EcoFlow

Security&Privacy Compliance White Paper

EcoFlow Inc.

2024.9

Legal Disclaimer

Preface

EcoFlow, founded in 2017, focuses on personal and household clean energy storage, dedicated to providing global users with simple, flexible, and reliable power solutions. As a global leader in clean and smart energy, EcoFlow continuously innovates and achieves technological breakthroughs. With the vision of "Empowering every home with energy independence," we are committed to creating portable and sustainable new energy solutions, opening a new, clean, and accessible power ecosystem for users worldwide. We strictly comply with all applicable rules governing our business activities, including but not limited to Chinese laws, international standards and practices, as well as the laws and regulations of the countries where we operate. Additionally, we are committed to fully integrating security and privacy compliance management into our internal corporate governance.

TABLE OF CONTENTS

1.EcoFlow’s Security Vision

1.1 Information Security Objectives

EcoFlow is committed to ensuring data security and privacy, providing reliable and sustainable energy services, and earning the trust of users worldwide. We have established the following information security objectives:

- **Protect Users' Private Data：** Protect the privacy and security of users' data, ensuring comprehensive protection throughout the entire product lifecycle.
- **Strengthen Cybersecurity Protections：** Build a multi-layered cybersecurity defense system to withstand external threats, such as hacking attacks, virus intrusions, and more.
- **Ensure System Stability and Reliability：** Ensure the continuous and stable operation of software and hardware platforms for mobile and home energy storage systems, minimizing unplanned downtime.
- **Enhance Users Trust：** Strengthen users trust in the products through transparent privacy policies and robust security measures.
- **Supply Chain Security：** Conduct security audits at all nodes of the supply chain to ensure that third-party suppliers and service providers comply with the company's security standards.

1.2 Security Compliance Strategy

EcoFlow's security compliance strategy covers the following key areas:

- **Establish a Security Management System：** Establish and improve the information security management system based on international standards such as ISO/IEC 27001, ensuring the confidentiality, integrity, and availability of information assets.

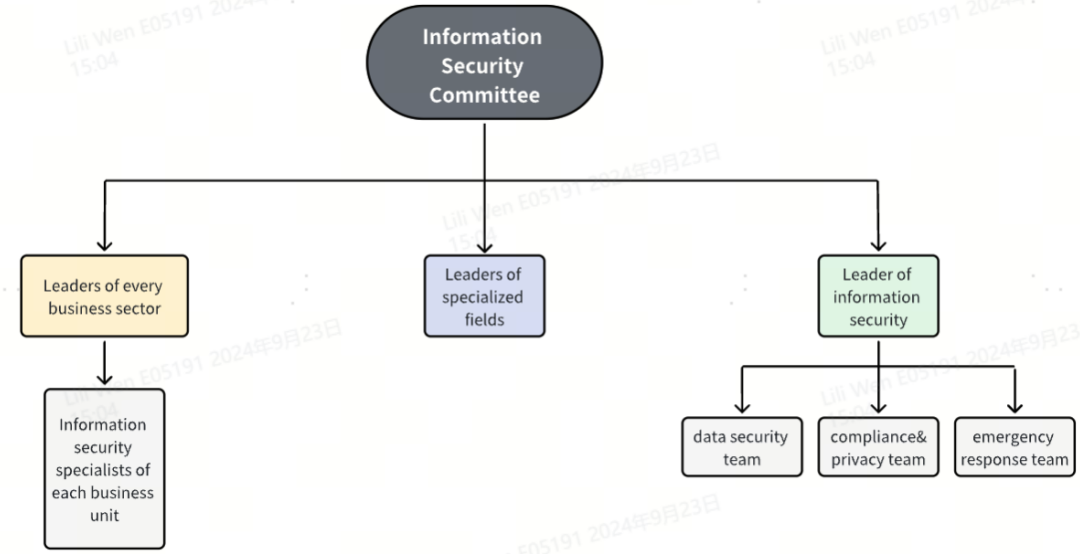
- **Compliance with Laws and Regulations:** Ensure that company operations comply with all applicable laws, regulations, and industry standards.
- **Security Protection System**: Establish a multi-layered security protection system that includes data encryption, access control, and cybersecurity measures.
- **Strengthen Employee Security Awareness**: Conduct regular information security training to enhance employees' awareness and skills, and encourage their active participation in security practices.
- **Emergency Response**: Establish an efficient incident response team and processes to ensure swift reactions in the event of a security incident, minimizing losses to the greatest extent possible.
- **Auditing and Monitoring**: Maintain transparent auditing and monitoring mechanisms to ensure the effectiveness and compliance of security measures.
- **Continuous Improvement and Monitoring:** Establish a continuous improvement mechanism to regularly review the effectiveness of information security policies and adjust them according to emerging threat landscapes.

