SolaXCloud
Security White Paper

SOLAX POWER NETWORK TECHNOLOGY (ZHEJIANG) CO., LTD.
Web: www.solaxpower.com
E-mail: info@solaxpower.com

Version: V 1.0

Release Date: 2025.3.18

01 Introduction

1.1 Introduction to SolaXCloud

SolaXCloud is a smart energy management cloud platform created by SolaX Power Network Technology (Zhejiang) Co., Ltd., which deeply integrates the Internet of Things (IoT), big data analysis, artificial intelligence (AI) and edge computing technologies to provide global users with photovoltaic system full life cycle management and energy efficiency optimization services. The platform supports real-time monitoring of photovoltaic power station power generation efficiency, device's operation status, energy storage system charging and discharging and user energy consumption data, generating optimization strategies through intelligent algorithms to help users maximize energy benefits and minimize carbon footprint. As a leader in the digital transformation of clean energy, SolaXCloud always regards data security and privacy protection as our core mission.

1.2 SolaXCloud Security White Paper Objectives

SolaX attaches great importance to security and hopes to lead customers to have a deeper understanding of SolaXCloud's security protection measures through the SolaXCloud Security White Paper. This white paper aims to systematically demonstrate SolaXCloud's full-stack capabilities and innovative practices in the fields of information security, privacy compliance and technical protection. Specific objectives include:

- **Transparent Security Commitment**: Clarify the global security standards and regulatory framework followed by the platform to establish a foundation for user trust.
- **Technical Defense-in-depth Analysis**: In-depth analysis of the multi-layer security architecture design from physical facilities to the application layer.
- **Industry Benchmark Certification display**: Verify the excellence of the platform's security capabilities through international authoritative certification.
- **User Empowerment Guide**: Provide best practice recommendations for users to participate in security co-construction.

Secure Energy Smart Future

CONTENTS

02 Security Protection Values

2.1 SolaXCloud Security Protection Values

SolaXCloud adheres to the concept of "Security as a Service" and builds a security system of "compliance-driven, technology-enabled, and ecological co-governance":

- **Compliance**: Strictly follow global data privacy regulations such as GDPR, CCPA, and PIPL to ensure the legality, transparency, and controllability of data processing.
- **Technical**: Adopt Zero Trust Architecture (ZeroTrust) and Privacy Enhanced Technology (REIS)Achieve data encryption and minimum privilege access throughout the life cycle.
- **Ecological**: Cooperate with industry organizations (such as Qi An Xin, CSA and OWASP) to share threat intelligence and promote the coordinated evolution of energy IoT security standards.

SolaXCloud always puts user privacy and data security first, and builds a full-range protection system through leading technology, transparent strategies, and continuous innovation. We are committed to providing users with safe and reliable energy management services with compliance-driven and dynamically evolving security capabilities, while strictly complying with global data protection regulations, promoting the improvement of industry security standards, and safeguarding the digital future of clean energy.

2.2 External Regulations and Industry Practices Referenced

During the design and operation process, SolaXCloud has been committed to complying with the requirements of data security and privacy protection regulations in various countries, and actively adopting industry best practices to ensure the security, compliance and reliability of the platform. Mainly including:

External Regulations

- **GDPR (General Data Protection Regulation):** As one of the most stringent data protection regulations in the world, GDPR requires SolaXCloud to ensure the legality, transparency and security of data when processing EU user data, and provide users with the right to access, correct and delete data.
- **CCPA (California Consumer Privacy Act:** SolaXCloud follows the requirements of CCPA to clearly inform users of how their data is collected and used, take reasonable and effective measures to protect consumer data, and provide the option of "not selling personal information".
- **PIPL (Personal Information Protection Law, China):** SolaXCloud strictly abides by China's Personal Information Protection Law to ensure that the collection, storage and use of user data complies with the principles of minimization, necessity and legality.
- **NIS2 Directive (EU Cybersecurity Directive):** SolaXCloud refers to the NIS2 Directive to strengthen cybersecurity measures and enhance the protection of critical infrastructure.
- **PSTI (UK Product Safety and Telecommunications Infrastructure Regulation):** For the security of connected devices, SolaXCloud follows the requirements of PSTI to ensure compliance with device password security, vulnerability reporting mechanism and security update cycle.

