正浩创新

安全&隐私合规白皮书

深圳市正浩创新科技股份有限公司

2024 年 9 月

法律声明

前言

EcoFlow 成立于 2017 年，专注于个人与家庭清洁储能领域，致力于为全球用户提供简单+灵活+可靠的用电方式，作为清洁与智慧能源的全球行业领跑者，EcoFlow 不断实现技术的创新与突破，我们以“注力全球家庭实现能源自主”为愿景，致力于创造便携、可持续的新能源解决方案，为全球用户开拓清洁普惠的电力新生态。我们严格遵守所有可适用的业务活动规则，包括但不限于中国法律、国际标准和惯例以及业务经营地的法律法规，并坚持将安全&隐私合规管理全面融入公司内部管理之中。

目录

1.EcoFlow 安全愿景

1.1 信息安全目标

EcoFlow 致力于保障数据安全与隐私，实现可靠、可持续的能源服务，赢得全球用户的信任。我们确立了以下信息安全目标：

- **保护用户隐私数据：**保护用户数据的隐私和安全，确保其在产品全生命周期中得到全面保障。
- **强化网络安全防护：**构建多层次的网络安全防御体系，抵御外部威胁，如黑客攻击、病毒入侵等。
- **保障系统稳定与可靠性：**确保移动储能和家庭储能系统的软件与硬件平台持续稳定运行，减少非计划停机时间。
- **增强用户信任：**通过透明的隐私政策和强大的安全措施，增强用户对产品的信任。
- **供应链安全：**对供应链中的各个节点进行安全审计，确保第三方供应商和服务提供商符合公司的安全标准。

1.2 安全合规战略

EcoFlow 的安全合规战略涵盖以下几个关键方面：

- **建立安全管理体系：**依据 ISO/IEC 27001 等国际标准，建立和完善信息安全管理体系，确保信息资产的保密性、完整性和可用性。
- **法律法规遵守**：确保公司运营符合所有可适用的法律法规和行业标准。
- **安全防护体系**：建立包含数据加密、访问控制和网络安全的多层次安全防护体系。
- **强化员工安全意识**：开展定期的信息安全培训，提高员工的安全意识和技能，鼓励他们参与安全实践。
- **应急响应**：建立高效的事件响应团队和流程，确保在发生安全事件时能够迅

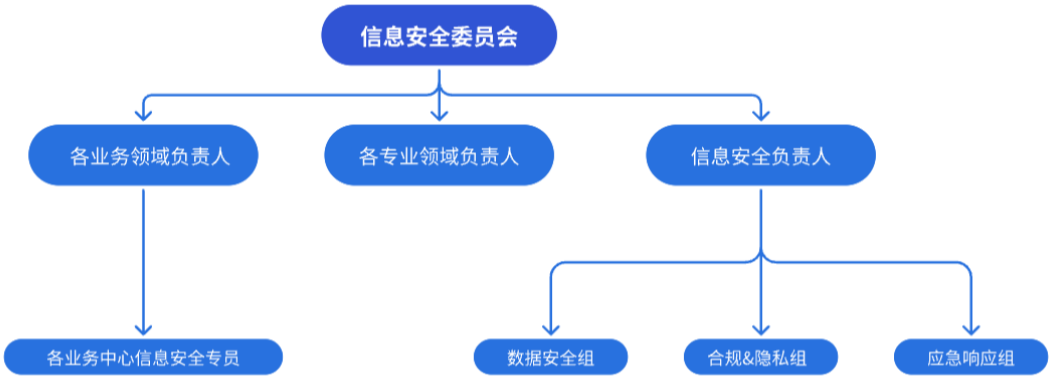
速反应，最大限度减少损失。

- **审计与监控**：保持透明的审计和监控机制，确保安全措施的有效性和合规性。
- **持续改进与监控：**建立持续改进机制，定期审查信息安全策略的有效性，并根据新的威胁形势进行调整

2.安全与隐私合规

2.1 安全组织结构

EcoFlow 高度重视信息安全与隐私保护，为促进公司产品与服务的安全合规管理，有效识别和主动管理、防范、处置安全合规风险，提高全体员工安全合规意识，公司成立安全合规委员会，作为公司安全合规管理领域最高级别的领导决策机构。安全合规委员会主任由公司 COO 担任，委员及分委会主任由各业务系统高管及公司首席合规官担任。为此建立了以下组织结构：