2. Security and Privacy Compliance

2.1 Security Organizational Structure

EcoFlow places a high priority on information security and privacy protection. To promote the security and compliance management of the company's products and services, effectively identify, proactively manage, prevent, and address security compliance risks, and enhance security compliance awareness among all employees, the company has established a Security and Compliance Committee. This committee serves as the highest

decision-making body in the field of security and compliance management. The committee is chaired by the company's COO, with members and subcommittee chairs consisting of senior executives from various business systems and the company's Chief Compliance Officer. Accordingly, the following organizational structure has been established:



- **Information Security Committee**

As the highest management body for information security and privacy compliance at EcoFlow, it reports to the company’ s top decision-making authority. Composed of the heads of various business and specialized fields, it is responsible for making decisions and approving the company’ s information security and privacy compliance strategies and execution.

- **Leaders of Every Business Sector**

The highest authority for information security and privacy protection within the business sector and center, responsible for providing decision-making and support for the implementation of information security and privacy compliance efforts.

- **Leaders of Specialized Fields**

As the head of this specialized field, responsible for evaluating and making decisions regarding standards, regulations, and strategies for information security and privacy compliance.

- **Leaders of Information Security**

Provide support for promoting and implementing technical and managerial measures, determining the direction and goals of data security and privacy protection management work; establish a cross-organizational data protection task force to create a cohesive management effort.

- **Information Security Officer of Each Business Unit**

From the perspective of the company's business areas, evaluate the current information security and privacy protection strategies by analyzing business scenario information, and propose improvement plans.

- **Data Security Team**

Based on the company's information security objectives, develop security strategies for each stage of the data security lifecycle, establish a data protection system, and organize data security awareness training programs.

- **Compliance&Privacy Team**

Based on the company's privacy compliance objectives, establish a privacy compliance protection system, and develop and maintain privacy protection policies and related processes to ensure that the company's applications, products, and services comply with domestic and international privacy compliance requirements.

- **Emergency Response Team**

Provide a unified response and traceability for external cybersecurity and privacy incidents.

2.1.1 Security & Privacy Compliance Training

- **Privacy Training Program**: Provide regular privacy compliance training for members of the information security team, including the latest security technologies and industry best practices, to ensure the team's expertise remains at the forefront of the industry.
- **Company-wide Security Awareness**: Implement a comprehensive security compliance awareness training program to ensure all employees understand their roles and responsibilities in protecting the company's information assets.
- **Continuous Advocacy Mechanism**: Establish a continuous advocacy mechanism that encourages employees to engage in learning about the latest security regulations, technologies, and trends to adapt to the ever-changing security landscape.
- **Promotion of Corporate Security Culture**: Strengthen the corporate security culture through training and awareness activities, enhancing employees' understanding of the importance of security compliance and promoting the adoption of security best practices.

2.2 Security & Privacy Compliance Framework

The EcoFlow Security & Privacy Compliance technical architecture primarily focuses on three areas: secure development, security protection, and privacy compliance, aiming to build an efficient, reliable, and secure system.

- **Security Research&Development**: Adopt secure coding standards and development processes to minimize security vulnerabilities from the outset. Conduct security testing and assessments at every stage of product development to ensure product security.
- **Security Protection**: Deploy multi-layered security measures, including network firewalls, intrusion detection systems, antivirus software, etc., to safeguard systems and data. Additionally, conduct regular vulnerability scans and patch updates to identify and address potential security threats promptly.

- **Privacy Compliance**: Adhere to relevant privacy regulations and standards, including but not limited to the Personal Information Protection Law of the People's Republic of China and the General Data Protection Regulation (GDPR), ensuring the lawful and compliant collection, use, storage, transmission, and destruction of user data. Implement classified management of user data and utilize technical measures such as encryption and anonymization to protect user privacy.

2.3 Security Compliance Certification

To demonstrate our commitment to user security and privacy protection, EcoFlow has successfully obtained multiple authoritative certifications, both domestically and internationally. These certifications cover key areas such as data security, privacy protection, and smart hardware.

