ECOVACS

Product Security White Paper

Ecovacs Robotics

A Global Leader in Innovative Service Robotics

Version: 1.1

Release Date: May 2026

ABSTRACT

In the era of smart homes, data security and privacy protection have become crucial components of a product's core competitiveness. ECOVACS Robotics firmly believes that trust is the foundation of all intelligent services. This white paper aims to comprehensively elaborate on ECOVACS' security and privacy protection framework integrated throughout the entire product lifecycle, detailing our systematic practices in device security,communication encryption, data governance, cloud protection, compliance certification, and other key areas.

Adhering to the principles of "Security-by-Design and Privacy-by-Default," we combine internationally recognized security technologies (such as secure boot and end-to-end encryption) with rigorous internal management processes. Our security capabilities are continuously validated through multiple authoritative certifications, including ISO 27001, ISO 27701, ETSI EN 303 645, and UL IoT Security Diamond Level. ECOVACS is committed to sustained investment in safeguarding every interaction and trust of over 38 million household users worldwide.

CONTENTS

DEEBOT X1 FAMILY

Intelligent Cleaning, Secure Guardian

About ECOVACS

ECOVACS Robotics Co., Ltd. is a globally leading service robotics company dedicated to enhancing the quality of human life through innovative technologies. Since its establishment, ECOVACS has focused on the R&D and manufacturing of intelligent household robots, successfully bringing floor-cleaning robots, window-cleaning robots, and other products into tens of millions of households worldwide. Currently, our products and services cover over 38 million households globally, with a solid user base and brand influence in major markets including Europe, North America, and the Asia-Pacific region.

By building an open product ecosystem and technical architecture, ECOVACS provides a broad innovation platform for third-party developers and partners, jointly promoting the in-depth application of intelligent robots in diverse scenarios such as home, commercial, and public services.

Our Security Commitment and Core Principles

As products become increasingly intelligent, ECOVACS regards **data security** and **privacy protection** as the cornerstone of product design and our core commitment to users. We firmly believe that only by winning users' trust can intelligent technology truly empower a better life. To this end, we embed the following core principles into every link of our products and services:

- **Transparency and Controllability:** We clearly and understandably inform users of the purposes of data collection and usage, and provide intuitive privacy control options to ensure users' right to know and

control over their own data.

- **Security-by-Design**: Security measures are integrated from the initial stage of product design, covering the entire chain of hardware, firmware, applications, communications, and the cloud. International standard encryption technologies and security protocols are adopted.
- **Data Minimization**: We only collect and process data necessary for realizing product functions, and minimize privacy risks to the greatest extent through technologies such as anonymization and pseudonymization.
- **End-to-End Protection**: Implement full-cycle encryption protection for user data from the device to the cloud, and during transmission and storage, to strictly prevent unauthorized access and leakage.
- **Independent Verification and Continuous Improvement**: We regularly undergo security audits and penetration tests by authoritative third-party institutions, verify our security level through international certifications, and establish a continuously improving security governance system.

Objectives and Scope of This White Paper

This white paper aims to systematically demonstrate ECOVACS' systematic achievements in product security and privacy protection to users, partners, and the public. The content covers key areas such as **device security, application security, data protection, communication security, cloud platform architecture, and compliance certifications.**

Through this document, we hope you can clearly understand how ECOVACS safeguards your data security and feel our determination and ability to create intelligent robot products trusted by users worldwide.


T80S

Comprehensive Technical Security Measures

ECOVACS has built an "end-pipe-cloud" integrated in-depth defense system covering hardware, software, communications, and the cloud. This chapter details the key security technologies implemented at each layer to ensure the security and reliability of products throughout their lifecycle.

【Figure 1: ECOVACS Product Security Architecture Diagram】

Hardware and Firmware Security

Hardware and firmware are the first line of defense for product security. ECOVACS integrates security into chip selection and design from the very beginning.

