《信息安全管理手册》

Information Security Management Manual

厦门海辰储能科技股份有限公司

Xiamen Hithium Energy Storage Technology Co., Ltd.

厦门市火炬高新区同翔高新城海辰产业园
HiTHIUM Industrial Park, Tongxiang High-Tech Zone
Xiamen, Fujian, China
www.hithium.com
0592-5513735
hithium@hithium.com

1. 目的 Purpose

为建立、实施、运行、监视、评审、保持和改进文件化的信息安全管理体系（简称 ISMS），确定信息安全方针和目标，对信息安全风险进行有效管理，确保全体员工理解并遵照执行信息安全管理体系文件、持续改进信息安全管理体系的有效性，特制定本手册。

This manual is formulated to establish, implement, operate, monitor, review, maintain, and improve a documented information security management system (ISMS), determine information security policies and objectives, effectively manage information security risks, ensure that all employees understand and comply with the implementation of information security management system documents, and continuously improve the effectiveness of the information security management system.

2. 范围 Scope of application

本管理策略适用于厦门海辰储能科技股份有限公司及其分子公司的信息安全管理各项工作。

This management strategy is applicable to the information security management work of Xiamen Hithium Energy Storage Technology Co., Ltd. and its subsidiaries.

3. 术语定义 Definition of Terms

3.1 ISMS（Information Security Management System）：信息安全管理体系。

3.2 PDCA（Plan-Do-Check-Act）：又称戴明环，即 Plan（计划）、Do（执行）、Check（检查）和 Act（处理）。

4. 职责 Responsibilities

4.1 信息中心负责组织制定信息安全管理手册、定期评审和更新工作；

IT&IS is responsible for organizing regular reviews and updates of the information security management manual;

4.2 信息安全管理者代表负责信息安全管理手册的审核和批准。

Information Security Manager Representative is responsible for reviewing and approving the information security management manual.

5. 文件内容 Document Content

信息安全策略管理 Information Security Policy Management

根据公司业务特点和信息安全需求，建立本《信息安全管理手册》，信息安全策略应经过相关管理层批准后发布执行，如果发生变更，也要进行相应管理层批准后再次发布执行。

Based on the company's business characteristics and information security needs, establish an "Information Security Management Manual." The information security strategy should be approved by the relevant management before being released and implemented. If there are changes, they should also be approved by the corresponding management before being released and implemented again.

对公司内相关员工进行与其工作相关的信息安全策略的培训和宣贯，如果外部相关方需要使用相关的信息安全策略，经相关管理层批准后，提供给外部相关方。

Provide training and promotion on information security strategies related to their work to relevant employees within the company. If external stakeholders need to use relevant information security strategies, they will be provided to external stakeholders after approval by relevant management.

为了保证信息安全各方面策略的有效性和适用性，公司每年组织各策略的相关部门开展策略的评审，并根据评审结果进行优化和改进。

In order to ensure the effectiveness and applicability of information security strategies in all aspects, the company organizes annual reviews of strategies by relevant departments, and optimizes and improves them based on the review results.

5.1 组织环境 Context of the organization

5.1.1 理解组织及其环境 Understanding the organization and its context

在建立信息安全管理体系时，应充分考虑内部组织架构和战略目标要求，分析公司信息安全管理和影响信息安全绩效相关的内外部事项，结合已经采用了 ISO/IEC 27001 等标准要求，建立的信息安全管理体系，并与公司的企业文化和战略目标相一致。包括，但不仅限于：

When establishing an information security management system, it is necessary to fully

consider the internal organizational structure and strategic objectives, analyze the company's information security management and internal and external matters that affect information security performance, and establish an information security management system that is consistent with the company's corporate culture and strategic objectives, taking into account the requirements of standards such as ISO/IEC 27001 that have been adopted. Including, but not limited to:

（1）组织结构、职责划分；

（2）业务发展战略目标和方针；

（3）可以使用的资源、知识和能力（如：资金、时间、人员、过程、系统和技术）；

（4）内部利益相关方对信息安全管理的观点和看法；

（5）企业文化；

（6）信息沟通和交流的策略和过程；

（7）目前已经采用的其他的管理标准要求。

(1) Organizational structure and division of responsibilities;

(2) Business development strategic goals and policies;

(3) Available resources, knowledge, and capabilities (such as funds, time, personnel, processes, systems, and technology);

(4) The views and perspectives of internal stakeholders on information security management;

(5) Corporate culture;

(6) Strategies and processes for information communication and exchange;

(7) Other management standard requirements that have already been adopted.