2.3.1 Data Security&Privacy Certification

EN certification（EN 303 645）

EN 303 645 is a cybersecurity standard for consumer Internet of Things (IoT) devices, aimed at ensuring the security of IoT devices and preventing potential cyberattacks.

TRUSTe Enterprise Privacy Certification

EcoFlow has obtained TRUSTe certification, which signifies that we have achieved higher standards in privacy policies and data protection. The TRUSTe certification demonstrates that we strictly adhere to privacy-related controls, ensuring compliance and transparency in data management and privacy protection. We are committed to providing users with a more secure and trustworthy experience.

NISTIR 8259

NISTIR 8259 provides cybersecurity guidelines for IoT devices, helping

manufacturers ensure that their devices are equipped with fundamental cybersecurity features and safeguard data privacy.

NISTIR 8425

NISTIR 8425 is a supplement to NISTIR 8259, providing additional operational guidelines to ensure that IoT devices protect data privacy and security during operation.

SB 327

SB 327 is California's IoT device security law, requiring devices to have reasonable security features to protect user privacy.

2.3.2 Smart Hardware Solution Certification

PSTI

PSTI certification originates from the UK's IoT device security law, aimed at ensuring that consumer IoT devices are protected from cyberattacks, preventing data breaches and privacy violations. This law reflects the growing need for IoT device security and mandates that manufacturers implement reasonable security measures to safeguard devices and user data.

FCC SDOC

FCC SDOC is a self-declaration certification that ensures products comply with the Federal Communications Commission's (FCC) electromagnetic compatibility standards, primarily applicable to communication devices.

MIC (TELEC)

MIC (TELEC) is a certification in Japan for radio equipment, ensuring that devices comply with wireless spectrum usage regulations to prevent unlawful interference.

SRRC

SRRC is the certification for radio equipment in China, ensuring that devices comply with regulations when used in the Chinese market, preventing frequency interference and indirectly ensuring communication security.

ISO 13849

ISO 13849 is a functional safety standard for machinery, primarily focused on the control systems of industrial equipment, ensuring the proper operation of safety functions.

2.3.3 System Certification

ISO 9001：2015 - Quality Management System Certification

ISO 9001 is an international standard that specifies the requirements for establishing and maintaining an effective Quality Management System (QMS). This standard applies to any organization seeking to improve the quality of its products or services and enhance customer satisfaction. Companies that achieve ISO 9001 certification demonstrate strong management capabilities in the following areas:

- Continuously meet customer and legal regulatory requirements.
- Continuously improve customer satisfaction.
- Effectively implement process control and risk management.

2.4 Data Security and Privacy Protection

2.4.1 Data Ownership Statement

- **Data Owner**: Individual users are the owners of their personal data, and the data belongs to the individual users.
- **Data Controller**: In the products or services provided to users by EcoFlow, EcoFlow determines the purposes of personal data collection, the scope of collection, and the methods of processing.

- **Data Processor**: EcoFlow's service providers process personal data according to EcoFlow's instructions, ensuring and enhancing the agreed-upon services and continuously providing them to individual users.

2.4.2 Protection of Individual Privacy Rights

EcoFlow respects and protects users' personal privacy rights and provides corresponding safeguards.

2.4.2.1 Right of Access

Users have the right to obtain a copy of the personal data we hold about them, as well as certain information related to how we process their personal data.

2.4.2.2 Right to Rectification

If a user's personal data is inaccurate or incomplete, the user has the right to request a correction. Users can log into their accounts at any time to directly update their details or contact us via email to update their personal data.

2.4.2.3 Right to Erasure

Users can request that EcoFlow delete their personal data. However, please note that we may not always be able to comply with a deletion request due to specific legal reasons. If applicable, we will inform users of this at the time of their request.

2.4.2.4 Right to Restrict Processing

A user may request the restriction of the processing of their personal data in certain circumstances. In the event of such a restriction, we may retain sufficient information about the user to ensure future compliance with that restriction.

2.4.2.5 Right to Data Portability

A user may request a copy of their personal data, or request the transfer of their personal data to another company. Please note that this right only applies to the automated data which the user initially consented to our use of, or where we used the data to fulfill a contract with the user.

2.4.2.6 Right to Object to Processing

Users have the right to object to the processing of their personal data for targeted advertising purposes.

2.4.2.7 Right to Withdraw Consent

Users may withdraw their previous consent to the use of their personal data at any time. If users withdraw consent, we may no longer be able to provide access to certain specific services. Please note that any use or disclosure of users' personal data prior to the withdrawal of consent will not be affected by such withdrawal.

