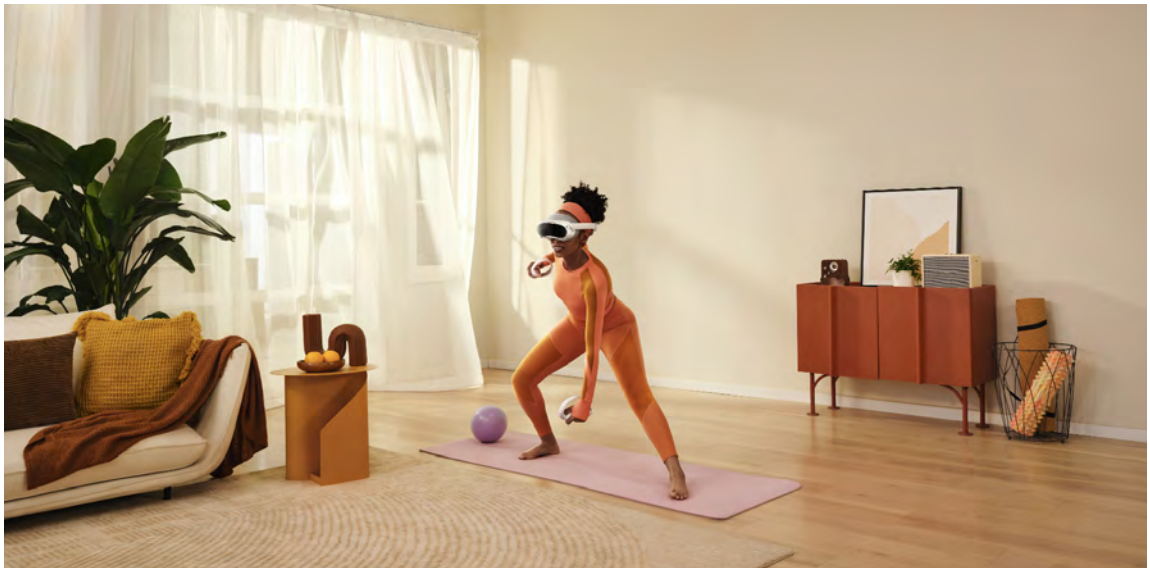
PICO

PICO Security White Paper

November, 2022

CONTENTS



Guard Your Security in the Virtual Reality World

Founded in 2015, PICO is committed to providing cutting-edge virtual reality (VR) products and services to consumers and businesses. PICO believes virtual reality is the next wave of innovation, a technology that will change everyone's daily life and how we perceive and think about the world.

PICO understands the importance of protecting the users' security across the real and virtual worlds. As a result, PICO takes a multi-pronged approach to create a powerful and comfortable full-scale virtual reality platform for users. All the products and services are designed with security as one of the top priorities.

This white paper details the specific management and technical measures we have implemented to improve the information security capabilities of our products and services. The main contents of the white paper are as follows:

- **Chapter 1: Comprehensive Security Protection.** This chapter introduces the overall security framework of PICO's products, and details the security measures we have implemented at each layer, including hardware, operating system, applications, and cloud services. This chapter can help you understand how these security measures can keep your information secure and safe and how the concept of Security by Design is ingrained in our product designs.

- **Chapter 2: Sustainable Security enabled by Security Management System.** This chapter introduces the information security management system of PICO, including security governance, security development processes, security training and awareness, managing security risks of third-party suppliers, incident and data breach response and other aspects related to information security protection.

In an interconnected world, evolving technologies bring new information security risks to us. PICO strives to provide users with safe, secure, and reliable products and services. Through this white paper, we hope all of you can better understand our concept and implementation of information security protection regarding PICO's products and services. If you have any concerns or questions about this white paper, please feel free to bring them to our attention via security@picoxr.com. You can also learn more about our approach to safety, privacy, and security in PICO Safety Center.

01.

Comprehensive Security Protection

When experiencing the virtual world, you may use various products and services provided by PICO, including hardware devices (e.g. headsets, etc.), system and software (e.g. operating system, applications, etc.), as well as internet services (e.g. games, video streaming, etc.). It is a complex undertaking to keep all these components secure at the same time. To protect users' information security, PICO has designed a comprehensive security protection framework and implemented administrative and technical safeguards.

1.1 Device and System Security

PICO hardware, together with operating system, namely PICO OS, are the basis for users to experience the virtual reality world. PICO OS is a customized operating system for virtual reality experience, which is based on the Android Open Source Project (AOSP).

1.1.1 Hardware Security

PICO headsets use a System-on-Chip (SoC) that supports ARM TrustZone technology. During the product design and production period, our engineers ensure that the correct security configurations are set for the SoC, which can provide the foundation of hardware-level trust and security protection capability.