Hardware Root of Trust-Based Secure Boot Chain

ECOVACS products adopt a secure boot mechanism based on the hardware root of trust. After the device is powered on, starting from the BootROM, it verifies the digital signature of the next-stage bootloader and

system kernel level by level, ensuring that only firmware officially signed by ECOVACS can be loaded and executed. This effectively prevents malicious software or unauthorized firmware from running on the device.

- Trusted Boot Process: Maskroom → SPL → UBOOT → KERNEL
- Tamper-Proof Guarantee: Each level of firmware must pass the cryptographic verification of the previous level, forming a complete trusted chain.

【Figure 2: Schematic Diagram of the Secure Boot Process】

Secure Control of Debug Interfaces

To protect core intellectual property rights and prevent unauthorized access to devices, ECOVACS implements strict control over the debug interfaces (such as UART, JTAG) of production devices:

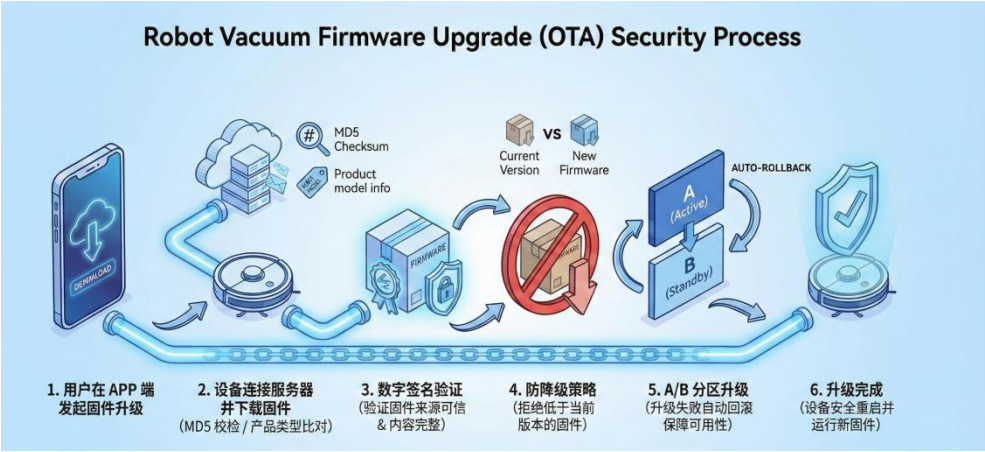
- Disabled by Default: All debug interfaces are disabled at the factory.
- Authorized Access: Temporary activation is only allowed through internal authorization processes in specific scenarios such as after-sales maintenance.
- Output Filtering: Logs output by enabled debug interfaces are processed to mask sensitive information, strictly preventing data leakage.

Chip-Level Security Protection

- Read Protection Mechanism: The main control chip (MCU) enables the Read Protection (RDP) function to prevent firmware or sensitive data from being extracted through debug interfaces.
- Secure Communication: In key hardware communication links (such as SPI/I²C), security chips or encryption measures are introduced to protect the confidentiality of bus data transmission and resist hardware probe attacks.

Firmware Update and Anti-Downgrade Mechanism

- Secure OTA Updates: Firmware upgrade packages are all digitally signed and verified. The device strictly verifies the validity of the signature before installation to ensure the update source is trustworthy and the content is complete.
- Anti-Downgrade Strategy: The system refuses to install firmware with a version number lower than the current version, preventing attackers from exploiting known vulnerabilities in older versions to cause damage.
- Failure Recovery (A/B Partition): Adopts an A/B dual-system partition design. If an accident occurs during OTA upgrades (such as power failure), the device can automatically roll back to the last normally working version to ensure device availability.



【Figure 3: Schematic Diagram of the Secure Update Process】

Communication Security

ECOVACS ensures that data transmitted through any network channel is protected by strong encryption, preventing data from being eavesdropped or tampered with during transmission.