2.4.2.8 Right to Object to Automated Decision-Making

When we engage in automated decision-making or analysis while processing your personal data, you have the right to request human intervention. This form of processing is permitted if it is necessary for the performance of a contract between us and the user, required by law with appropriate safeguards, or based on the user's consent. Users may notify us via our external email address to opt out of such automated decision-making and analysis.

We will make every effort to respond to all valid, verified requests within one month or as required by law. Occasionally, if a request is particularly complex or if multiple requests have been made, we may need more than one month. In such cases, we will inform the user and keep them updated on the progress.

We may need to request specific information from the user to help us confirm their identity in accordance with applicable law. This is a security measure aimed at preventing the unauthorized disclosure of personal data.

2.4.2.9 Right to Lodge a Complaint

If users have any concerns or complaints about how we handle their data, they can contact us via email. Users also have the right to lodge a complaint with a data protection supervisory authority. If possible, please contact us first so we can assist you in the most effective way.

2.4.3 Data Lifecycle Security Management

To ensure the security of data throughout its entire lifecycle, we have implemented systematic data lifecycle management measures. From data collection, usage, storage, transmission, modification, to destruction, we enforce strict security controls at every stage. Upon collection, data is encrypted and classified, ensuring that only authorized personnel have access. During the storage phase, we use advanced encryption technologies and conduct regular security audits to prevent unauthorized access. While data is in use, we safeguard its security through access controls and monitoring measures. In the final destruction phase, we use secure and scientific methods to ensure that data is irrecoverable, preventing any potential data breach risks. Through these measures, we ensure the confidentiality and integrity of data throughout its entire lifecycle.

2.4.4 Data Security Governance

We ensure data protection and compliance by establishing a comprehensive data security governance framework. A dedicated data security team is responsible for developing and implementing data security policies, enforcing strict access controls and encryption measures, and conducting continuous monitoring and audits. We adhere to regulations such as GDPR and CCPA,

regularly reviewing and updating data security strategies to adapt to evolving threats and technological environments. Through these measures, we are committed to maintaining the integrity and confidentiality of data while ensuring ongoing business compliance.

2.4.5 Privacy Compliance

EcoFlow protects the personal information shared with us by strictly adhering to the principles of legality, fairness, and necessity. We implement the following compliance measures:

1. Through the Privacy Policy, we clearly, transparently, and comprehensively inform users about the collection and use of their personal information. The company has made the Privacy Policy available on the official website and mobile application interface, providing users with clear and complete details about the collection and use of personal information, including but not limited to the types of personal information collected, the scenarios and purposes of use, device permissions accessed, cookies and similar technologies, third-party SDKs, the sharing, transfer, disclosure, and storage of personal information, users' rights regarding their personal data, protection of minors, and channels for complaints and contact.

2. In the product feature settings, users are only required to provide the necessary data when using certain functions or services. Prior to this, we will seek the user's consent to obtain the corresponding device permissions. Users can choose to withdraw or disable authorization at any time.

3. Based on the sensitivity and scope of the data, we implement strict classification management and secure access control for the database. Only administrators with the appropriate permissions can manage and view the corresponding user data. Additionally, we place great importance on assessing the data security impact of our products and services, continuously advancing and updating our data security management processes.

4. In terms of adopting technical security tools, we utilize various encryption strategies to ensure the security of data throughout its entire lifecycle, including during collection, usage, storage, transmission, and deletion.

5. When it comes to downloading and using the app, users have the right to independently decide whether to download and use the app, as well as whether to share their personal information with us. The purpose of providing the app is to enhance the user experience, including features such as device status monitoring, function settings, remote control, and OTA updates.

6. For third-party data authorization and sharing, we have established strict control measures, including but not limited to providing prior notice to users and obtaining their consent, assessing the third party's data security management capabilities, and agreeing on and binding all parties' responsibilities for personal data protection through contracts and personal information security clauses.

2.4.6 Privacy Impact Assessment (PIA)

EcoFlow has established a Data Protection Impact Assessment (DPIA) process to ensure privacy compliance is embedded in product design. The DPIA is implemented for significant and emerging technological developments, product designs, or operational activities that involve personal data processing. This process identifies potential risks to the rights and freedoms of individuals resulting from the processing activities and introduces appropriate risk management measures.