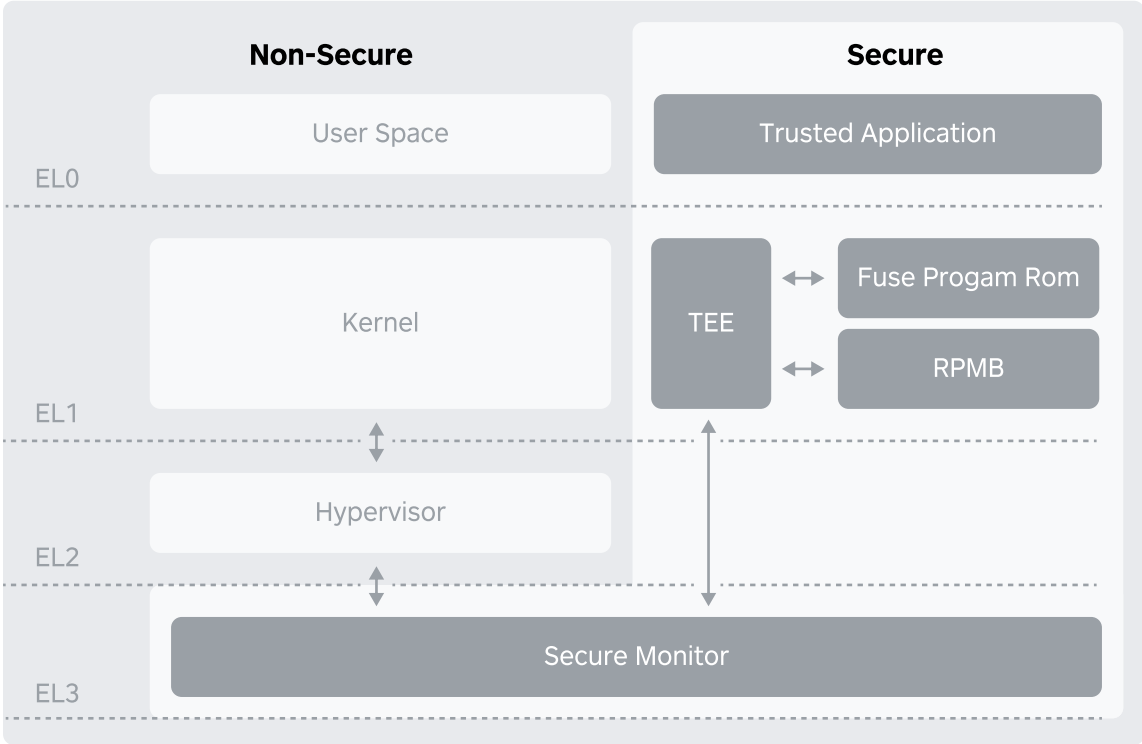
In addition, the SoC currently used in the PICO headset also includes a secure processor unit (SPU). The SPU is based on ARM SecureCore and meets the requirements of CC EAL 4+ and FIPS 140-2, and it can resist differential power analysis (DPA) attacks. Highly-sensitive encryption operations are carried out in the SPU, which can effectively balance security and encryption performance.

The SoC of the PICO headset is preset with a unique key internally, which is called the hardware unique key (HUK). The HUK of each device is different and cannot be tampered with. The key has strict access controls and can only be accessed by the hardware encryption engine. HUK guarantees the keys used by the file system encryption functions to be unique for the device.

1.1.2 Trusted Execution Environment

TrustZone technology divides the execution environment of the processor into two parts - the secure world and the non-secure world. The secure world is also called Trusted Execution Environment (TEE). The TEE protects and isolates hardware resources, and guarantees device security through execution process protection, key confidentiality, data integrity, and access rights. It can prevent malicious software attacks from ordinary execution environments and ensure that programs with high-security requirements can run in a secure environment.

At present, TEE has played an important role in many functions and scenarios on PICO devices, including user key management, file-based encryption (FBE), digital rights management (DRM), enterprise device activation management, etc.



In order to ensure that the device is trusted, we preset a unique device certificate for each device when it is produced, and this certificate is stored in the TEE. Based on this device certificate, we can perform trusted verification on the device based on a dedicated device certificate protocol, which is designed to ensure the security of device activation, binding, and sharing.

1.1.3 System Boot Security

1) Secure Boot

Secure Boot ensures that all code loaded and executed when the device starts up can be trusted.

When the system is compiled, the private key is used to sign the boot image, sub-system, etc. PICO uses one-time-programs (OTP) to write the certificate information corresponding to the private key into the fused space, which can ensure that the certificate information cannot be modified again.

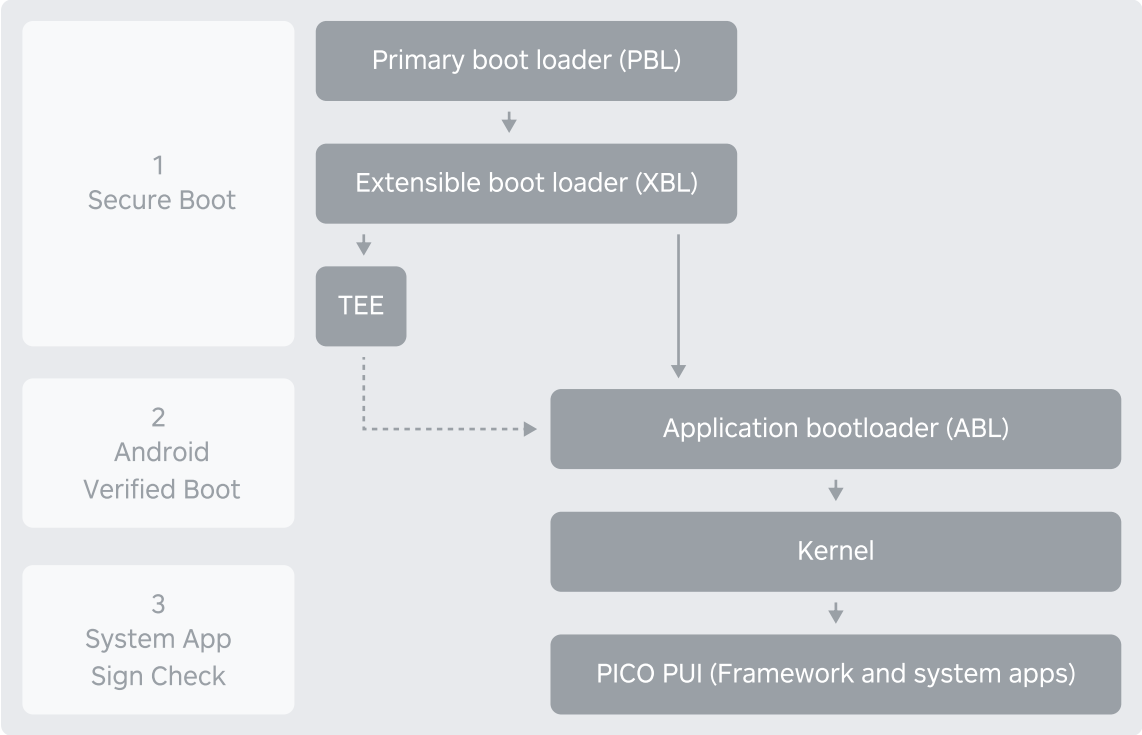
When the device boots, it first executes the immutable ROM SoC boot loader stored in the read-only memory (ROM), which is the root of trust for device boot. After that, in each step, the certificate is used to verify the signature of the image to be loaded to ensure the integrity of the code to be loaded and executed, and therefore to make sure the trust chain transmission during the boot process.