5.1.2 理解相关方的需求和期望 Understanding the needs and expectations of interested parties

在建立信息安全管理体系时，除了了解内部的相关因素外，还应关注和识别相关方对信息安全管理的需求和期望。公司信息安全相关方包括政府机构、监管单位、外部认证单位、客户、供应商、管理层、内部部门及员工等。

When establishing an information security management system, in addition to understanding internal factors, attention should also be paid to and identification of the needs and expectations of relevant parties for information security management. The company's information security stakeholders include government agencies, regulatory agencies, external certification units, customers, suppliers, management, internal departments, and employees.

5.1.3 确定信息安全管理体系范围 Determining the scope of the information security management system

根据业务特征、组织结构、地理位置、资产和技术定义了范围和边界，信息安全管理体系的范围包括：

The scope and boundaries of the information security management system are defined based on business characteristics, organizational structure, geographical location, assets, and technology. The scope includes:

（1）组织范围：厦门海辰储能科技股份有限公司；

（2）业务范围：锂离子可充放电电芯、电池模组、电池簇和电化学储能系统的设计和制造；

（3）物理范围：中国福建省厦门火炬高新区同翔高新城本源路 1 号

(1) Organizational scope: Xiamen Hithium Energy Storage Technology Co., Ltd;

(2) Business scope: Design and manufacturing of lithium-ion rechargeable discharge cells, battery modules, battery clusters, and electrochemical energy storage systems;

(3) The physical scope is located on the No.1 Benyuan Road, Tongxiang High-Tech Town, Xiamen Torch High-Tech Industrial Development Zone, Fujian Province, China.

5.1.4 信息安全管理体系 Information security management system

公司按 ISO/IEC 27001:2022《信息安全-网络安全和隐私保护-信息安全管理体系-要求》规定，参照 ISO/IEC 27002:2022《信息安全-网络安全和隐私保护-信息安全控制集》标准，建立、实施、运行、监视、评审、保持和改进文件化的信息安全管理体系。

According to ISO/IEC 27001:2022 "Information Security - Network Security and

Privacy Protection - Information Security Management Systems - Requirements" and referring to ISO/IEC 27002:2022 "Information Security - Network Security and Privacy Protection - Information Security Control Set" standard, establish, implement, operate, monitor review, maintain, and improve a documented information security management system.

5.2 领导 Leadership

5.2.1 领导和承诺 Leadership and commitment

最高管理者通过以下活动，对建立、实施、运行、监视、评审、保持和改进信息安全管理体系的承诺提供证据：

The top management provides evidence of their commitment to establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security management systems through the following activities:

（1）建立信息安全方针；

（2）确保信息安全目标和计划得以制定和实施；

（3）向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性；

（4）提供充分的资源，以建立、实施、运行、监视、评审、保持并改进信息安全管理体系；

（5）决定接受风险的准则和风险的可接受等级；

（6）确保内部信息安全管理体系审核得以实施；

（7）实施信息安全管理体系管理评审。

(1) Establish information security policies;

(2) Ensure the development and implementation of information security goals and plans;

(3) Communicate to the organization the importance of meeting information security goals, complying with information security policies, and fulfilling legal responsibilities, and continuously improving;

(4) Provide sufficient resources to establish, implement, operate, monitor, review, maintain, and improve information security management systems;

(5) Determine the criteria for accepting risks and the acceptable level of risks;

(6) Ensure the implementation of internal information security management system audits;

(7) Implement information security management system management review.

5.2.2 信息安全方针 Information Security Policy

根据组织的业务特征、组织结构、地理位置、资产和技术定义了 ISMS 方针，该信息安全方针符合以下要求：

The ISMS policy is defined based on the business characteristics, organizational structure, geographical location, assets, and technology of the organization, and meets the following requirements for information security:

（1）为信息安全目标建立了框架，并为信息安全活动建立整体的方向和原则；

（2）符合业务及法律或法规的要求，涵盖合同的安全义务；

（3）与组织战略和风险管理相一致的环境下，建立和保持 ISMS；

（4）经最高管理者批准。

(1) establishing a framework for information security objectives and establishing overall direction and principles for information security activities;

(2) Comply with business and legal or regulatory requirements, covering contractual security obligations;

(3) Establish and maintain an ISMS in an environment consistent with organizational strategy and risk management;

(4) Approved by the top management.

5.2.3 信息安全组织架构和职责 Information Security Organizational roles, responsibilities and authorities

通过建立自上而下的信息安全组织策略，搭建信息安全管理疏通桥梁，建立合理的信息安全管理组织结构与职能，以保障、协调、监控安全目标的实现。

By establishing a top-down information security organizational strategy, building a bridge for information security management, and establishing a reasonable information security management organizational structure and functions, to ensure, coordinate, and

monitor the achievement of security goals.