Industry Practice

- **ISO/IEC 27001 Information Security Management System:** SolaXCloud adopts the ISO 27001 standard and has established a comprehensive information security management system covering risk identification, security control, audit and improvement.
- **NIST Cybersecurity Framework:**With reference to the Cybersecurity Framework of the National Institute of Standards and Technology (NIST), SolaXCloud implements five core functions of identification, protection, detection, response and recovery to ensure the overall security of the platform.
- **ETSI EN 303 645 Standard:** As the baseline standard for cybersecurity of consumer IoT devices, SolaXCloud follows ETSIEN 303 645 to ensure compliance in terms of device password security, vulnerability management and privacy protection.
- **OWASP Top 10:** SolaXCloud refers to the top ten security risks published by the Open Web Application Security Project (OWASP) and implements protection measures for common vulnerabilities (such as injection attacks, cross-site scripting, etc.).
- **Cloud Security Alliance (CSA) Best Practices:** SolaXCloud adopts the guidelines of the Cloud Security Alliance to ensure the security, reliability and compliance of cloud services.

Compliance and Certification

- **Regular Audits and Certifications:** SolaXCloud regularly undergoes third-party security audits and passes international certifications such as ISO 27001, SOC2 and ETSI EN 303 645 to verify the security and compliance of the platform.
- **Industry Cooperation and Information Sharing:** SolaXCloud actively participates in industry security organizations, shares threat intelligence and best practices with peers, and jointly improves the overall security level of the industry.

03 All-round Security Protection

SolaX knows that security protection management methods are as important as security protection technology. Therefore, we have established corresponding management systems and a company-wide security and confidentiality culture from the company management level, while increasing investment in security technology to continuously enhance SolaXCloud's security capabilities. We will introduce how SolaXCloud performs security protection from two aspects: management measures and technical measures.

3.1 Security Protection Management Measures

3.1.1 Governance Framework and Leadership

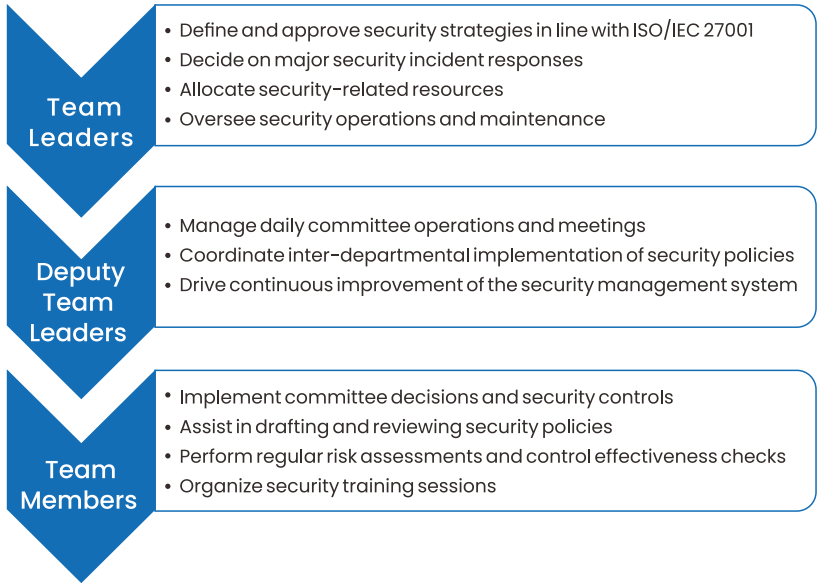
SolaX's leadership attaches great importance to SolaXCloud security, and regards data security and privacy protection as one of the company's core strategies, which is achieved through a top-down governance structure. The implementation of security throughout the company is the core cornerstone of the SolaXCloud platform and the foundation of user trust. As a leader in the field of clean energy, we always regard data security, privacy protection and system reliability as the top priority of corporate development. We firmly believe that only through continuous technological innovation, strict security management and transparent communication can we provide users with truly trustworthy smart energy solutions.