Implementing a DPIA helps effectively manage privacy compliance risks. Organizations should conduct a DPIA in advance when:

- Processing sensitive personal information;
- Using personal information for automated decision-making;
- Entrusting the processing of personal information, providing personal information to other processors, or publicly disclosing personal information;

- Transferring personal information abroad;
- Engaging in other personal information processing activities that significantly impact individual rights.

According to the GDPR, conducting a DPIA is also mandatory when data processing activities are "likely to result in a high risk to the rights and freedoms of natural persons."

2.4.7 Vendor Security & Privacy Compliance Audit

EcoFlow places a high priority on the security and privacy management of its vendors, with a comprehensive internal vendor security management framework in place. During the provision of services, EcoFlow authorizes only trusted third-party data processors to participate in necessary data processing activities. We rigorously review every stage of the vendor's data lifecycle according to these standards. For new vendors, we conduct a thorough risk assessment to ensure they have adequate security and privacy protection capabilities. Based on the assessment results, we may require the signing of agreements such as NDAs, DPAs, or SCCs to ensure data security and compliance.

2.5 Cloud Security

2.5.1 Cloud Infrastructure Security

EcoFlow leverages industry-leading cloud service providers, including AWS, Azure, Tencent Cloud, and Alibaba Cloud, to build a comprehensive security framework. Our key security measures include:

- **Identity and Access Management**: Ensuring account security through fine-grained permission controls and multi-factor authentication (MFA).
- **Data Protection**: Utilizing advanced data encryption services to ensure the confidentiality and integrity of the data.

- **Security Monitoring and Response**: Real-time monitoring of system status with rapid response and handling of security incidents.
- **Multi-Region Deployment**: Deploying multiple data centers globally to enhance system availability and redundancy.
- **Cross-Platform Integration**: Ensuring secure integration between different cloud platforms, safeguarding the security of data flow and service access across platforms.
- **High Availability and Disaster Recovery**: Implementing high availability solutions and disaster recovery strategies to ensure continuous and stable business operations.

2.6 Endpoint Devices Security

2.6.1 App User-End Security

To ensure the security of the app, EcoFlow employs advanced code hardening and encryption techniques to protect the application and its data. We ensure that communication uses TLS/SSL encryption and implement strict input validation to prevent common attacks. During compliance reviews, we rigorously adhere to relevant data protection regulations (such as GDPR and CCPA) and industry standards, conducting detailed security audits and vulnerability scans. Our release process includes comprehensive security testing and reviews, ensuring that all functions meet security requirements before the app is officially launched, safeguarding user security and privacy.

2.6.2 IoT Device Security

To ensure the security of IoT devices, EcoFlow implements comprehensive security measures, including certificate management for device identity verification, the use of TLS protocol to encrypt communication between devices and servers, and secure firmware and software updates via Over-the-

Air (OTA) mechanisms. These measures ensure the confidentiality and integrity of data, as well as the continuous security of devices, effectively preventing unauthorized access and cyberattacks.

2.6.3 Continuous Improvement of Security Measures

EcoFlow recognizes that the constantly evolving cybersecurity landscape requires us to continuously update and improve our security measures. We are committed to maintaining and enhancing endpoint security through the following key areas:

- **Continuous Monitoring**: We continuously monitor the security posture to quickly identify and respond to new security threats and vulnerabilities.
- **User Education**: We provide regular security education and best practice guides to raise user awareness of security issues and enhance their ability to protect themselves.
- **Technological Iteration**: We continuously research and deploy the latest security technologies to ensure our security measures can defend against increasingly sophisticated cyberattacks.

2.7 Secure Development

EcoFlow follows secure development best practices by integrating security into every stage of the product development lifecycle. From requirement analysis, design, coding, and testing to release, each phase adheres to strict security standards and processes.

2.7.1 Security Requirement Analysis

During the requirement analysis phase, we identify potential security risks and requirements and incorporate them into the overall project planning. Through

security reviews, we engage in thorough communication with the business team, discussing specific business logic, processes, and technical frameworks to ensure a clear and consistent understanding of the security requirements on both sides.

2.7.2 Product Security Design

During the product design phase, we prioritize security by adhering to the following nine security design principles: "Defense in Depth," "Minimizing Attack Surface," "Least Privilege," "Separation of Duties," "Secure by Default," "Fail-Safe," "Protect the Weakest Link," "Psychologically Acceptable," and "Privacy Protection." These principles guide our design process to reduce the potential attack surface and enhance overall security.