Encrypted Communication Between Devices and the Cloud

- Mandatory TLS Encryption: All communications between devices and the ECOVACS cloud platform are forced to use TLS 1.2 and above security encryption suites for transmission encryption and identity authentication.
- Mutual Authentication: Mutual identity authentication is performed between devices and the cloud to ensure that devices connect to legitimate ECOVACS servers, and at the same time, servers only provide services to legitimate connected devices.

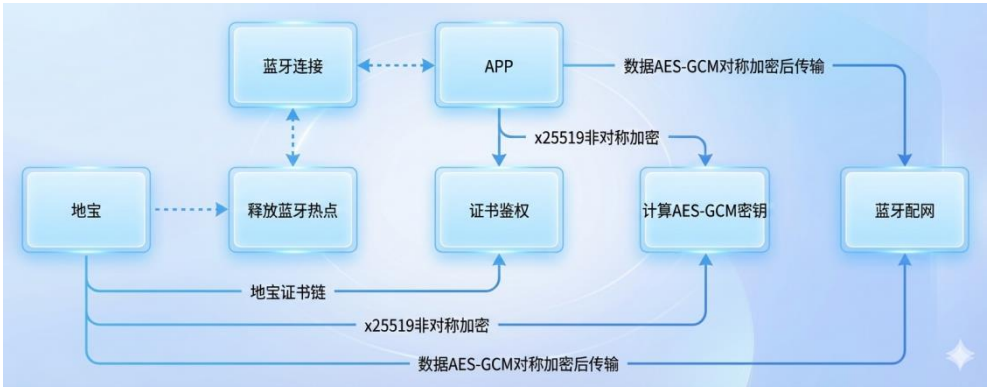
Local Network Access Security

- Wi-Fi Security: Supports mainstream encryption protocols such as WPA2/WPA3 to ensure the security of devices accessing the home network.

- Restricted AP Hotspot: The AP hotspot function enabled by devices in network configuration mode is strictly restricted:
  - Only necessary ports (such as 8888) are opened for network configuration communication.
  - The hotspot has an automatic timeout shutdown function.
  - Strict network isolation to prevent attacks on the home local area network through the device's AP hotspot.
- Secure Bluetooth Pairing:
  - Physical Confirmation: Key binding operations require confirmation via the device's physical buttons to prevent malicious binding.
  - Link Encryption: Uses link-layer encryption of BLE 4.2 and above to protect the pairing process.
  - Session Key: Bluetooth control commands are encrypted with dynamically negotiated keys for each session, effectively resisting replay attacks.

Network Configuration Authentication and Encryption

The device network configuration process adopts certificate-based mutual authentication and asymmetric encryption (such as x25519) to negotiate symmetric keys, and finally establishes a secure channel through high-strength symmetric encryption (such as AES-GCM), fundamentally eliminating man-in-the-middle attacks.



【Figure 4: Schematic Diagram of the Secure Network Configuration Process】

Application Security

Client Runtime Environment Security Detection

The ECOVACS App has the ability to detect the security of the runtime environment to ensure it serves users in a trusted environment:

- Root/Jailbreak Detection: Identifies and alerts risks of running on rooted or jailbroken devices by checking system files, attributes, logs, and behavioral characteristics from multiple dimensions.
- Emulator Detection: Detects hardware features, sensor parameters, and graphics rendering performance to prevent the application from being analyzed and debugged in a simulated environment.
- Security Hardening: Application code undergoes security hardening processes such as obfuscation and packing to increase the difficulty of reverse engineering.

Local Data Encryption and Key Management

- Sensitive Data Protection: All sensitive user data (such as maps, logs) is encrypted when stored locally on the device.
- Key Security: Fully utilizes the secure storage areas provided by the operating system (such as Android Keystore, iOS Keychain) to manage encryption keys, ensuring the keys themselves are difficult to extract.

User Account and Authentication Security

- Strong Password Policy and Multi-Factor Authentication (MFA): Encourages users to set strong passwords and provides MFA options to add an extra layer of protection for account login.
- Session Management: Implements a secure session token management mechanism, including idle timeout, token renewal, and prevention of session fixation attacks.