To strengthen information security management, enhance the level of information asset protection, and ensure business continuity and the effectiveness of risk management, the company has established an Information Security Committee in accordance with the international standard ISO/IEC 27001. The committee, composed of key personnel from cross - departmental teams, focuses on promoting inter - departmental collaboration and the integration of professional knowledge, further improving information security, ensuring the stable operation of the organization, and maintaining customer trust.

3.1.2 System and Process

SolaX has built a comprehensive security management system from the system level to ensure that every aspect of the company's operations meets the security requirements of high standards. We have formulated a strict security management system covering data protection, privacy security, network security and physical security, and continuously optimize the management process through regular internal audits and risk assessments.

At the same time, we have established a complete security training mechanism to regularly provide employees with information security, privacy protection and emergency response training to enhance the safety awareness and skills of all employees. Through institutionalized security management, SolaX is committed to providing users with safe and reliable products and services, while laying a solid foundation for the sustainable development of the company.



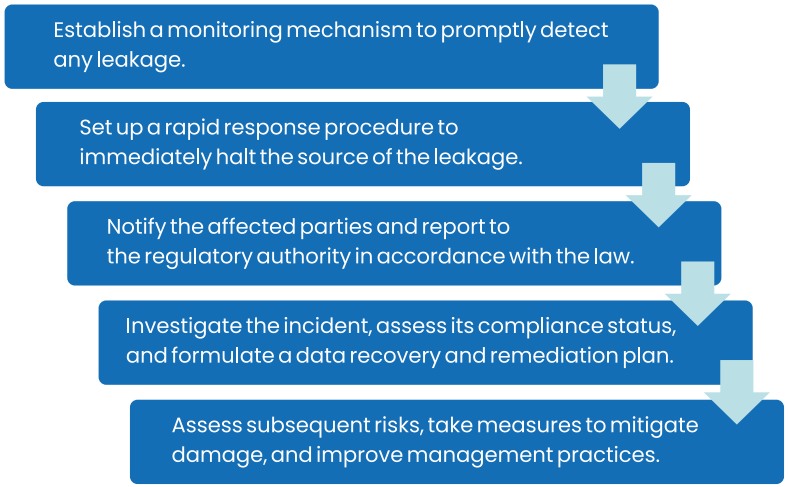
In accordance with the requirements of the ISO/IEC27001:2022 standard issued by the International Organization for Standardization (ISO), combined with the company's actual situation and characteristics, the company uses a process approach, combined with the PDCA management cycle and risk-based thinking methods, and introduces the ISO 27001 information security management system. That is, to ensure that information security awareness is raised throughout the organization, and to timely adjust and optimize processes and measures according to business changes and risk dynamics to ensure that the system is sufficient, appropriate and effective, and to achieve the company's information security policies and goals. More than 30 systems and specifications have been issued, including the "Network Security Management System", "Information Security Management System", "Encryption System Management System", "Cryptography Technology Management System", "Security Operation and Maintenance Management System", "Cloud Service Information Security Management Specifications", and "Third-Party Service Management Security Specifications".

3.1.3 People and Culture

SolaX knows that employees' security awareness training is an important cornerstone to ensure the overall security of the enterprise. We firmly believe that only when every employee has a high level of security awareness and skills can we effectively prevent potential risks and ensure the stability of the company's operations and the security of user data. Therefore, SolaX has established a systematic security training system to regularly provide employees with professional training covering network security data protection, privacy compliance, etc., and help employees identify and respond to security threats in actual work through simulation exercises and case analysis. We are committed to building a team with strong security awareness and high sense of responsibility to escort the company's sustainable development, while also providing users with a safer and more reliable service experience.