- **信息安全委员会**

作为 EcoFlow 信息安全与隐私合规保护的最高管理机构，向公司经营最高决策机构汇报。由公司各业务领域和专业领域负责人组成，负责决策和批准公司的信息安全与隐私合规战略和执行。

- **各业务领域负责人**

该业务领域与中心信息安全&隐私安全的最高负责人，为信息安全与隐私合规安全工作的落实提供决策和支持。

- **专业领域负责人**

作为该专业领域的负责人，为信息安全与隐私合规安全的标准、规范、策略进行评估与决策。

- **信息安全负责人**

对技术和管理执行的推动和落实提供支持，确定数据安全与隐私保护管理工作的方向和目标；建立跨组织的数据保护横向团队，形成管理合力。

- **各业务中心信息安全专员**

从公司业务领域角度，综合业务场景信息，评估当前的信息安全与隐私保护策略，给出改进方案。

- **数据安全组**

依据公司信息安全目标，制定数据安全生命周期各环节的安全策略，建立数据安全保护体系，组织开展数据安全意识培训。

- **合规&隐私组**

依据公司隐私合规目标，构建公司隐私合规保护体系，制定、维护隐私保护政策及相关流程确保公司应用系统、产品、服务符合境内外隐私合规要求。

- **应急响应组**

统一响应、溯源外部网络安全与隐私事件。

2.1.1 安全&隐私合规培训

- **隐私培训计划**：为信息安全团队成员提供定期的隐私合规培训，包括最新的安全技术和行业最佳实践，确保团队的专业能力保持行业领先。
- **全员安全意识**：实施全面的安全合规意识培训计划，确保所有员工了解他们在保护公司信息资产中的角色和责任。
- **持续宣贯机制**：建立持续宣贯机制，鼓励员工参与最新的安全法规、技术和趋势的学习，以适应不断变化的安全环境。
- **企业安全文化推广**：通过培训和宣传活动，强化企业安全文化，提高员工对安全

合规重要性的认识，促进安全最佳实践的普及。

2.2 安全&隐私合规架构

EcoFlow 安全&隐私合规技术架构主要聚焦在安全研发、安全防护、隐私合规三个方面，致力于构建一个高效、可靠、安全的系统。

- **安全研发**：采用安全的编码规范和开发流程，从源头上减少安全漏洞的出现。在产品研发的各个阶段，进行安全测试和评估，确保产品的安全性。
- **安全防护**：部署多层级的安全防护措施，包括网络防火墙、入侵检测系统、防病毒软件等，保障系统和数据的安全。同时，定期进行安全漏洞扫描和修复，及时发现和处理潜在的安全威胁。
- **隐私合规**：遵循相关的隐私法规和标准，包括但不限于《中华人民共和国个人信息保护法》、《通用数据保护条例》（GDPR）等，确保用户数据的采集、使用、存储、传输和销毁合法合规。对用户数据进行分类管理，采取加密、匿名化等技术手段保护用户隐私。

2.3 安全合规认证

为展示我们对用户安全和隐私保护的承诺，EcoFlow 已经成功获得了多项国内外权威认证，这些认证覆盖了数据安全、隐私保护以及智能硬件等多个关键领域。

2.3.1 数据安全&隐私认证

EN 认证（EN 303 645）

EN 303 645 是针对消费者物联网设备的网络安全标准，旨在确保物联网设备的安全性，防止潜在的网络攻击。

TRUSTe 企业隐私认证

EcoFlow 已获得 TRUSTe 认证，这标志着我们在隐私政策和数据保护方面达到了更高的标准。TRUSTe 认证表明我们严格遵循隐私相关控制措施，确保在数据管理和隐私