- Anomaly Monitoring: Real-time monitors and alerts on abnormal login behaviors (such as remote login, multiple failed attempts).

Data Security

- During network transmission, files undergo SHA-256 integrity verification to safeguard the "digital fingerprint" of the data.
- Performs validity verification (such as format, type, length) on data transmitted over the network to build the first gate of security.

Video Security

Certain models of household robot products provide official video services, including security alerts and fixed-point monitoring functions.

When users access the robot's camera through the Video Butler function, secondary password verification is required. Encrypted transmission and access control mechanisms are adopted to ensure the security and privacy of home image data are not accessed without authorization.

【Figure 5: Illustration of Video Butler】

Cloud Platform Security

The ECOVACS cloud platform has built a security system with in-depth defense capabilities to provide reliable protection for IoT services.

Cloud Infrastructure Security Protection

- Network Isolation and Segmentation: Strictly isolates development, testing, and production environments. Within the production network, micro-segmentation isolation is performed according to the risk level of different workloads.
- DDoS Protection: Deploys a distributed denial-of-service protection system to ensure service availability.
- Intrusion Detection/Prevention System (IDS/IPS): Real-time monitors network traffic to detect and block malicious attack behaviors.

Identity Authentication and Access Control

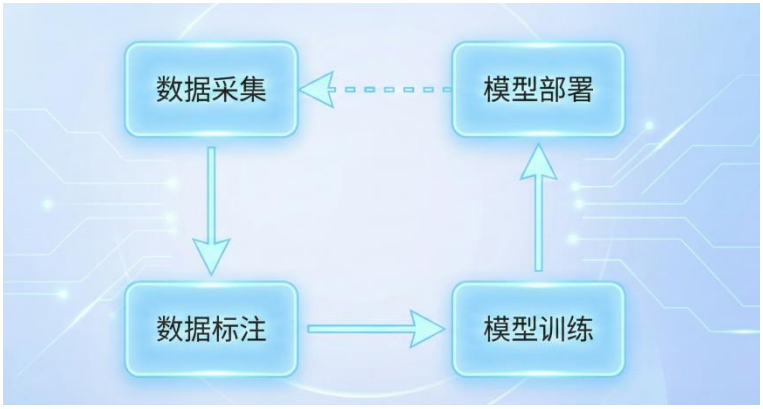
- Principle of Least Privilege: Implements strict access control policies (RBAC) following the principle of least privilege. All API access requires mandatory authentication and authorization.
- API Security Gateway: All service APIs are released through a unified gateway, implementing security policies such as rate limiting and anti-replay attacks.
- Operation and Maintenance Security: All operation and maintenance operations in the production environment must be performed through a bastion host and subject to strict audit log monitoring.

Security Monitoring and Threat Detection

- Centralized Log Auditing: Collects all key logs for centralized monitoring and analysis to achieve traceability of security incidents.
- Threat Intelligence and Anomaly Detection: Uses automated security monitoring tools to detect potential threats and abnormal activities in real-time and respond promptly.

AI Algorithm Training and Usage Security

- Training Phase: Legally collect core data, construct datasets after anonymization and cleaning, iteratively train models using training frameworks (such as TensorFlow), and optimize through validation sets.



【Figure 6: Illustration of Algorithm Training】

- Deployment Phase: First test the model's stability in multiple scenarios, then package and deploy it. Ensure security with encrypted transmission/isolated storage. After launch, monitor performance and update and optimize as needed.。

DEEBOT *mini*

Data and Privacy Protection Practices

ECOVACS firmly believes that privacy is a fundamental right of users. We strictly comply with global privacy protection regulations and integrate the principle of "Data Protection by Design and by Default" into every link of product design, ensuring users have full transparency and control over their data.