SolaX conducts more than 500 internal training sessions throughout the year, including more than 90 sessions related to information security, privacy security, confidentiality awareness and other fields. Based on a comprehensive training management system, we ensure that every employee can receive systematic and multi-level security education, from basic theory to actual combat exercises, to comprehensively improve employees' safety literacy and risk response capabilities. Through regular assessment and feedback mechanisms, we continuously optimize the training content to ensure that it keeps up with the latest industry trends and actual needs. SolaX firmly believes that only through continuous education and practice can a solid security line be built to provide solid protection for the stable operation of the enterprise and the data security of users.

To safeguard the personal privacy of employees, customers, visitors, etc., obtained by the company in its daily operations and ensure proper management of personal information within the company, the company has incorporated data and privacy compliance work into its overall compliance management framework.



Security White Paper
All-round Security Protection

3.1.4 Third-party supplier management

Based on the needs of user services, SolaX may provide some of the user's desensitized data to a third party for entrustment or joint processing, such as sharing inverter operation data with a third party for unified Home Energy Management System (HEMS). The data we provide to third parties does not contain the user's personal data. SolaX has established a strict supplier introduction and management process for suppliers based on privacy and security.

All SolaX's third-party partners must sign NDA and SLA with SolaX. Through NDA and SLA , we establish a strict privacy and data security framework in cooperation with third parties; ensure the protection of confidential information by third parties through NDA; ensure data security through technical measures and service standards stipulated in SLA; respect and protect user privacy rights through transparent policies and response mechanisms. These measures not only meet the requirements of international privacy regulations (such as CCPA and GDPR), but also reflect SolaX's high sense of responsibility for user data security and privacy protection.

3.1.5 Security Emergency Response Mechanism

In today's digital wave, network security challenges are like undercurrents, threatening the stable operation of user data and systems at all times. SolaX deeply understands this severe situation and carefully builds a scientific, efficient and complete security emergency response mechanism. With its excellent foresight and adaptability, it protects customers' data security and business continuity.

SolaX has formed a professional Security Incident Response Team (SIRT). The team consists of experienced security experts, skilled engineers and responsive emergency response personnel. Like vigilant guards, they adhere to the 7x24-hour monitoring mode, using advanced monitoring technology and intelligent analysis tools to capture and evaluate potential security threats in real time, ensuring that any security risks can be discovered at the first time.

Once a suspicious security incident is discovered, SIRT immediately initiates a hierarchical response process, which has been carefully designed and repeatedly optimized, and is highly targeted and operational. SIRT conduct the rigorous and meticulous incident confirmation, accurately identify the nature, scope and severity of the security incident; and operate decisive and rapid threat isolation, timely cut off the attack path and prevent the further spread of the threat; then efficiently and accurately repair vulnerability, deeply explore the root cause of the problem and completely eliminate security risks. Finally, SIRT would make a comprehensive and profound post-event review to summarize the entire incident handling process, analyze the lessons learned, propose improvement measures, as well as continuously optimize the emergency response strategy.