保护方面的合规性和透明度。我们致力于为用户提供更加安全和可信赖的使用体验。

NISTIR 8259

NISTIR 8259 提供物联网设备的网络安全指南，帮助制造商确保设备具备基本的网络安全功能，确保数据隐私。

NISTIR 8425

NISTIR 8425 是对 NISTIR 8259 的补充，进一步提供操作指南，确保物联网设备在运行中保护数据隐私和安全。

SB 327

SB 327 是加利福尼亚州的物联网设备安全法律，要求设备具备合理的安全功能以保护用户隐私。

2.3.2 智能硬件方案认证

PSTI

PSTI 认证源自英国的物联网设备安全法律，旨在确保消费者的物联网设备不会遭受网络攻击，防止数据泄露和隐私侵犯。该法律反映了对物联网设备的安全需求日益增加，强制要求制造商采取合理的安全措施以保护设备和用户数据。

FCC SDOC

FCC SDOC 是一种自我声明的认证，确保产品符合美国联邦通信委员会的电磁兼容性标准，主要适用于通信设备。

MIC（TELEC)

MIC（TELEC） 是日本针对无线电设备的认证，确保设备符合无线频谱的使用规定，防止非法干扰。

SRRC

SRRC 是中国无线电设备的认证，确保设备在中国市场使用时符合法规，避免频率干扰，间接确保通信安全。

ISO 13849

ISO 13849 是机械设备的功能安全标准，主要针对工业设备的控制系统，确保安全功能的正常运作。

2.3.3 体系认证

ISO 9001：2015 - 质量管理体系认证

ISO 9001 是一项国际标准，规定了建立和维持有效质量管理体系（QMS）所需的要求。此标准适用于任何希望改进其产品或服务质量及用户满意度的组织。获得 ISO 9001 认证的企业在以下方面具有良好的管理能力：

- 持续满足用户和法律法规的要求。
- 持续提升用户满意度。
- 有效实施过程控制和风险管理。

2.4 数据安全及隐私保护

2.4.1 数据归属声明

- **数据所有者**：个人用户是个人数据的所有者，数据为个人用户所有。
- **数据控制者**：在 EcoFlow 为用户提供的产品或服务中， EcoFlow 决定个人数据收集目的、收集范围、处理的方式。
- **数据处理者**：EcoFlow 的服务提供商根据 EcoFlow 数据处理的指示，为 EcoFlow 提供处理个人数据的服务，保证并完善双方约定的服务并持续性地提供给个人用户。

2.4.2 个人隐私权利保障

EcoFlow 尊重并保护用户的个人隐私权利，并提供相应保障措施。

2.4.2.1 访问权

用户有权获得我们持有的有关用户的个人数据的副本以及与我们处理用户的个人数据有关的某些信息。

2.4.2.2 更正权

如果用户的个人数据不准确或不完整，用户有权要求更正。用户可以随时登录用户的帐户并直接更新用户的详细信息，或发送电子邮件联系我们来更新用户的个人数据。

2.4.2.3 删除权

用户可以要求 EcoFlow 删除用户的个人数据。但请注意，由于特定法律原因，我们可能无法始终遵从用户的删除请求，如适用，我们将在用户提出请求时通知用户。

2.4.2.4 限制处理

用户可以在某些情况下要求限制对用户的个人数据的处理。在限制处理的情况下，我们可以保留有关用户的足够信息，以确保将来遵守该限制。

2.4.2.5 数据可携带权

用户可以请求获取用户的个人数据的副本，或请求将用户的个人数据转移给其他公司。但请注意，此权利仅适用于用户最初同意我们使用的自动化数据或我们使用这些数据与用户签订合同的情况。

2.4.2.6 反对处理权

用户可以选择不让我们为定向广告目的处理用户的个人数据。

2.4.2.7 撤销同意权

用户可以撤回之前对用户个人数据的使用同意。如果用户撤回同意，我们可能无法为用户提供某些特定服务的访问权限。请注意，在用户撤回同意之前对用户的个人数据的任何使用或披露均不受此类撤回的影响。

2.4.2.8 反对自动化决策权

当我们在处理用户的个人数据时进行自动决策或分析时，用户可以要求人工干预。如果我们与用户签订的合同有此必要，并且法律要求采取适当的保护措施或征得用户的同意，则允许进行这种处理形式。用户可以通过我们的对外电子邮件地址通知我们，