2) Android Verify Boot

During the Android image loading process, we check the integrity of the device partition image (including the kernel, system, manufacturer and other images) to ensure that the relevant image files are not tampered with. If any step of the verification fails, the system will stop booting to make sure that any code in the tampered partition will not be executed, and the related data will not be trusted either.

3) System App Sign Check

As applications with system signature generally undertake core system functionality, their integrity is critical to the security of system operation. When the system applications are being loaded, we also check the integrity of the system applications to ensure that they are trusted execution carriers.



1.1.4 Kernel Security

- **Security-Enhanced Linux, SELinux**

SELinux is a security architecture for Linux systems that enforces access control based on security policies, and allows administrators to have more control over who can access the system. The security policy is loaded into the system kernel when the

system boots and cannot be modified at will. SELinux can minimize the permissions of users and system processes to reduce the impact of potential security attacks on the system, and also can help prevent system processes from bypassing the kernel security mechanism or attacking other processes.

- **Kernel Address Space Layout Randomization, KASLR**

KASLR can offset the address mapped by the kernel image relative to the uniform resource identifier (URL), and randomly generate an offset value every time the device is booted, to ensure that the kernel image will be loaded to a different address at each boot, which can effectively resist code reuse attacks and improve the security of the system kernel.

KASLR can make the load address of the kernel image have a random offset relative to the link address when the system boots, to ensure that the kernel image is loaded to a different address each time. It can effectively resist code reuse attacks and improve system kernel security.

- **Privileged Access/Execute Never, PAN/PXN**

PAN and PXN separate kernel-state code and data from user-state, and prohibits the kernel from accessing data and executing code in user space, which can effectively prevent attackers from accessing user-state data or executing user-state code by attacking the kernel.

1.1.5 Wi-Fi Network Access Security

PICO headsets use Wi-Fi to access the internet. The device supports the WPA3 protocol, which is a new industry standard with higher security protection capability for personal and enterprise networks, and can help improve the security of WLAN connections by using stronger encryption tools. PICO will help store the SSID and password in the keystore of the system to set up Wi-FI connections more conveniently.

1.1.6 Data Encryption and Application Sandbox

PICO OS supports Android file-based encryption (FBE), which can encrypt different files with different keys or decrypt files individually. At the same time, PICO OS also supports application sandboxes and implements security protection between apps and systems by setting kernel-level application sandboxes for each application. Application sandboxes separate different apps and protect applications and systems from being attacked by malicious applications.

1.1.7 System Upgrade

PICO currently provides users with two ways to upgrade devices, including 1) Online upgrades based on over-the-air technology (OTA), and 2) Manual upgrades using offline upgrade files.

To ensure the security of offline upgrades, PICO will sign the upgrade file when it is released. During the upgrade process, the system will validate the signature of the upgrade file, to ensure that it has not been tampered with. Users will be notified of upgrades when they're available.

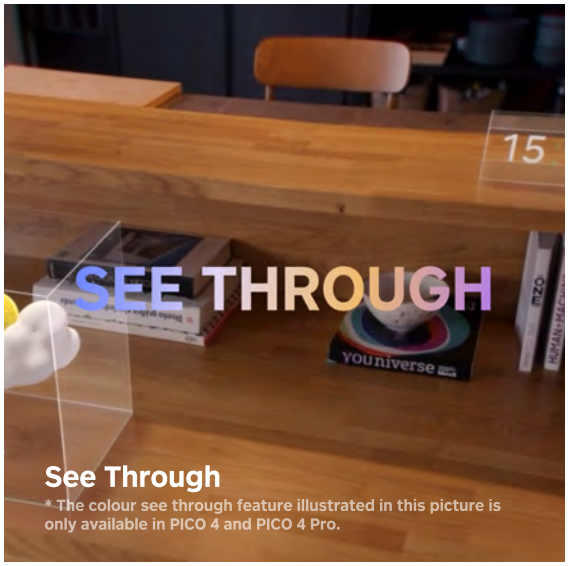
1.2 Application and Data Security

1.2.1 Device-side Computing and Algorithm Security

PICO integrates our technologies in hardware, software and technology to provide developers and users with high-performance, high-quality and secure solutions for the virtual reality experience, especially in terms of environment construction and body positioning tracking. The device-side computing technology, powered by the SoC, helps us achieve a win-win result between performance and security.