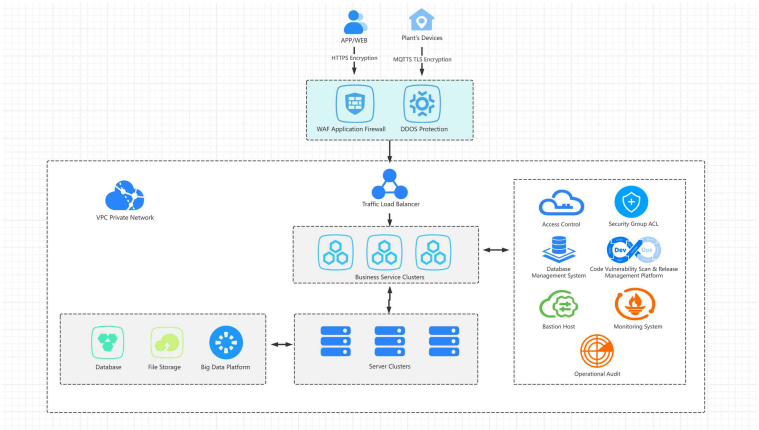
It is worth mentioning that SolaX is well aware of the principle that "good tools are prerequisite to the success" and always insists on conducting emergency drills regularly. Each drill strictly simulates real scenarios and strives to be as close to the complex and changeable network attack environment as possible. During the drill, team members performed their duties and worked together, exercising their rapid response, teamwork and problem-solving abilities. After the drill, SIRT conducted an in-depth analysis and evaluation of the drill results, identified existing problems and deficiencies, and formulated corresponding improvement plans based on the PDCA cycle management concept and put them into practice. Through continuous cycle improvement, the security emergency response mechanism has been continuously optimized and improved, and has always maintained a high degree of adaptability and effectiveness. At the same time, SolaX actively establishes close cooperative relations with authoritative security institutions in the industry, joins the security information sharing platform, conducts regular communication activities, and obtains the latest threat intelligence and defense technologies around the world in a timely manner. Through this in-depth cooperation and data sharing, SolaX can timely gain insight into new attack methods and trends, make preparations in advance, and ensure that it can respond quickly and effectively when facing new attacks.

Security White Paper
All-round Security Protection

3.2 Security Protection Technical Measures

3.2.1 Security Architecture

SolaXCloud adopts a multi-level, full-dimensional security architecture design, covering physical security, network security, data security and application security and other levels.



3.2.2 Cloud Service Security

The SolaXCloud platform leverages the advanced security services offered by cloud service providers and, by integrating our own technological strengths, has constructed a cloud infrastructure characterized by high availability, high reliability, and high security. This infrastructure serves as a robust bulwark to safeguard user data security and ensure the stable operation of the system, thereby minimizing risks and offering users reliable security assurances. Below are the key measures adopted by SolaXCloud in enhancing cloud service security:

VPC (Virtual Private Cloud)

SolaXCloud realizes network isolation by leveraging a Virtual Private Cloud (VPC). It creates an independent virtual network environment for each specific scenario, ensuring the privacy and security of network connections. Meanwhile, the VPC offers flexible access control strategies, effectively preventing unauthorized access and network attacks.

WAF (Web Application Firewall)

By deploying a Web Application Firewall (WAF), SolaXCloud is capable of detecting and blocking common attacks targeting web applications in real-time, including SQL injection, Cross-Site Scripting (XSS), and the like, thereby ensuring the platform's resilience against attacks.

DDoS Protection

SolaXCloud leverages a globally DDoS protection system to effectively mitigate large-scale Distributed Denial-of-Service (DDoS) attacks, ensuring the stable operation of the platform even under malicious high-traffic attacks.

Security Monitoring

SolaXCloud integrates an industry-leading security monitoring system. It collects and analyzes real-time data on the platform's operational status, resource utilization, and security incidents. This enables the operations and maintenance team to promptly identify and respond to potential issues, guaranteeing high availability and security of the system.

Through these comprehensive security measures, SolaXCloud not only meets users' high demands for data security and system reliability but also provides global users with a secure, stable, and efficient smart energy management platform.

3.2.3 Data Security

Communication Security

Applications and devices establish data communication with SolaXCloud via SSL/TLS security protocols. This ensures the confidentiality and integrity of data as it traverses each network topology node, effectively eliminating the risk of eavesdropping or tampering during transmission.

Data Encryption

SolaXCloud encrypts sensitive data stored in its database or file system. By adhering to regulatory requirements, it strengthens data storage security and significantly mitigates the risk of data breaches.