【Figure 7: Illustration of Data and Privacy Protection】

Privacy Protection Principles

【Figure 8: Illustration of Privacy Protection Principles】

Our privacy practices are underpinned by the following core principles:

- Lawfulness, Fairness, and Transparency: We process data solely upon user consent or as otherwise permitted by applicable laws. We ensure that users are clearly informed of the purpose, scope, and methods of data processing.
- Purpose Limitation: Data collection and processing are strictly confined to fulfilling defined product functionalities and shall never be repurposed for any unauthorized objectives.
- Data Minimization: We collect only the minimum amount of data strictly necessary to deliver our services.
- Storage Limitation: We retain personal data in strict accordance with relevant legal and regulatory requirements.
- Integrity and Confidentiality: We implement rigorous access controls to ensure the security of user data during both transmission and storage, thereby preventing unauthorized access, disclosure, or compromise.
- Accountability: We have established comprehensive privacy governance frameworks and robust incident response mechanisms, assuming full responsibility for the protection of personal data.

Data Lifecycle Management

【Figure 9: Illustration of Data Lifecycle Security】

Data Collection Minimization

In the data collection link, we practice the principle of minimization through technical and management measures:

- Functionally Necessary: Only collect necessary environmental information such as room size and obstacle positions to provide cleaning services.
- Differential Privacy Technology: When data needs to be collected for product optimization, we use advanced technologies such as differential privacy to anonymize the data, ensuring it cannot be traced back to specific individuals or households.
- Explicit Authorization: Any new data collection requirements will be re-informed to users through the App, and implemented only after obtaining users' explicit consent or having the corresponding legal basis.

Data Transmission Encryption

All data leaving the device, including maps and logs, is transmitted through a strongly encrypted channel (TLS) to ensure the confidentiality and integrity of the data during its transmission to the ECOVACS secure cloud platform. Internationally recommended algorithms, key strengths, and usage methods are adopted for encryption, as shown in the following table:

Algorithm	Key Strength	Usage
AES	128 bits and 256 bits	Encryption
RSA	2048 bits and4096 bits	Signature
ECC	256 bits	Signature
ECDSA	256 bits	Signature
Ed25519	256 bits	Signature

Data Storage and Anonymization

- Encrypted Storage: All sensitive user data is stored in encrypted form in the cloud, and even system administrators cannot directly access the plaintext content.
- Classification and Grading: Implement classification and grading management of data, and adopt different access control and protection strategies for data of different security levels.
- Anonymized Aggregation: Data used for big data analysis is subjected to aggregation and anonymization processing to completely remove personal identifiers.

Right to Data Deletion

We fully protect users' rights to their data:

- Data Deletion: Users can clear their personal data on the device and in the cloud through the account cancellation function in the App.

Protection of User Rights

ECOVACS products provide an intuitive privacy control center, allowing users to easily:

- Manage User Data Authorization Settings: Independently decide whether to enable necessary information authorization functions (such as personal account information, mobile device information, etc.).
- Product Improvement Program: Independently decide whether to participate in product improvement programs, product promotion services, etc.
- Access and Correct Data: View and modify intelligently generated home map models at any time.

【Figure 10: Illustration of User Rights】

For more detailed information, please refer to ECOVACS' complete Privacy Policy:

Mainland China:

https://gl-cn-wap.ecovacs.cn/content/agreementNewest/PRIVACY/DEFAULT/DEFAULT

Singapore:

https://gl-sg-wap.ecovacs.com/content/agreementNewest/PRIVACY/SG/DEFAULT

Germany:

https://gl-us-wap.ecovacs.com/content/agreementNewest/PRIVACY/US/DEFAULT

United States:

https://gl-us-wap.ecovacs.com/content/agreementNewest/PRIVACY/US/DEFAULT

ECOVACS ROBOTICS

Brand New WINBOT Featuring TruEdge Scrubber

WINBOT W2S OMNI

RIGHT ON THE EDGE

EVERY CORNER IN REACH

Security Audits and Compliance Certifications

ECOVACS' security and privacy protection capabilities are not only derived from strict internal management but also verified through numerous international authoritative third-party institutions. These certifications are strong evidence of our commitment to security to users.。