PICO now supports the following features:

- Head Tracking: Head tracking is a fundamental capability of VR devices. It uses the images of user's surrounding environment taken by the fish-eye camera on the headset, and the sensor data generated by inertial measurement unit (IMU) in the headset, to compute the rotation and movement state of the headset on the X, Y, and Z axes, i.e. six degrees of freedom (6Dof) spatial positioning.



- Hand Tracking: Similar to head tracking, hand tracking combines the images of controllers and the sensor data generated by the IMU in the controller to identify the rotation and movement of the controllers on the X, Y, and Z axes.

- See-Through: See-through allows users to see the real physical world through the camera on the headset, so that users can experience hybrid reality. As one of the most commonly used functions, the play boundary setting is powered by the see-through capability.

- Eye Tracking*: Eye tracking is one of the fundamental features of the VR experience. It uses the image of eyes to analyze the real-time gaze point and direction, thus can help adjust the visual field image (such as gaze-contingent rendering, zoom display, etc.).

- Face Tracking**: Face tracking identifies the facial expressions of users by recognizing the facial images. We can further identify the movement of lips with additional analysis of the audio input stream from the microphone. Together with eye tracking, these features can help enhance the user's interactive experience in the virtual reality world. For example, users can create an avatar in the VR world and then synchronize their expressions and lip movements in real-time.

To realize these features, different types of cameras and sensors on the device will be used, and the raw data will be collected and then computed to get the processed data. **For performance and security reasons, the whole process is conducted on the device completely.**

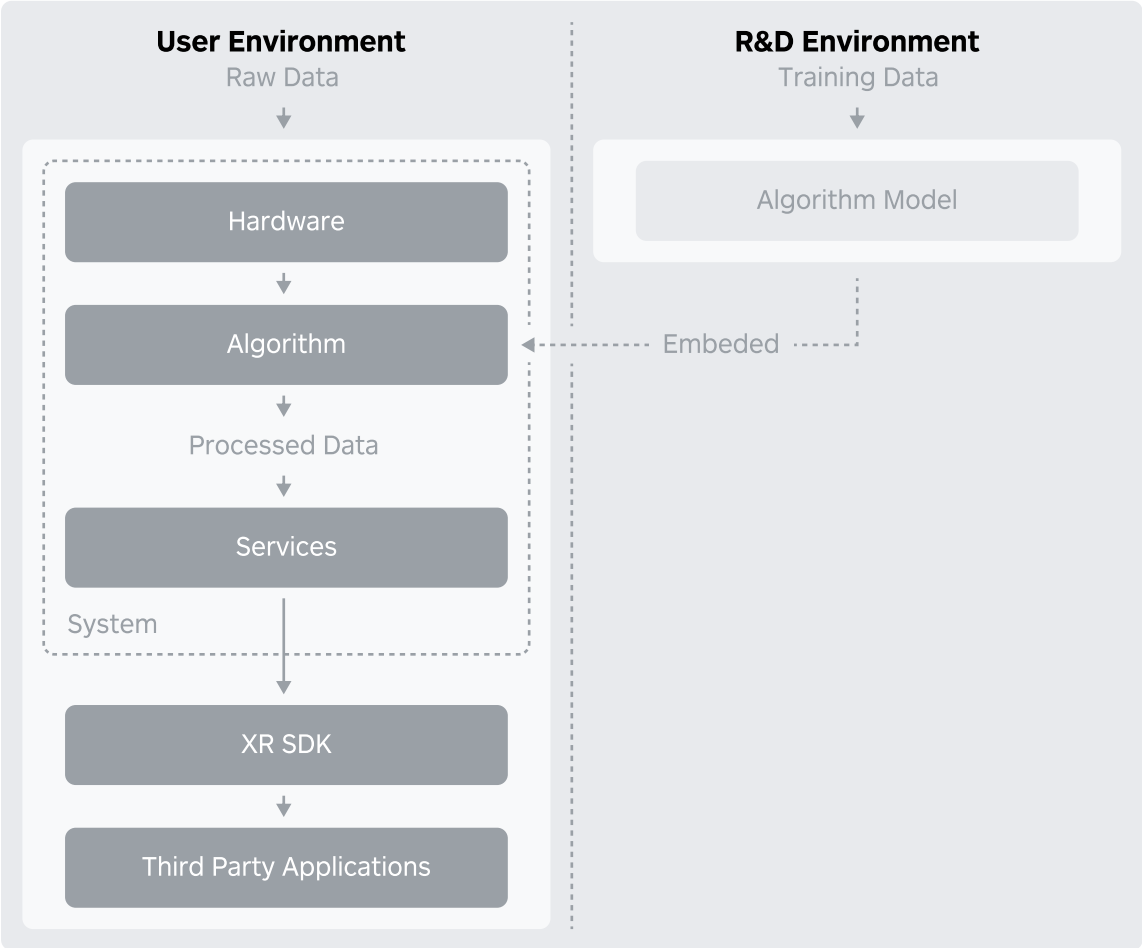
Let's take the head tracking feature as an example to explain the process of device-side computing in detail.

Firstly, when you wear the headset and move your head, the cameras will capture a series of photos of the surrounding environment, and the IMU will generate corresponding sensor data. All the data above is regarded as raw data, since it only records the original information about the headset movement and cannot be directly used to identify the relative position and motion state. Secondly, after the raw data is gathered together, driven by the processing chip on the device, the raw data will be processed and computed by the algorithms. Then, we can finally get the processed data describing the headset's relative position and motion state. At the same time, these photos and IMU sensor data will be discarded immediately after processed by the algorithms, and will not be retained on the device. Finally, the processed data can be used by other applications in real-time to track the position and motion state of your headset. The system will not retain the processed data either.