Data Isolation

Currently, in SaaS platforms, multi-tenant architecture has become the mainstream design mode. How to ensure data isolation under multi-tenancy? The current platform uses logical isolation solutions:

Data Backup and Recovery

- Data Backup:
  -SolaXCloud manages the data backup processes for various underlying databases. By establishing disaster recovery mechanisms, it ensures the high availability and security of data in the event of irreversible hardware failures, such as those affecting servers and data centers.
- Data Recovery:
  - SolaXCloud has established an efficient data recovery system. When irreversible hardware failures occur in servers, data centers, etc., lost data can be promptly restored using safe and compliant technical methods.

Security White Paper
All-round Security Protection

3.2.4 Access Control

Authentication

In the digital age, to address the ever-increasing complexity of cybersecurity threats, SolaXCloud has implemented a robust password policy. This policy enforces strict password rules and incorporates multi-layered security measures to comprehensively safeguard the security of user accounts.

Permission Management

Within SolaXCloud, permission management serves as the core mechanism to ensure the security of system access and the integrity of system functions. We have adopted an industry-leading access control framework, which enables flexible and efficient permission allocation and access control, along with fine-grained permission control for users.

- **Minimize Permissions:** Permissions are managed at the finest granularity to grant users only the necessary privileges.
- **Separation of Duties:** Permissions are isolated from each other to avoid any interference or unintended impact between different permission sets.

Session Management

In SolaXCloud, session management maintains the user's identity state to enable authentication and access control, ensuring that only legitimate users can gain access. It employs mechanisms such as generating secure session identifiers and setting timeouts to prevent session hijacking and attacks. Additionally, it ensures data confidentiality and integrity by encrypting session data and restricting access permissions. This comprehensive approach supports SolaXCloud's user-level access security control.

3.2.5 Network Security

We adopt the strategy of "safety first, prevention oriented," meticulously planning our production, office, and R&D networks through zoning and establishing a data center to ensure data security. By implementing multi-dimensional measures including access control, data encryption, security audits, emergency response mechanisms, and comprehensive employee training, we construct a secure and trustworthy network environment. Meanwhile, we enhance network availability and security by adopting measures such as secure access control, firewalls, load balancing, and real-time monitoring, thereby safeguarding the business continuity and data security of the industrial Internet cloud platform and the data center.

Firewall

The firewall is one of the core devices of the network security system, responsible for monitoring and controlling traffic in and out of the company network. SolaXCloud deploys the industry-leading firewall, which can provide multi-level protection to ensure the security of the company's internal network.

- **External Defense Internal Strategy:** This strategy is designed to effectively prevent external threats from infiltrating the internal network while ensuring that attacks on internal systems do not impact the company's external resources.
- **Packet-based DDoS Protection:** By identifying and blocking malicious packets, the firewall can effectively thwart common DDoS attacks, such as TearDrop and Smurf.

DDoS Attack Protection

Distributed Denial-of-Service (DDoS) attacks inundate the target server with an overwhelming number of requests, swiftly depleting network bandwidth or computational resources. As a result, the target server becomes incapable of responding to legitimate requests. Common types of DDoS attacks encompass SYN Flood, UDP Flood, DNS Flood, and ICMP Flood. We employ firewall protection mechanisms and DDoS mitigation strategies to prevent such security incidents.