【Figure 11: Illustration of Security Audits and Compliance Certifications】

Compliance with International Standards

ECOVACS' product design and operation processes fully comply with the following international and domestic regulations and standards:

- International Privacy Regulations: General Data Protection Regulation (GDPR), UK Product Security and Telecommunications Infrastructure Act (UK-PSTI), California Consumer Privacy Act (CCPA), etc.
- International Security Standards: ISO/IEC 27001 (Information Security Management System), ISO/IEC 27701 (Privacy Information Management System), ISO/IEC 27018 (Protection of Personal Data in Public Clouds), etc.
- Chinese Laws and Regulations: Cybersecurity Law of the People's

Republic of China, Personal Information Protection Law of the People's Republic of China, Data Security Law of the People's Republic of China.

- Industry-Specific Certifications: Proactively comply with IoT product-specific security standards such as ETSI EN 303 645 and EU RED-DA Directive.

Product Security Certifications

Many of ECOVACS' flagship products have obtained the following authoritative security and privacy certifications, indicating that their security level has reached the international advanced level:

- **ISO 27001 & ISO 27701 Certifications:** ECOVACS has established and continuously operated an information security and privacy information management system compliant with international standards, covering the entire process of robot R&D, manufacturing, App, and cloud services. (Certification Body: BSI, 2021)
- **ETSI EN 303 645 Certification:** ECOVACS' product matrix of floor-cleaning robots and lawn-mowing robots is among the world's first products to pass the European IoT cybersecurity standard certification, verifying its excellent performance in resisting network attacks and preventing data leakage. (Certification Body: TÜV Rheinland, 2021)
- **UL IoT Security Rating Diamond Level Certification:** ECOVACS series products such as X8, X9, T80, and X11 have obtained the highest level of UL IoT Security Rating—Diamond Level (Level 5), indicating that their products meet the requirements of the world's strictest consumer IoT security standards. (Certification Body: UL Solutions, 2025)
- **EU RED-DA Cybersecurity Certification:** Before the mandatory implementation of the EU EN 18031 series standards, ECOVACS

products have taken the lead in passing this certification, meeting the requirements of 14 major categories of security mechanisms, and possessing the cybersecurity access qualification for sales in the EU market. (Certification Bodies: TÜV Rheinland & Intertek, 2025)

- **TÜV Rheinland 2PfG CH0003 Privacy Protection Certification:** ECOVACS ECOVACS HOME App and IoT cloud services have obtained TÜV Rheinland's first privacy protection certification for the floor-cleaning robot category in the Greater China region, passing more than 200 rigorous tests. (Certification Body: TÜV Rheinland, 2021)
- **UK PSTI COC Compliance Statement:** ECOVACS products fully comply with the core requirements of the UK PSTI Act regarding the prohibition of default passwords, transparency of vulnerability disclosure, and security update guarantees, and have published compliance statements on the official website. (Certification Body: TÜV Rheinland, 2024)
- **CQC IoT Security and Personal Information Protection Certification:** ECOVACS products have passed the authoritative evaluation of the China Quality Certification Center, complying with the standards CQC1167-2023 and GB/T 40979-2021, and meeting the regulatory requirements of the Chinese market. (Certification Body: CQC, 2023)
- **AU-ACT COC Certification:** On March 5, 2025, the Australian government officially released the Cybersecurity (Consumer IoT Security Standards) Rules 2025, a core regulation under the Cybersecurity Act 2024. This rule will take effect on March 4, 2026, aiming to address the cybersecurity challenges of smart devices. Our DEEBOT X11 has obtained the first compliance certificate for this regulation from TÜV Rheinland. (Certification Body: TÜV Rheinland, 2025)

Penetration Testing and Third-Party Audits

We firmly believe in "trust, but verify." Therefore, we regularly invite world-class cybersecurity companies to conduct penetration testing and red team exercises on our products, Apps, and cloud platforms. In 2025, we invited Qi'anxin and TÜV SÜD to conduct penetration testing on our products, Apps, cloud platforms, and online mall to proactively identify and fix vulnerabilities. At the same time, we accept supervision and audits of our information security and privacy management systems by third-party audit institutions every year to ensure continuous compliance with standards such as ISO.