---

* Eye Tracking is available in PICO Neo 3 Eye and PICO 4 Pro.
** Face Tracking is only available in PICO 4 Pro.

To make the most of the processed data and bring users a rich virtual reality experience, developers need to integrate our XR SDK and use the data securely by calling the relevant APIs provided by the SDK.



In addition, the algorithm models are trained and optimized in the R&D environment. We embed the algorithms into the system afterward. The training data we use in the R&D environment is purchased or obtained legally. We will not use the data from real users to train, test or optimize the algorithm models.

1.2.2 Application Security

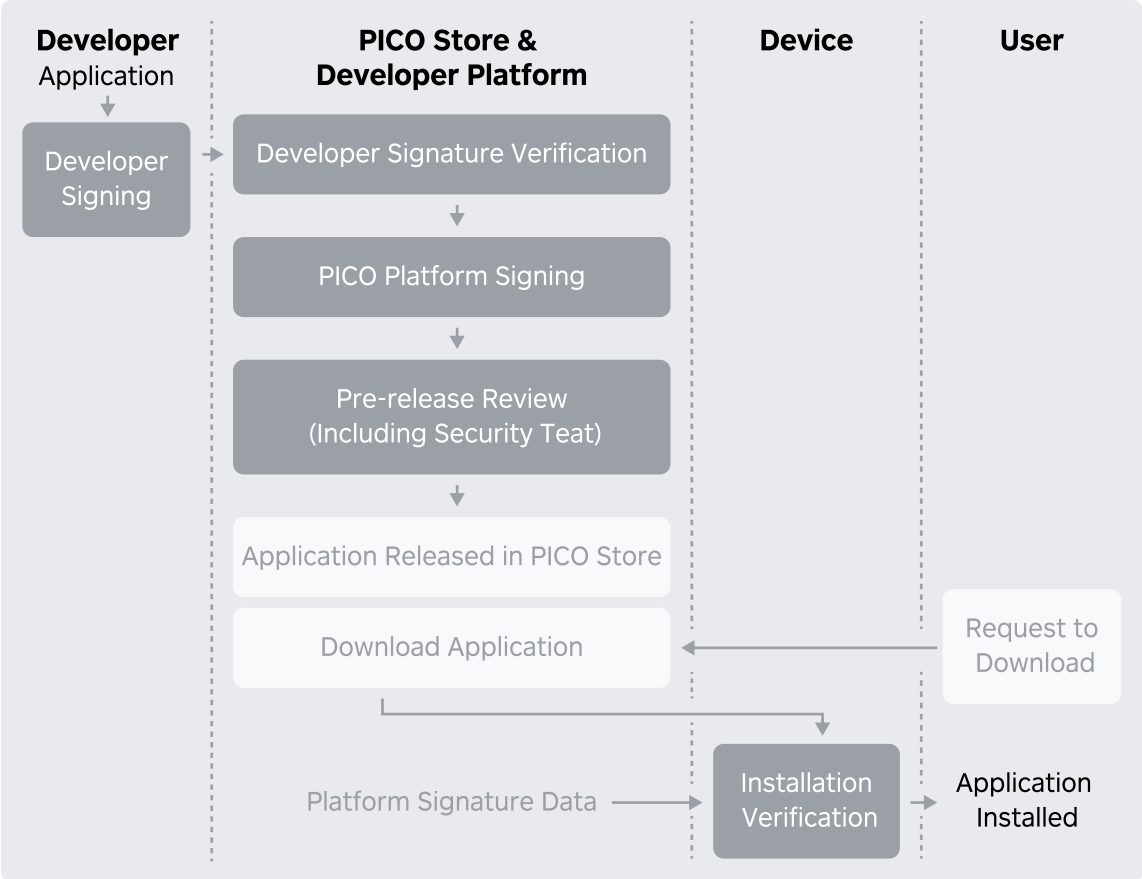
The Security of PICO Proprietary Apps

PICO has established a complete security development lifecycle (SDLC) management mechanism based on industry best practices, and conducts strict security tests on all PICO-owned applications. Only applications that pass the test can be released.