Intrusion Detection System and Intrusion Prevention System (IDS/IPS)

- **Intrusion Detection and Prevention Overview**
  - Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are employed to identify and respond to abnormal activities within the network, thereby effectively preventing attackers from exploiting the system.
- **Enabled Protection Strategies**
  - Botnet Detection: Conduct real-time monitoring of malware and botnet activities to prevent network devices from becoming the originators of attacks.
  - Vulnerability Analysis and Patch Management: Perform regular vulnerability scans using automated tools and promptly repair any discovered vulnerabilities.
  - SAVE Security Intelligent File Detection: Leverage artificial intelligence technology to analyze potential security threats within files, ensuring that files are free of malicious code.
- **Protection Measures**
  - Traffic Monitoring: Continuously monitor network traffic in real-time, detect abnormal traffic patterns, and implement appropriate defensive measures.
  - Intrusion Response Mechanism: Upon detecting an intrusion attempt, the firewall will automatically initiate response actions, such as traffic blocking and IP banning.

API Security

SolaXCloud attaches great importance to the security of API interfaces and adopts multiple protection measures to ensure the security and reliability of API communication. All API requests are transmitted via SSL/TLS encryption to prevent data from being stolen or tampered with during transmission. At the same time, we implement strict identity authentication and authorization mechanisms to ensure that only authorized users and devices can access API resources.

Content Security

- **Content Security Overview**
  As more and more attacks enter corporate networks through malicious content (such as viruses, Trojans, malicious scripts, etc.), content security protection is particularly important.
- **Enabled Content Security Strategies**
  Sangfor AI-based Vanguard Engine(SAVE): Perform thorough scans on all uploaded files to ensure they are devoid of any malicious code.
  Botnet Monitoring: Analyze abnormal traffic patterns to ascertain whether there is any malicious software control activity.
  Vulnerability Analysis: Perform regular scans and apply patches to both known and potential vulnerabilities, ensuring the system remains in a secure state at all times.

3.2.6 Confrontation Drills

To ensure the security, reliability, and compliance of the SolaXCloud cloud platform, SolaX has established a regularized, multi-dimensional security monitoring and defense system. By leveraging advanced technical approaches such as Red Team/Blue Team exercises, baseline scanning, vulnerability scanning, and penetration testing, and integrating international security standards with a continuous improvement mechanism, SolaX continuously enhances the platform's security baseline capabilities.

(1) Red Team/Blue Team Exercises

Goal: Simulate real-world attack scenarios to verify the effectiveness of the defense system.

(2) Baseline Scanning

Goal: Ensure that system configurations comply with security baseline standards to prevent security vulnerabilities arising from configuration errors.

(3) Vulnerability Scanning

Goal: Proactively identify known vulnerabilities in systems, applications, and dependent libraries.

(4) Penetration Testing

Goal: Thoroughly explore potential security risks, encompassing logical vulnerabilities and business-scenario vulnerabilities.

04 SolaXCloud's Certifications in Security

SolaXCloud has always adhered to the principles of high standards and strict requirements in the field of security. By obtaining a number of international authoritative certifications, it has fully verified the platform's outstanding capabilities in information security, data protection and privacy management. The following are the main certifications SolaXCloud has obtained in terms of security and their significance:

4.1 ISO 27001 Information Security Management System Certification

ISO 27001 is an internationally recognized information security management system standard. SolaXCloud has passed this certification, proving its systematic and standardized information security management:

- A comprehensive information security management system has been established, covering risk identification, security control, auditing and improvement.
- Ensure the confidentiality, integrity and availability of user data, and effectively prevent data leakage and network attacks.
- Enhance user trust in the platform and provide safe and reliable smart energy management services to global users.

4.2 SOC 2 Certification

SOC 2 (System and Organization Controls 2) is a service organization security and privacy control standard established by the American Institute of Certified Public Accountants (AICPA). SolaXCloud is SOC 2 certified, verifying its compliance with security, availability, processing integrity, and privacy protection:

- Ensure that the platform follows strict security and privacy control measures when processing user data.
- Provide transparent audit reports to enhance users' confidence in the platform's security capabilities. Meet the high requirements of international customers for data security and privacy protection, and help expand global business.