A CUT ABOVE THE REST

GOAT G1

1600m²

ECOVACS GOAT G1

Emergency Response and Future Commitments

Security protection is a dynamic and evolving process. ECOVACS is not only committed to building a strong pre-defense system but also establishing an efficient post-incident response mechanism, and pledges sustained investment in security.

Vulnerability Management Process

We attach great importance to security feedback from external sources and have established an open, transparent, and efficient vulnerability collection and response mechanism.

- Official Vulnerability Disclosure Channel: We operate a Product Security Incident Response Team (PSIRT) and a security email, welcoming security researchers, users, and partners to report potential security vulnerabilities to us.
- Standardized Processing Process: For each vulnerability report received, we follow a standardized process of reception-evaluation-fix-release-disclosure, and maintain close and professional communication with the reporter.
- Vulnerability Reward Program: We plan to launch a vulnerability reward program to thank and reward researchers who contribute to the security of ECOVACS products.

Security Incident Response Mechanism

To effectively respond to potential security incidents, we have formulated detailed emergency response plans for security incidents.

- Rapid Response: We are committed to initiating emergency

response within 72 hours of discovering a security incident and notifying regulatory authorities and affected users in accordance with laws and regulations.

- Root Cause Analysis (RCA): A thorough root cause analysis will be conducted for any security incident, and based on this, improvements will be made to our products, processes, and systems to prevent similar incidents from happening again.
- Continuous Monitoring: A 7×24-hour security monitoring system ensures that we can detect abnormalities and take actions in a timely manner.

Continuous Improvement and Future Plans

Security has no end. ECOVACS pledges to take security and privacy protection as a long-term core strategy with sustained investment:

- Forward-Looking Technological Research: We will continue to track cutting-edge security technologies (such as HSM hardware cryptography solutions, AI security) and integrate them into product planning in a timely manner to address future threats.
- Expansion of Compliance System: We will proactively respond to new laws, regulations, and standards continuously introduced worldwide to ensure products continue to meet the access requirements of various national markets.
- Ecosystem and Supply Chain Security: We will extend security requirements to the supply chain and partners to jointly improve the security level of the entire ecosystem.
- User Security Education: We will continue to communicate security best practices with users through various channels to jointly safeguard the security of the smart home environment.

ECOVACS promises to provide users with firmware security update

support for no less than 3 years, ensuring that products can receive the latest security protection throughout their lifecycle.。


PULL
工作中

Building a Trustworthy Intelligent Future Together

At ECOVACS, we firmly believe that true intelligence starts with trust. Every robot entering a home bears not only the responsibility of cleaning the home but also the user's entrustment to us to protect their data security and life privacy.

This white paper systematically elaborates on ECOVACS' systematic thinking, technical practices, and compliance achievements in the field of product security and privacy protection. From secure hardware boot to encrypted cloud storage, from the principle of data minimization to international authoritative certifications, we have built a multi-layered, in-depth, and full-lifecycle protection system. Behind all this is ECOVACS' core philosophy of "**user-centric, Security-by-Design.**"

However, we are well aware that the road to security is long and challenging. We will always maintain a respectful attitude and cooperate closely with users, the security community, industry partners, and regulatory authorities with a transparent and open mindset to jointly address future security challenges.

We promise that ECOVACS will continue to invest resources in security and privacy protection, and constantly consolidate our technical, process, and management systems. Our goal is not only to manufacture excellent cleaning robots but also to become the most trusted intelligent technology partner for users worldwide.

Let us work together to create a cleaner, smarter, and safer future.


ECOVACS Robotics
Committed to innovative technology, safeguarding every family's trust
Learn more:www.ecovacs.com