The Security of 3rd-Party Apps in PICO Store

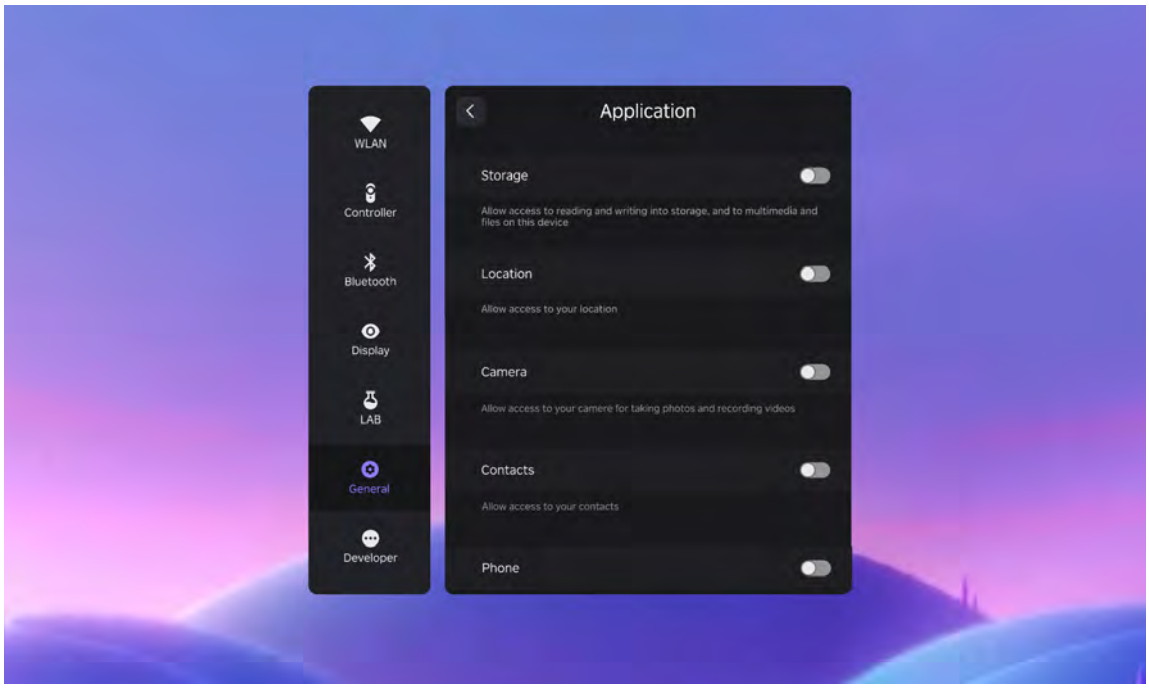
PICO Store helps users discover and easily get VR apps and games. PICO Store takes the following actions to ensure the security of applications published on it.

- Platform Signing: This step aims to make sure the apps installed by the user are consistent with the apps provided by the developer. To protect the integrity of the apps published in PICO Store, PICO will verify the developer signature of the apps, and perform platform signing before the apps are released.
- Pre-release Security Test: PICO has established a security test process before releasing the app in PICO Store. We set up a security test platform to conduct comprehensive tests on the Trojan horse virus, security vulnerabilities and other aspects of the app. Only the apps that pass the security test will be finally released in PICO Store.
- Installation Verification: When the app is installed, the system will verify its signature information to confirm the legitimacy of the source of the installation package. If the installed app is not signed by the platform, the system will prompt the user for security risks before running it.



1.2.3 System Permission Control

PICO OS now allows users to manage the permissions of a certain application, which can effectively prevent malicious applications from abusing system permissions to obtain users' sensitive data. When an application asks users to grant any permission to access data, such as accessing photos, or using the microphone, the system will inform users with a pop-up window and try to obtain users' consent. Users have the choice to grant permissions or not. In addition, users can change the authorized permissions of an app at any time through the permission management settings.



1.2.4 Data Transmission and Storage Security

PICO has established a complete data life cycle security management system, and formulated clear management and technical measures for data collection, storage, transmission, use, and destruction, to ensure the security of user data throughout its life cycle.

- Data Classification: PICO classifies user data into different types and protection levels, and implements security measures according its security level.
- Data Transmission: When using PICO's products and services, the user data will be transmitted between the device, the cloud server and the mobile applications. In order to ensure the security of the data in transit, we use transport layer security (TLS) and other appropriate algorithms to encrypt the data.

- Data Storage: Whether the user data is stored on a local device or a cloud server, we will take security measures to protect the security of it, such as data encryption or strict access control.

1.3 Online Service Security

1.3.1 Infrastructure Security

Following the defense-in-depth security concept, PICO has established a complete cloud security protection architecture, and adopts advanced security protection technologies at all levels from the network to the host and container.

For example, we have deployed an advanced network traffic analysis (NTA) at the network boundary to detect and alert malicious network intrusions. All network traffic is also verified by the web application firewall (WAF) to ensure its security and legality, and any malicious requests will be blocked in real-time. The server is deployed with a host-based intrusion detection system (HIDS), which can monitor and discover abnormal processes and behaviors, such as unexpected network connections and Trojan backdoors, and respond on time. In order to deal with distributed denial-of-service attacks (DDoS), we have also deployed a DDoS protection system to automatically intercept traffic anomaly and forward it back to make sure that all the online services will not be affected.

In addition, the security team will closely track the security trends and the latest attack methods, and constantly iterate and upgrade security defense measures to ensure continuous security.

1.3.2 Online Service Security

In order to improve the security and availability of the online service provided by PICO, and prevent it from potential security attacks, we will conduct strict pre-launch security tests. Only services that pass the test can be released. During the security test, we will refer to industry best practices, such as OWASP Top Ten.

1.4 Continued Security Maintenance

The world we live in is constantly changing and our products are updated continuously, so we continue to face new security risks and challenges. Therefore, it is critical to provide users with ongoing security support and sufficient protection all the time.

1.4.1 Security Vulnerability Management and Response

PICO has established a complete security vulnerability management process, which

can detect, analyze and respond to new security vulnerabilities, and provide risk remediation and repair measures as soon as possible.

Our security team will regularly conduct security tests and attack defense drills to find security vulnerabilities and risks in products as much as possible.

We also consider external security researchers and our end users the most important partners in maintaining the security safeguards of our products. We actively accept and respond to issues reported by them. Where appropriate, we will address the issue with product changes, technical bulletins and/or responsible disclosures to the public.

If you find any potential security vulnerabilities in PICO's products, please feel free to report it to us via security@picoxr.com.

1.4.2 Security Patch and Support Policy

PICO will include necessary security patches in regular system updates, including security patches from AOSP, upstream Linux kernel and SoC manufacturers, etc.

When a monthly Android security patch is released, we will incorporate the relevant security patch into the next available OTA update. We take the integration of security patches as one of the checkpoints in the OTA release quality review to ensure that the device does not have open known vulnerabilities left.