信息安全组织实行“高层牵头、统一组织、分工协作、全员参与”的组织原则。

The information security organization implements the organizational principle of "high-level leadership, unified organization, division of labor and cooperation, and full participation."

（1）信息安全组织架构设置信息安全领导组、信息安全工作组。

（2）信息安全领导组由总经理，副总经理。公司总经理作为公司信息安全工作第一负责人，做出信息安全承诺，对信息安全进行方向性指导，对信息安全建设等重大问题做出决策。

（3）信息安全工作的日常管理职能设在 IT&IS。

（4）IT&IS 设置信息安全主管岗，负责全面组织协调公司的信息安全管理工作。

（5）各部门配置一名信息安全协调员。

(1) The information security organizational structure includes an information security leadership group and an information security working group.

(2) The Information Security Leadership Group consists of a General Manager and a Deputy General Manager. The General Manager of the company, as the first person in charge of information security work, makes information security commitments, provides directional guidance for information security, and makes decisions on major issues such as information security construction.

(3) The daily management function of information security work is located in IT&IS.

(4) IT&IS has set up an information security supervisor position, responsible for comprehensively organizing and coordinating the company's information security management work.

(5) Each department is equipped with an information security coordinator.

保持与公安网监部门、消防部门等政府监管机构、外部安全专家（包括相关权威人士）或专业化组织的联系，以便随时获取信息，跟踪行业趋势，响应安全事件，必要时调整公司信息安全策略。

Maintain contact with government regulatory agencies such as public security network

supervision departments and fire departments, external security experts (including relevant authorities), or specialized organizations to obtain information at any time track industry trends, respond to security incidents, and adjust the company's information security strategy if necessary.

识别外部组织对公司信息资产的访问风险，并进行有效管理，主要包括。

Identify the access risks of external organizations to company information assets and effectively manage them, mainly including.

（1）与外部组织签订协议，并向其声明公司的信息安全策略要求；

（2）在外部组织访问过程中采取有效的控制措施和手段。

(1) Sign agreements with external organizations and declare the company's information security policy requirements to them;

(2) Take effective control measures and means during external organization visits.

5.3 规划 Planning

5.3.1 应对风险和机会的措施 Actions to address risks and opportunities

公司应对识别的信息安全方面面临的风险和机遇，相关方对信息安全的需求进行处置，制定处置措施，并按照措施的性质分配相关部门实施。IT&IS 应跟踪相关处置的落实情况和实施效果，确保相关风险得到管控，相关方的信息安全需求得到满足。

The Company shall address the identified risks and opportunities in information security as well as the information security needs of relevant parties, develop treatment measures, and assign relevant departments to implement them according to the nature of the measures. IT&IS should track the implementation and effectiveness of relevant disposal measures to ensure that relevant risks are controlled and the information security needs of relevant parties are met.

5.3.2 信息安全风险评估 Information security risk assessment

应建立适用于信息安全管理体系和已经识别的业务信息安全、法律和法规要求的风险评估方法，建立接受风险的准则并识别风险的可接受等级。所选择的风险评估方法应确保风险评估能产生可比较和可重复的结果。

Risk assessment methods applicable to information security management systems and identified business information security, legal and regulatory requirements should be established, criteria for accepting risks should be established, and acceptable levels of risks should be identified. The selected risk assessment method should ensure that the risk assessment produces comparable and repeatable results.

5.3.3 信息安全风险处置 Information security risk treatment

应制定并应用信息安全风险处置过程：

Information security risk management processes should be developed and app lied:

（1）在考虑风险评估结果的基础上，选择适合的信息安全风险处置选项；

（2)选择风险处置措施时，充分借鉴 ISO/IEC27001:2022 附录 A 中的控制措施；

（3）编制 ISO/IEC 27001:2022 适用性声明，包含必要的控制及其选择的合理性说明；

（4)信息安全风险处置计划以及对信息安全残余风险应获得风险责任人的批准。

(1) On the basis of considering the risk assessment results, select suitable information security risk disposal options;

(2) When selecting risk disposal measures, fully reference the control measures in Appendix A of ISO/IEC 27001:2022;

(3) Prepare a declaration of applicability for ISO/IEC 27001:2022, including necessary control s and justification for their selection;

(4) The information security risk disposal plan and the approval of the risk owner for residual information security risks should be obtained.