4.3 ETSI EN 303 645 Standard Certification

ETSI EN 303 645 is the baseline standard for cybersecurity for consumer IoT devices. SolaXCloud has passed this certification, demonstrating its leading capabilities in IoT device security:

- Ensure that networked devices (such as inverters and energy storage systems) comply with requirements such as password security, hole management, and privacy protection.
- Improve the ability of devices to resist cyber attacks, protect user data and system security,
- Promote the popularization of industry security standards, and set a benchmark for the security of IoT devices.

4.4 PSTI Compliance Certification

PSTI is the UK's mandatory security regulation for connected consumer products. SolaXCloud ensures the legality and security of its products in the UK market through PSTI compliance:

- Prohibit the use of common default passwords to ensure the uniqueness and security of device passwords.
- Provide a clear security vulnerability reporting mechanism so that users can promptly feedback security issues.Clearly define the minimum security update support period for devices to ensure that products are protected throughout their life cycle.

By obtaining ISO 27001, SOC2, ETSIEN 303645 standards and PSTI compliance certification, SolaXCloud not only verifies its outstanding capabilities in information security, data protection and privacy management, but also provides users with a safe, reliable and compliant smart energy management platform. These certifications are not only a reflection of SolaXCloud's security capabilities, but also the fulfillment of our commitment to users. In the future, SolaXCloud will continue to uphold high standards of security, promote the sustainable development of the clean energy industry, and create a safer and smarter energy future for global users.

05 User Security Guide and Suggestions

5.1 User Security Guide

5.1.1 Account Security

SolaXCloud recommends setting a strong password, as follows.

Steps:

Log in to your SolaXCloud account and go to "Personal Center" ➧ "Password Settings"
Enter the current password, new password, and confirm password.
The new password must meet the following requirements:
- Length 6-32 characters.
- Contain at least 3 characters of uppercase and lowercase letters, numbers, and special symbols (symbols support @#$%^&*_+-.!?)

Save the new password to avoid reusing the old password.

Notes:

Do not use easily guessed information such as birthdays and names.
It is recommended to update the password every 3 months.

5.1.2 Network Connection Security

Suggested Operations:

Use An Encrypted Network: Make sure the Wi-Fi to which the device is connected has WPA3 or WPA2 encryption enabled.
Isolate IoT Devices: Use a router to divide photovoltaic devices and other home devices into independent networks.
Disable Remote Access (unless necessary): Turn off the "remote management" function in the device settings.

5.1.3 Phishing Attack Prevention

Common Phishing Forms:

Forged emails or text messages on the SolaXCloud login page to induce the user to enter the account password.
Impersonate customer service to ask for device verification codes.

Countermeasures:

Official links are only accessible through the *www.solaxcloud.com* domain.
Do not click on links from unknown sources, but log in to the platform directly.

5.2 Resources and Support

Users can obtain corresponding resources and support in the "Help center" in the "Service" module.
The main contents include: Online service, Hot line, Service group, Feedback, and User Guide.

06 Conclusion

In today's rapidly developing digitization and intelligence, SolaXCloud always puts user privacy and data security first, and is committed to providing global users with a safe, reliable and efficient smart energy management platform. Through strict security management measures, leading technical means and comprehensive security certification, we have built a multi-level, all-round security protection system to ensure the security, integrity and privacy of user data during transmission, storage and use.

SolaXCloud not only complies with international and regional data protection regulations such as GDPR, CCPA, PIPL, etc., but also actively adopts industry best practices such as ISO27001, SOC2, ETSIEN 303 645 and other standards to ensure the security and compliance of the platform. We are well aware that security is a process of continuous improvement, so we continue to optimize security strategies and enhance security capabilities to cope with increasingly complex cybersecurity threats.

In the future, SolaXCloud will continue to uphold high standards of security concepts and promote the sustainable development of the clean energy industry. We believe that only through continuous technological innovation and security practices can we create a safer and smarter energy future for users. Thank you for your trust and support for SolaXCloud. We will continue to provide you with safe and reliable services and work together towards a bright future of green energy.