2.7.3 Security Control During the Development Phase

During the development phase, we ensure comprehensive security control through strict code reviews, static analysis, and open-source component approval measures. These processes help identify and mitigate potential vulnerabilities early in the development cycle.

Code Review: The review process focuses on identifying security issues in the code, such as input validation, error handling, and access control. It also includes evaluating compliance with secure coding standards to ensure the code adheres to best security practices.

Static Analysis: Utilize static code analysis tools to automatically detect security vulnerabilities in the code, ensuring potential issues are identified and resolved before release.

Open Source Component Admission: Conduct security evaluations for all open-source components, including verifying their source, version, and known security issues. Only verified and well-maintained components are allowed to be introduced and used.

2.7.4 Security Testing and Vulnerability Remediation

To ensure that our products and services meet the highest security standards, we have implemented a comprehensive security testing strategy and established an effective closed-loop vulnerability management mechanism. These measures help us respond quickly when security vulnerabilities are discovered and ensure that they are promptly addressed.

2.7.4.1 Safety Test

- **Dynamic Testing**: Use Dynamic Application Security Testing (DAST) tools to detect security vulnerabilities in applications during runtime, simulating attacks to assess the system's security.
- **Penetration Testing**: Conduct regular penetration tests, where professional security teams simulate attacks to evaluate the system's defense capabilities and provide recommendations for improvements.

2.7.4.2 Closed-loop Vulnerability Management

- **Vulnerability Detection**: Vulnerabilities identified during security testing and code reviews are recorded and categorized, ensuring each vulnerability is effectively tracked and addressed.
- **Vulnerability Remediation**: Discovered vulnerabilities are assigned to the relevant developers or security teams for remediation. The process includes analyzing the vulnerability, developing a fix plan, implementing the fix, and performing validation testing to ensure the issue is resolved.
- **Remediation Validation**: After the fix is completed, retesting is conducted to ensure the vulnerability has been successfully resolved and that the remediation has not introduced any new issues.
- **Updates and Documentation**: Once remediation is complete, update the relevant security documentation and vulnerability records to ensure all information is properly maintained. Include the details of vulnerability fixes

and improvements in regular security audit reports.

- **Feedback Mechanism**: Establish a feedback mechanism to share discovered vulnerabilities and remediation experiences with the team, in order to improve development and testing processes and enhance future security protection.

2.8 Business Continuity

Ensuring business continuity during security incidents or unexpected events is a key component of our security strategy. We ensure business continuity and recovery capabilities through the following measures:

- **Risk Assessment and Business Impact Analysis (BIA)**: Conduct regular risk assessments and BIAs to identify potential threats and risks that could impact business operations. These evaluations help assess the impact on business functions and prioritize critical business functions accordingly.
- **Business Continuity Plan**: Develop a detailed business continuity plan, including recovery time objectives (RTO) and recovery point objectives (RPO), backup strategies, key resources, and personnel arrangements. This ensures that business operations can be maintained through backup solutions when primary systems or facilities are unavailable.
- **Data Backup and Recovery**: Implement a regular data backup strategy, storing backup data off-site or in cloud environments. Regularly test the data recovery process to ensure that business operations can be quickly restored in the event of data loss or system failure.
- **Emergency Response and Communication**: Establish an emergency response plan and communication strategy to ensure a swift response during security incidents. Provide timely information to employees, users, and other stakeholders to minimize confusion and impact.

- **Drills and Training**: Conduct regular business continuity and disaster recovery drills, simulating different scenarios to test the effectiveness of the plans. Provide employees with business continuity and emergency response training to ensure they understand their roles and responsibilities.
- **Plan Updates and Improvement**: Regularly review and update the business continuity plan, continuously improving it based on new threat scenarios, technological changes, and drill outcomes to ensure its effectiveness and adaptability.

Conclusion

In this white paper, we provide a detailed overview of the strategies and measures in place for data security, privacy protection, disaster recovery, and business continuity. By implementing stringent security controls, conducting regular risk assessments, and maintaining continuous improvement and training, we are committed to protecting users' data and ensuring business security.

Our goal is to offer users a secure and reliable service environment, with the ability to respond swiftly and recover from various challenges. We recognize that security is not just a technical issue but a commitment to earning and maintaining user trust. We will continue to invest in cutting-edge technologies and best practices to ensure that our systems and processes are prepared to face future security threats and business challenges. If you have any questions or need further information, please do not hesitate to contact us.