Currently, we provide these security updates for all released models. The specific update frequency and content are subject to the actual updates received by your device. We will prompt you to upgrade your device when a new update is available. If our support policy changes, we will post a related support change announcement.

02.

Sustainable Security enabled by Security Management System

PICO is committed to continuously creating secure and reliable products and services for all users. To achieve this goal, PICO has established a complete information security management system. By continuously operating this management system, we are able to bring together experts and resources from various fields within the organization to fully implement our concepts of information security and privacy protection in our products and services.

2.1 Security Governance

PICO pays great attention to the information security of users. So we bring various cross-functional teams together to work collaboratively to ensure that our policies, procedures and requirements related to information security protection can be implemented throughout the life cycle of PICO's products and services.

2.2 PICO Security Lab

The PICO Security Lab is composed of excellent security researchers and experts in the industry, and its mission is to continuously pay attention to and deal with possible security risks in PICO's products, and work closely with the product team to ensure the security of the products. Their work includes:

- Continue to conduct security research to understand and learn the latest security technologies and development trends.
- Introduce new security technologies into the product development process in a timely manner and build a more reliable security protection mechanism.
- Conduct regular security and penetration tests for the products to enhance and improve the security of PICO's products.

2.3 Security By Design and Security Development Process

In order to provide users with better security protection, we implement the concepts of Security By Design, and establish the security development lifecycle processes that cover the product requirements, design, R&D, testing, launch, and monitor phases. Starting from the product requirement and design phase, we take information security protection into consideration.

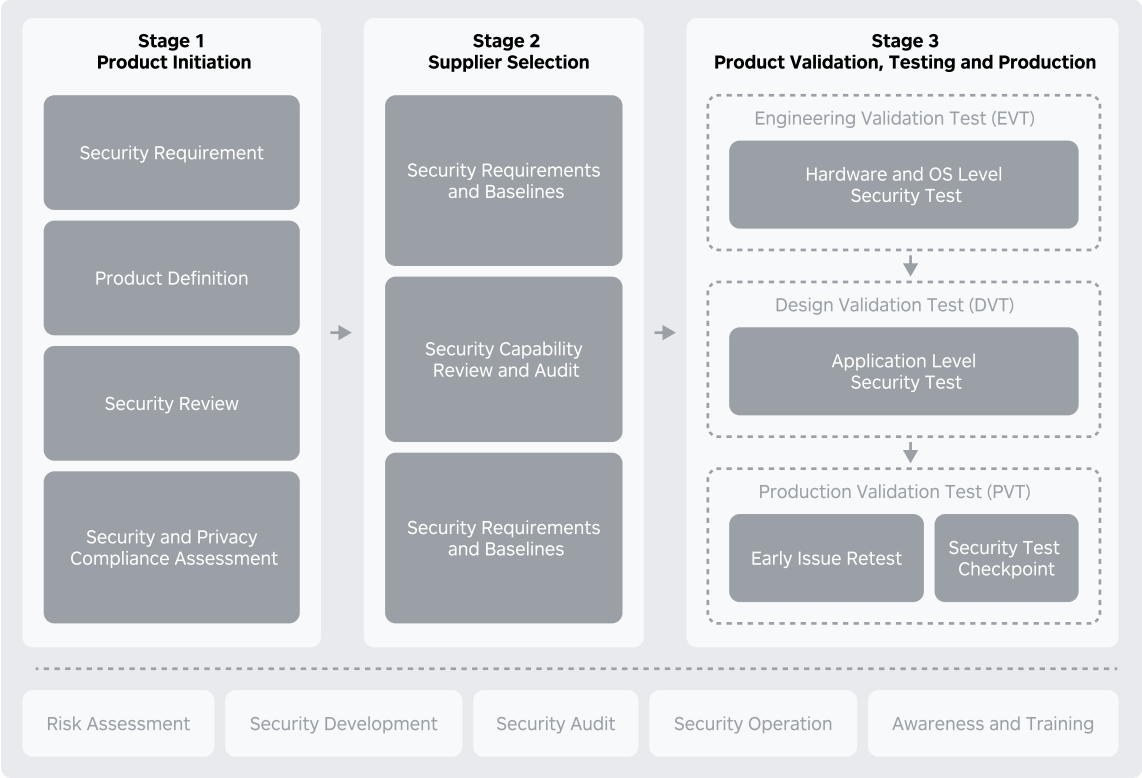
Based on the differences between hardware and software development, we have established tailored processes for different types of products and services to meet the goals of product iteration and security protection.

Security Development Lifecycle Process for Hardware:

- In the product initiation stage, our security experts will provide security requirements to the product team and participate in the product definition process . At the same time, they will also participate in the product review to ensure that security requirements can be implemented.

- In the supplier selection stage, our security team will review the security capabilities of suppliers involved, and provide security baseline requirements to them. At the same time, they will also perform a comprehensive review and management of suppliers during the process.