选择退出此类自动决策和分析。

我们将尽力在一个月内或法律另有要求的情况下回复所有合法、经过验证的请求。偶尔，如果用户的请求特别复杂或用户提出了多项请求，我们可能需要一个月以上的时间。在这种情况下，我们会通知用户并及时向用户通报最新情况。我们可能需要向用户索取特定信息，以帮助我们根据适用法律确认用户的身份。这是一项安全措施，旨在防止个人数据被泄露给未经授权的人。

2.4.2.9 投诉权

如果用户对我们处理数据的方式有任何疑虑或投诉，可以通过邮件联系我们。用户还有权向数据保护主管机构提出投诉。如果可能，请先与我们联系，以便我们以最有效的方式为用户提供帮助。

2.4.3 数据生命周期安全管理

为确保数据在整个生命周期内的安全性，我们实施了系统化的数据生命周期管理措施。从数据采集、使用、存储、传输、更改到销毁的每个阶段，我们都采取了严格的安全控制。数据在采集时即进行加密和分类，确保只有授权人员可以访问。存储阶段，我们使用先进的加密技术保护数据，定期进行安全审计以防止未经授权的访问。数据使用期间，通过访问控制和监控措施保障数据的安全性。数据的最终销毁阶段，我们采用安全科学的销毁方法，确保数据不可恢复，防止任何潜在的数据泄露风险。通过这些措施，我们保障了数据在其整个生命周期中的机密性和完整性。

2.4.4 数据安全治理

我们通过建立全面的数据安全治理框架来确保数据的保护和合规性。我们设立有专门的数据安全团队，负责制定和实施数据安全政策、执行严格的访问控制和加密措施，并进行持续的监控与审计。我们遵循 GDPR、CCPA 等法规要求，定期审查和更新数据安全策略，以适应不断变化的威胁和技术环境。通过这些措施，我们致力于维护数据的完整性和机密性，并保障业务的持续合规性。

2.4.5 隐私合规

EcoFlow 保护用户与我们共享的个人信息，严格遵守合法、正当、必要原则，并采取以下合规措施：

1. 通过隐私政策明确、清晰、全面地告知用户个人信息的收集和使用情况。公司在官方网站、手机应用程序界面设置《隐私政策》，向用户清晰、完整地说明了收集和使用个人信息的情况，包括但不限于收集使用的个人信息类型、使用的场景和目的、设备权限调取情况、Cookie 和同类技术、第三方 SDK、个人信息的共享、转让、公开、存储、用户的个人信息主体权利、未成年人保护、投诉与联系渠道等。

2. 在产品功能的设置上，用户只有在使用某些功能或服务时，才需要向我们提供相应的数据，在此之前我们会征求用户的同意，获取相应的手机设备权限，用户可以随时选择撤回、关闭授权。

3. 我们根据数据的敏感程度和影响范围，对数据库采取严格的分类管理和安全访问权限管理，只有具有相应权限的管理员才能管理和查看对应的用户数据。并且，我们十分重视对产品和服务的数据安全影响评估，推进数据安全管理流程的不断更新和进步。

4. 在技术安全工具的采用上，我们采用各种密码加密策略，来保障数据在收集、使用、存储、传输、删除等全数据生命周期的安全性。

5. 在 APP 的下载和使用上，用户有权自主决定是否下载和使用 APP，并且将其个人信息分享给我们。我们提供 APP 的目的，是为了给用户带来更好的产品体验，包括设备的状态检测、功能设置、远程控制和 OTA 升级。

6. 对第三方数据授权和分享，制定由严格的管控措施，包括但不限于向用户事先说明和征得同意，对第三方的数据安全管理能力进行评估，与第三方通过合同、个人信息安全保障条款等约定和约束各方的个人信息安全保障责任等。

2.4.6 隐私保护影响评估

EcoFlow 建立了个人信息保护影响评估（DPIA） 个人信息保护影响评估（简称为“DPIA”），以确保隐私合规嵌入到产品设计中；针对重大、新兴的技术开发、产品设计或运营活动策划引入个人信息处理风险评估流程，识别处理活动对自然人的权益和自由可能产生的风险，并采取相 应风险管理措施。

实施 DPIA 有助于有效管理隐私合规风险，企业应当在事前进行 DPIA:

