upgrade the versions of TLS and DTLS.
- **Packet Scrambling:** TUTK supports the scrambling of packets using compatible devices. Spoofing technology enhances the randomness and complexity of data, thereby enhancing data security and making it more challenging for unauthorized individuals to parse and decrypt the data.

Through the aforementioned encryption and protection measures, TUTK is dedicated to ensuring secure data transmission between devices and safeguarding the confidentiality and integrity of its customers' data. TUTK continuously researches and implements the latest security technologies and algorithms to mitigate emerging security threats and offer dependable data protection solutions.



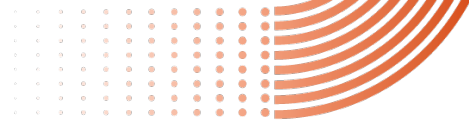
5. PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT)

The Product Security Incident Response Team (PSIRT) is responsible for monitoring, assessing, and handling security incidents related to our products and services, and ensuring that effective mitigation measures are taken and external communications are made in the shortest possible time.

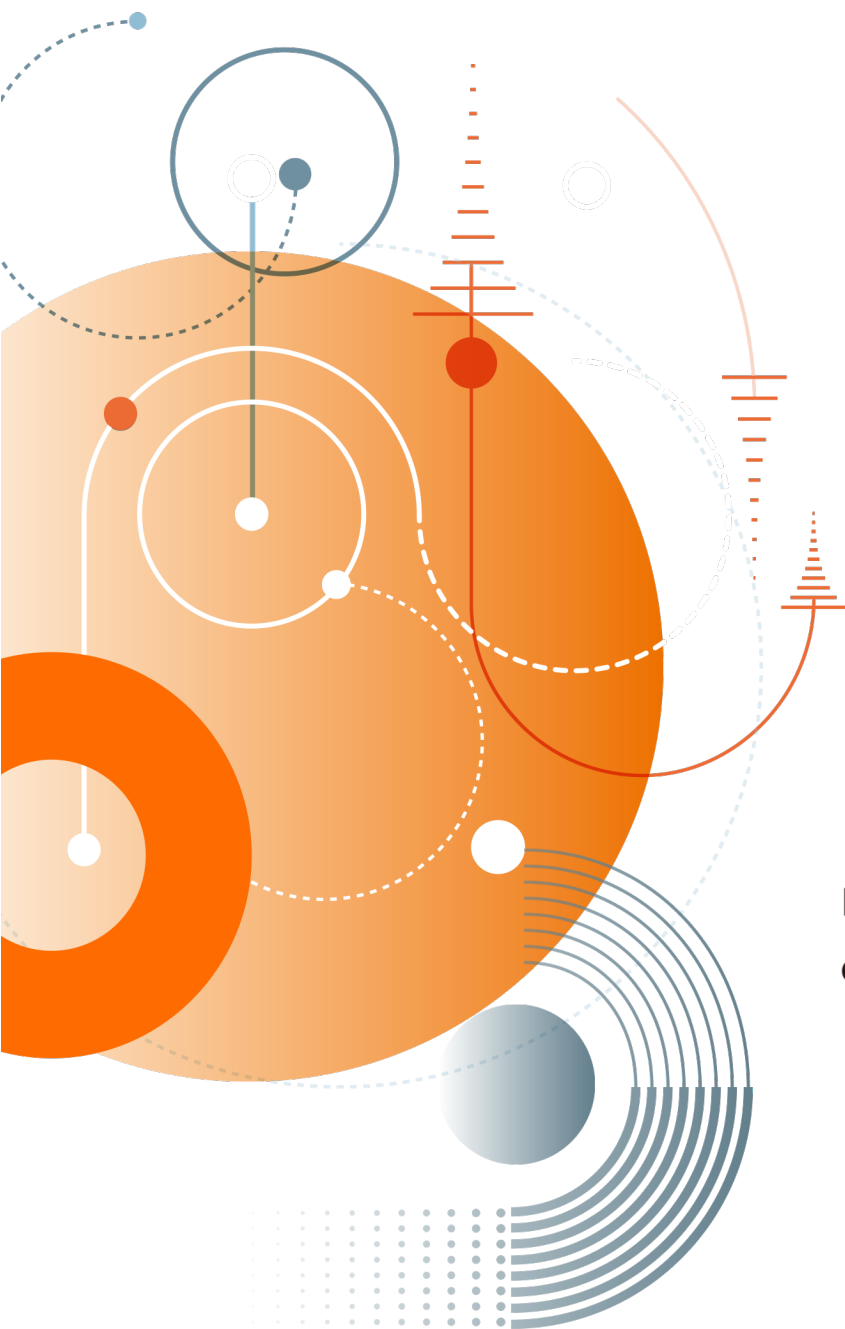
The main tasks of PSIRT include:

- **Incident Detection and Assessment:** Continuously monitor the operational status of products and services, and assess security incidents identified through internal testing, external reports, or third-party monitoring.
- **Incident Reporting and Response:** For major personal data or security incidents, notify the relevant authorities and affected customers within 72 hours of confirmation, in accordance with Article 33 of the GDPR and other applicable regulations.
- **Patching and Mitigation Measures:** Collaborate with the R&D team to develop patches or alternative solutions after confirming vulnerabilities, and complete security testing and verification before release.
- **Vulnerability Disclosure Policy (VDP):** Provide a dedicated channel for security researchers and partners to report potential vulnerabilities, and disclose relevant information in a timely manner based on assessment results and patching progress.
- **Supply Chain Cybersecurity Incident Handling:** If an incident involves third-party services or supply chain partners, the Company will simultaneously initiate the supply chain cybersecurity incident handling process, collaborate with relevant parties to mitigate risks and minimize the scope of impact, and notify affected partners and customers as necessary to assist in implementing protective measures.

To protect user safety, the Company will only disclose necessary incident information after patches or mitigation measures are available, to avoid increasing the risk of exploitation before the issue is resolved. The Company will continue to optimize PSIRT processes and tools and conduct regular cybersecurity incident response drills to enhance its ability to address emerging threats.



Disclaimer: The Company will make every effort to detect, assess, and address information security incidents in a timely manner in accordance with applicable laws and international best practices, and promptly complete reporting and remediation activities. However, given the evolving nature of cybersecurity threats and attack methods, the response measures or reporting timelines described in this white paper may not completely prevent damage in certain circumstances. The Company shall not be liable for any losses resulting from force majeure, third-party actions, or unauthorized operations.



Follow Us On    
or visit www.throughtek.com