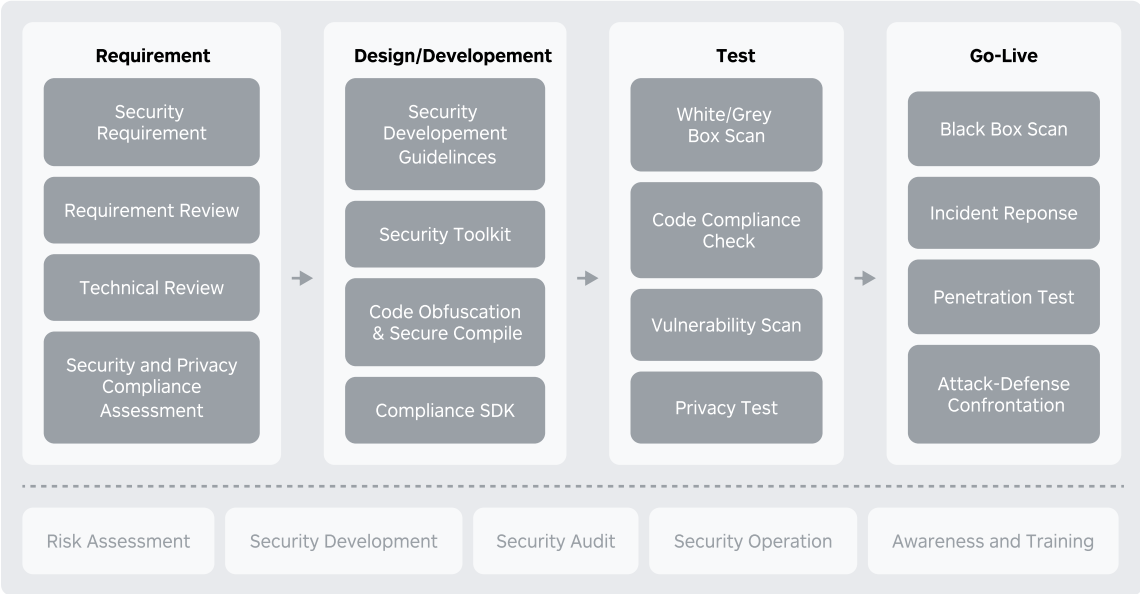
- In the product verification, testing and production stage, we will conduct security tests at different test phases, covering hardware, systems and applications, etc. And in the final testing, we will verify and retest earlier security issues, and set up security checkpoints. Only the products that pass the checkpoint test can enter formal production and finally deliver to end users.



Security Development Lifecycle Process for Software

- As software, applications and internet services are iterated faster than hardware products, we follow a more agile security management process that improves security through continuous iteration.

- Our security team works closely with the R&D team to discover and deal with potential security risks, including participating in the requirements and technical reviews, providing security development guidelines, providing security toolkit (including self-developed code security add-ons and vulnerability prevention components, etc.) , code security and privacy test, etc.



2.4 Human Resource Security and Security Awareness

PICO has established a comprehensive training, awareness and learning program for staff and employees for information security protection, including mandatory information security training for new employees. In addition, annual information security training is required for employees. We also host information security activities and promote awareness of security protection with emails and posters.

2.5 Change Management

PICO has defined the requirements and processes regarding change management, covering change plan, approval, and implementation. We also take the impact regarding information security into consideration during the change review. Our sound change management make it possible to ensure the stability and security of our products and services.

2.6 Managing Third-Party Supplier Security Risks

PICO cooperates with many different third-party suppliers, outsourcers, and partners throughout the product life cycle, such as parts suppliers, logistics companies, dealers, etc. So it is also essential for us to effectively manage third-party security risks to ensure the security of the products and services.

Before entering the formal contract, we conduct security assessments and due diligence on our third-party suppliers to check whether they meet our security compliance requirements. When signing the contract, we include information security protection clauses to define the relevant responsibilities and obligations of third-party suppliers in the contract. We also conduct security audits when necessary to check whether the third-party suppliers have adopted appropriate security measures.

2.7 Incident and Data Breach Response

We have established processes and procedures for responding to security incidents and data breaches, which can guarantee that potential security incidents and data breaches can be reported and responded to as soon as possible, and allow us to investigate and remediate impacted products and services, and as appropriate, make any reports, disclosures or notifications as required by relevant laws and regulations. At the same time, according to the requirements of laws and regulations from different countries and regions, we will promptly notify relevant regulatory agencies and data subjects of data breaches when necessary.

Appendix - Glossary

Short form	Full name
AOSP	Android Open Source Project
DDoS	Distributed Denial-of-Service Attack
Dof	Degree of Freedom
DPA	Differential Power Analysis Attack
DRM	Digital Rights Management
FBE	File-based Encryption
HIDS	Host-based Intrusion Detection System
HUK	Hardware Unique Key
IMU	Inertial Measurement Unit
SELinux	Security-Enhanced Linux
KASLR	Kernel Address Space Layout Randomization
NTA	Network Traffic Analysis
OTA	Over-the-Air Technology
OTP	One-Time-Programs
PAN	Privileged Access Never

Appendix - Glossary

Short form	Full name
PXN	Privileged Execute Never
RGB	Red Green Blue
ROM	Read-Only Memory
R&D	Research and Development
SDLC	Security Development Lifecycle
SDK	Software Development Kit
SoC	System on Chip
SPU	Secure Processor Unit
TEE	Trusted Execution Environment
TLS	Transport Layer Security
UI	User Interface
URI	Uniform Resource Identifier
VR	Virtual Reality
WAF	Web Application Firewall

Disclaimer

This document only serves as a general reference to understand the information security capabilities of the products of PICO. The information about the features and specifications of the products described in this document are for reference only and do not constitute any form of commitment. Some of the features described in this document may only be provided in typical device models or system versions, or may be gradually provided to users via system upgrades.

However, due to potential issues such as technology upgrade, product iteration, changes of applicable laws and regulations, and consistency of wording, PICO hereby expressly declares that it does not make any express or implied guarantee on the completeness, accuracy and applicability of the contents of this document.

Due to the continuous improvement of the product or service, PICO may update the content of this document. You can get the latest version of this document at our Safety Center.