5.3.4 信息安全目的及其实现规划 Information security objectives and planning to achieve them

应根据本公司的实际情况，结合标准要求，制定信息安全目标，信息安全目标应与公司的信息安全方针保持一致，尽量量化，并保证可比较性。

Information security objectives should be formulated based on the actual situation of the company and in combination with standard requirements. Information security objectives should be consistent with the company's information security policy,

quantified as much as possible, and comparable.

信息安全目标从信息的保密性、完整性和可用性三个方面设置：

Information security objectives are set from three aspects: confidentiality, integrity, and availability of information:

（1）保密性：公司绝密文件泄露次数，年度为 0 次。

（2）完整性：一级业务系统数据丢失≤30 分钟（RPO 为 30 分钟）。

（3）可用性：一级业务系统年度可用性≥99.7%；一级业务系统的 RTO 为 24 小时。

(1) Confidentiality: The number of times the company's top secret documents are leaked is 0 times per year.

(2) Integrity: Level1 business system data loss ≤ 30 minutes (RPO of 30 minutes).

(3) Availability: Annual availability of Level1 systems ≥ 99.7%; The RTO of the Level1 system is 24 hours.

信息安全目标应在内部各部门进行沟通和宣贯。

The information security objectives should be communicated and promoted within various internal departments.

应每年对信息安全目标的完成情况进行统计分析，并根据达标完成情况进行必要的更新。

Statistical analysis should be conducted annually on the completion of information security goals, and necessary updates should be made based on the achievement of standards.

各信息安全目标相关部门应针对目标制定实现策划，指定负责人、分析完成目标需要的资源和必须开展的工作、确定测量时间和评价的方式方法等。

Each department related to information security goals should develop implementation plans for the goals, designate responsible persons, analyze the resources and necessary work required to achieve the goals, determine measurement time, and evaluate methods and methods.

5.3.5 信息安全管理体系变更的策划 Planning for changes to the information

security management system

根据信息安全管理体系运行情况和内外部审核检查，发现需要进行体系优化和变更时，应进行全面策划，考虑各文件的相互依赖关系，进行关联分析和改进。变更的文件应重新进行审批和受控，并在相关部门和人员进行培训和宣贯。

Based on the operation of the information security management system and internal and external audits, when it is found that system optimization and changes are necessary, comprehensive planning should be carried out, considering the interdependence of various documents, and correlation analysis and improvement should be carried out. The changed documents should be reapproved and controlled and trained and promoted by relevant departments and personnel.

5.4 支持 Support

信息安全管理体系所要求的记录是体系符合标准要求和有效运行的证据。制定并维持易读、易识别、可方便检索又考虑法律、法规要求的记录管理办法，规定记录的标识、储存、保护、检索、保管、废弃等事项。

The records required by the information security management system are evidence of the system's compliance with standard requirements and effective operation. Develop and maintain records management methods that are easy to read, identifiable, and retrievable, while also considering legal and regulatory requirements, and regulate the identification, storage, protection, retrieval, custody, and disposal of records.

信息安全体系的记录包括信息安全管理体系运行所需的所有记录。

The records of the information security system include all records necessary for the operation of the information security management system.

5.5 运行 Operation

5.5.1 运行规划和控制 Operational planning and control

为了满足信息安全要求，公司应规划、实现和控制信息安全管理所需要的过程，实现为达到信息安全目的一系列计划。

In order to meet information security requirements, companies should plan, implement, and control the processes required for information security management, and

implement a series of plans to achieve information security objectives.

应保持信息安全管理体系运行的所有记录作为信息安全管理体系运行的证据。应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

All records of the operation of the information security management system should be maintained as evidence of its operation. Changes within the plan should be controlled and the consequences of unexpected changes should be reviewed, and necessary measures should be taken to mitigate any negative impacts.

应确保与信息安全相关的外包过程是确定的和受控的。

It should be ensured that outsourcing processes related to information security are determined and controlled.

5.5.2 信息安全风险评估 Information security risk assessment

应按照确定的信息安全风险评估方法，每年组织各部门开展信息资产识别和信息安全风险评估工作，形成风险评估报告，并报领导批准。

According to the determined information security risk assessment method, each department should be organized to carry out information asset identification and information security risk assessment work every year, form a risk assessment report, and submit it to the leader for approval.

应保留信息安全风险评估的相关记录文件。

Relevant record files for information security risk assessment should be retained.

5.5.3 信息安全风险处置 Information security risk treatment

应根据各部门评估的风险进行统计分析，将风险进行归类，制定风险处置策略和处置计划。应安排专人跟踪风险处置计划的执行，并对残余风险（如果有的话）形成报告，提交管理者代表批准。

Statistical analysis should be conducted based on the risks assessed by each department, and risks should be classified and risk disposal strategies and plans developed. A dedicated person should be arranged to track the implementation of the risk disposal plan and form a report on residual risks (if any), which should be submitted to the management representative for approval.