- 处理敏感个人信息；
- 利用个人信息进行自动化决策；
- 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
- 向境外提供个人信息；
- 其他对个人权益有重大影响的个人信息处理活动。

根据 GDPR，当数据处理活动“可能对自然人的权益和自由造成高风险”时，实施 DPIA 也是强制性要求。

2.4.7 供应商安全&隐私合规审核

EcoFlow 高度重视供应商的安全与隐私管理，内部制定了完善的供应商安全管理规范。在提供服务的过程中，EcoFlow 仅授权可信赖的第三方数据处理机构参与必要的数据处理活动。我们严格按照规范，对供应商数据生命周期的各个环节进行审查。对于引入的供应商，我们都会进行风险评估，以确保其具备足够的安全与隐私保护能力，并根据评估结果，可能要求签署 NDA、DPA、SCC 等协议，确保数据的安全性与合规性。

2.5 云安全

2.5.1 云基础设施安全

EcoFlow 依托业界领先的云服务提供商，包括 AWS、Azure、腾讯云和阿里云，构建了一套全面的安全体系。我们的关键安全措施包括：

- **身份与访问管理**：通过细粒度的权限控制和多因素认证（MFA），保障账户的安全性。
- **数据保护**：利用先进的数据加密服务，确保数据的机密性和完整性。
- **安全监控与响应**：实时监控系统状态，快速响应和处理安全事件。
- **多区域部署**：在全球范围内部署多个数据中心，提高系统的可用性和冗余性。
- **跨平台集成**：确保不同云平台之间的安全集成，保障跨平台的数据流动和服务访

问的安全性。

- **高可用性与灾难恢复**：实施高可用性解决方案和灾难恢复策略，确保业务的持续稳定运营。

2.6 终端安全

2.6.1APP 用户端安全

为确保 APP 的安全性，EcoFlow 采用了先进的代码加固和加密技术来保护应用程序及其数据，确保通信使用 TLS/SSL 加密，并实施严格的输入验证以防止常见攻击。在合规审查中，我们严格遵循相关数据保护法规（如 GDPR、CCPA）和行业标准，进行详细的安全审计和漏洞扫描。上线流程包括全面的安全测试和审查，确保所有功能符合安全要求后，才会正式发布应用程序，以保障用户的安全和隐私。

2.6.2 物联网（IoT）设备安全

为确保物联网设备的安全，EcoFlow 实施了全面的安全措施，包括使用证书管理来验证设备身份、应用 TLS 协议加密设备与服务器之间的通信，以及通过 OTA（Over-the-Air）机制安全地进行固件和软件更新。这些措施确保了数据的机密性、完整性和设备的持续安全性，有效防止未授权访问和网络攻击。

2.6.3 安全措施的持续改进

EcoFlow 认识到网络安全环境的不断演变要求我们必须持续更新和改进我们的安全措施。我们致力于通过以下几个方面来维护和加强终端安全：

- **持续监控**：我们对安全态势进行持续监控，以便快速识别和响应新的安全威胁和漏洞。
- **用户教育**：我们提供定期的安全教育和最佳实践指南，以提高用户对安全问题的认识和自我保护能力。
- **技术迭代**：我们不断研究和部署最新的安全技术，以确保我们的安全措施能够抵御日益复杂的网络攻击。

2.7 安全开发

EcoFlow 遵循安全开发的最佳实践，将安全集成到产品开发的整个生命周期中。从需求分析、设计、编码、测试到发布，每个阶段都有严格的安全标准和流程。

2.7.1 安全需求分析

在需求分析阶段，我们识别潜在的安全风险和需求，并将其纳入项目的整体规划中。通过安全评审的方式与业务团队进行深入沟通，针对特定业务逻辑、流程和技术框架讨论，以确保双方对安全需求有清晰且一致的理解。

2.7.2 产品安全设计

在产品设计阶段，我们充分考虑安全，遵从"纵深防御原则"、"减少攻击面"、"最小特权原则"、"职责分离原则"、"默认安全原则"、"故障保护原则"、"保护最薄弱环节原则"、"心理可接受原则"、"隐私保护原则"9 大安全设计原则，以减小潜在攻击面的大小。