应保留信息安全风险处置的相关记录文件。

Records and documents related to the disposal of information security risks should be retained.

5.6 绩效评价 Performance evaluation

5.6.1 监视、测量、分析和评价 Monitoring, measurement, analysis and evaluation

为了确保信息安全管理体系有效运行，公司应策划对信息安全管理体系的有效性进行测量，包括对信息安全目标和信息安全管理策略的测量。

In order to ensure the effective operation of the information security management system, the company should plan to measure the effectiveness of the information security management system, including the measurement of information security objectives and information security management strategies.

开展信息安全有效性测量应制定测量计划，按照相关人员开展测量工作。负责测量工作的各部门相关人员收集与测量任务相关的数据，并进行统计分析。

To carry out effective measurement of information security, a measurement plan should be developed and measurement work should be carried out according to relevant personnel. The relevant personnel of each department responsible for measurement work collect data related to measurement tasks and conduct statistical analysis.

各部门将本部门统计好的数据提交给信息安全工作小组，由信息安全工作小组进行汇总。对于未达成信息安全目标的，按照相关标准进行考核。

Each department submits the data collected by their own department to the Information Security Working Group, which will summarize it. For those who fail to achieve information security goals, assessment will be conducted according to relevant standards.

5.6.2 内部审核 Internal audit

应每年(两次间隔时间不超过 12 个月)策划和组织信息安全管理体系内部审核，包括策划和实施审核以及报告结果和保持记录的职责和要求，以确定其信息安全管理体系的控制 目标、控制措施、过程和程序是否：

Internal audits of the information security management system should be planned and

organized annually (with an interval of no more than 12 months), including planning and implementing audits, reporting results, and maintaining records, to determine whether the control objectives, measures, processes, and procedures of the information security management system are:

（1）符合本标准的要求和相关法律法规的要求；

（2）符合已识别的信息安全要求；

（3）得到有效地实施和维护；

（4）按预期执行。

(1) Comply with the requirements of this standard and relevant laws and regulations;

(2) Meet the identified information security requirements;

(3) Effectively implemented and maintained;

(4) Execute as expected.

应考虑拟审核的过程和区域的状况和重要性以及以往审核的结果，对审核方案进行策划，确定审核的准则、范围、频次和方法。

Consideration should be given to the status and importance of the process and area to be audited, as well as the results of previous audits. The audit plan should be planned to determine the criteria, scope, frequency, and method of the audit.

每次审核前，应编制内审计划，确定审核的准则、范围、 日程和审核组。审核员的选择和审核的实施应确保审核过程的客观性和独立性。审核员不应审核自己的工作。

Before each audit, an internal audit plan should be prepared to determine the audit criteria, scope, schedule, and audit team. The selection of auditors and the implementation of audits should ensure the objectivity and independence of the audit process. Auditors should not audit their own work.

5.6.3 管理评审 Management review

每年（两次间隔时间不超过 12 个月）开展管理评审会议，从管理层角度评审信息安全管理体系，以确保其持续的适宜性、充分性和有效性。管理评审包括评价信息安全管理体系改进的机会和变更的需要，包括对信息安全方针和信息安

全目标的评审。管理评审的结果应清晰地形成文件，记录应加以保持。

Every year (with an interval of no more than 12 months), a management review meeting is held to review the information security management system from the perspective of management to ensure its continuous suitability, adequacy, and effectiveness. Management review includes evaluating opportunities for improvement and the need for changes in the information security management system, including a review of information security policies and objectives. The results of management reviews should be clearly documented, and records should be maintained.

5.7 改进 Improvement

5.7.1 持续改进 Continual improvement

每年对信息安全管理体系进行评审并根据评审意见进行改进，对信息安全方针、信息安全目标的有效性进行评价和分析，对审核发现的不符合和事件采取纠正措施，每年开展管理评审活动等，持续改进信息安全管理体系的适宜性、充分性和有效性。

Every year, the information security management system is reviewed and improved based on the review opinions. The effectiveness of information security policies and objectives is evaluated and analyzed, corrective measures are taken for non conformities and events found in the audit, and management review activities are carried out every year to continuously improve the suitability, adequacy, and effectiveness of the information security management system.

厦门海辰储能科技股份有限公司

Xiamen Hithium Energy Storage Technology Co., Ltd.

2025 年 8 月

August 2025