2.7.3 开发阶段安全管控

在开发阶段，我们会通过严格的代码审查、静态分析和开源组件准入措施，确保在开发阶段对安全性的全面把控。

代码审查： 审查过程中重点检查代码中的安全问题，如输入验证、错误处理和权限控制，包括对安全编码标准的遵守情况进行评估。

静态分析： 使用静态代码分析工具自动检测代码中的安全缺陷，确保在发布前发现并修复潜在问题。

开源组件准入： 对所有开源组件进行安全评估，包括检查其来源、版本和已知的安全问题。仅经过验证和维护的组件可被引入和使用。

2.7.4 安全测试和漏洞闭环

为确保我们的产品服务具备最高的安全性，我们实施了全面的安全测试策略，并建立了一个有效的漏洞闭环管理机制。这些措施帮助我们在发现安全漏洞时迅速响应，并确保漏洞得到及时修复。

2.7.4.1 安全测试

- **动态测试：** 通过动态应用程序安全测试（DAST）工具在运行时检测应用程序的安全漏洞，模拟攻击以评估系统的安全性。
- **渗透测试：** 定期进行渗透测试，由专业的安全团队模拟攻击，评估系统的安全防护能力并提供改进建议。

2.7.4.2 漏洞闭环管理

- **漏洞发现：** 安全测试和代码审查过程中发现的漏洞会被记录和分类，确保每个漏洞都得到有效跟踪。
- **漏洞修复：** 发现的漏洞会分配给相关的开发人员或安全团队进行修复。修复过程包括对漏洞进行分析、制定修复计划、实施修复和进行验证测试。
- **修复验证：** 修复完成后，进行重新测试以确保漏洞已被成功修复，并且修复措施没有引入新的问题。
- **更新和文档：** 修复完成后，更新相关的安全文档和漏洞记录，确保所有相关信息都得到妥善维护。将漏洞修复情况和改进措施纳入定期的安全审计报告中。
- **反馈机制：** 建立反馈机制，将发现的漏洞和修复经验分享给团队，以改进开发和测试流程，增强未来的安全防护能力。

2.8 业务持续性

确保业务在面临安全事件或突发情况时能够持续运作是我们安全战略的关键组成部分。我们通过以下措施保障业务的连续性和恢复能力：

- **风险评估与业务影响分析：** 定期进行风险评估和业务影响分析（BIA），识别可能影响业务运作的威胁和风险，并评估这些风险对业务功能的影响，确定关键业务功能的优先级。
- **业务连续性计划：** 制定详细的业务连续性计划，包括恢复目标（RTO 和 RPO）、备用方案、关键资源和人员安排。确保在主要系统或设施不可用时，能够通过备用方

案维持业务运作。

- **数据备份与恢复：** 实施定期的数据备份策略，将备份数据存储在异地或云环境中。定期测试备份的恢复过程，确保在数据丢失或系统故障时能够快速恢复业务。
- **应急响应与沟通：** 建立应急响应计划和沟通策略，确保在安全事件发生时，能够迅速响应并向员工、用户和其他相关方提供及时的信息，减少混乱和影响。
- **演练与培训：** 定期进行业务连续性和灾难恢复演练，模拟不同场景以检验计划的有效性。对员工进行业务连续性和应急响应培训，确保他们了解各自的角色和职责。
- **计划更新与改进：** 定期审查和更新业务连续性计划，根据新的威胁情境、技术变更和演练结果不断改进，以保持计划的有效性和适应性。

结束语

在本白皮书中，我们详细介绍了在数据安全、隐私保护、灾难恢复和业务连续性方面的战略和措施。通过实施严格的安全控制、定期的风险评估以及持续的改进和培训，我们致力于保护用户的数据和业务安全。

我们的目标是为用户提供一个安全、可靠的服务环境，并在面对各种挑战时能够迅速响应和恢复。我们深知，安全不仅仅是技术问题，更是对用户信任的承诺。我们将继续投资于最前沿的技术和最佳实践，以确保我们的系统和流程能够应对未来的安全威胁和业务挑战。如果有任何问题或需要进一步的信息，请随时与我们联系。