Securing Energy Storage for a Resilient Future:

POWIN'S CYBERSECURITY SOLUTIONS

POWIN

ORGANIZATIONAL AND OPERATIONAL CONVERGENCE

Our integrated approach aligns organizational policies with operational practices to deliver comprehensive cybersecurity and system resilience. By unifying governance with real-time controls, we achieve full visibility, faster threat response, and streamlined operations—safeguarding both business processes and critical infrastructure without compromising performance.

POWIN STRUCTURE

ORGANIZATIONAL

Govern

Cybersecurity programs, policies, and processes that encompass every aspect of Powin's business and products. Modeled after guidelines set forth by National Institute of Standards and Technology (NIST 800-53), Department of Energy (C2M2 Cybersecurity Maturity Model) and regulatory frameworks like NERC CIP Low and Medium Impact, AESCSF, NIS2.

Verify

3rd party validation of our claims, including certifications for SOC 2 Type 2 & ISO 27001.

OPERATIONAL

Identify

Understand what needs to be protected by assessing assets, data, risks, and third-party dependencies to prioritize security efforts.

Protect

Implement safeguards like encryption, access controls, and secure development practices to ensure data and systems remain secure.

Detect

Continuously monitor networks and systems for threats, anomalies, and potential security breaches to enable rapid response.

Respond

Take action when security incidents occur by containing threats, notifying stakeholders, and mitigating impacts.

Recover

Restore systems, data, and operations after an incident through backups, redundancy, and disaster recovery planning.

Protected from threats on-site and in the cloud

VIGILANT CYBERSECURITY

SECURE BY DESIGN

In-House Software Development: Our entire software stack is developed internally, providing full visibility and control over all system code, preventing potential vulnerabilities that could affect system operation and data security.

Multi-layered Network Protection: Segmented network architecture proactively limits intrusion spread, effectively quarantining threats and minimizing operational impact.

Complete Code Oversight: All operational code for our Battery Energy Storage Systems (BESS) is written internally, strictly adhering to our stringent security and quality standards throughout the Software Development Lifecycle (SDLC).

Continuous Source Code Review: Our code is regularly inspected throughout its lifecycle, swiftly identifying and resolving vulnerabilities.

Robust Data Encryption: Data protection meets stringent regulatory standards through encryption both in transit and at rest.

PROACTIVE RISK MITIGATION

Dedicated Cybersecurity Team: An expert internal cybersecurity team conducts ethical hacking and threat simulations to preemptively eliminate vulnerabilities.

Continuous Monitoring: Human and automated monitoring of Powin IT systems and customer BESS assets ensures round-the-clock vigilance against threats.

Customized Security Solutions: Powin has a successful history of delivering customized cybersecurity solutions to meet unique and evolving customer requirements.

Integrated Incident Response: Our robust response program combines automated threat detection, third-party expertise, and comprehensive documentation for recovery and continuity.

Secure Supply Chain: Our flexible supply chain strategy regularly inspects and verifies components to ensure ethical sourcing, integrity, and protection against tampering or vulnerabilities.

VERIFIED COMPLIANCE WITH HIGHEST STANDARDS

SOC 2 Type 2 Certification: Our SOC 2 Type 2 certified cybersecurity program is independently audited, validating our stated practices. ISO 27001 and ISO 9001 certifications are in progress, with completion expected in 2025.

Accelerated Regulatory Compliance: Our cybersecurity framework aligns with NERC CIP, AESCSF, and NIS2 to support security best practices and streamlines customer cybersecurity compliance goals.

Industry-Standard Frameworks: Network architecture adheres to ISA/IEC 62443 framework and the Purdue Reference Model.

Supply Chain Security: Meets rigorous NIST and ISO 27001 standards, reinforcing comprehensive cybersecurity at every level.

Case Study

SECURING CRITICAL INFRASTRUCTURE **IN UKRAINE**

In 2022, one of our customer stations was located in eastern Ukraine during the outbreak of a major conflict. As the situation escalated, Powin proactively prepared a special script that could wipe the hard drive of the station's Energy Management System (EMS) if needed, blocking all unauthorized access to BESS system controls and data.

While the station was still operational, and the risk of its location being captured by Russian forces increased, we reached out to the customer to offer to deploy the script, but we never received a response. Shortly after the offer, the station "went dark" — meaning it stopped communicating with the Powin Cloud around the same time the region changed control.

About a year later, in 2023, the station unexpectedly resumed sending telemetry data, even though it remained under uncertain conditions. To prevent any cybersecurity risks, we immediately took action and locked the station out of the Powin Cloud. Reconnection of the site requires security keys securely stored and managed by Powin.

This swift and decisive action ensured that sensitive information remained secure and that the station could not be misused, reinforcing the strength and reliability of our cybersecurity practices. While we await peace in the region, the site remains quarantined from the Powin ecosystem.

COMPLIANCE WITH INDUSTRY STANDARDS

Powin's commitment to robust cybersecurity is demonstrated by our adherence to the most respected industry standards and frameworks. By aligning with them, we further demonstrate that our systems are secure, resilient, and capable of mitigating both current and emerging threats.

NERC CIP

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards focus on securing critical infrastructure by enforcing strict controls over operational technology (OT). Powin complies with NERC CIP to protect the reliability of energy systems, ensuring robust access controls, real-time monitoring, and effective incident response protocols.

NIST-800

The National Institute of Standards and Technology (NIST-800) framework provides comprehensive guidelines for managing cybersecurity risks. It focuses on areas such as identity management, continuous monitoring, and incident response, helping Powin ensure its systems are resilient and adaptable to emerging threats.

NIS2

The EU's Directive on Security of Network and Information Systems (NIS2) enhances cybersecurity across essential and important sectors by mandating comprehensive risk management, incident reporting, and supply chain security measures. Powin aligns with NIS2 requirements to strengthen the resilience of critical infrastructure and ensure compliance with evolving European cybersecurity regulations.

SOC 2

Service Organization Control 2 (SOC 2) is a framework designed to secure customer data by evaluating the effectiveness of controls in five key areas: security, availability, processing integrity, confidentiality, and privacy. SOC 2 is essential for ensuring that Powin's systems safeguard sensitive information and meet industry expectations for data protection.

ISO27001

ISO/IEC 27001 is an internationally recognized standard for information security management. It sets the requirements for establishing, implementing, maintaining, and continuously improving an organization's information security management system (ISMS). Powin is currently in the process of achieving compliance with ISO27001.

AESCSF

The Australian Energy Sector Cyber Security Framework (AESCSF) provides a sector-specific model for assessing and improving cyber resilience within energy organizations. Aligned with global standards such as NIST, it supports maturity assessments, risk mitigation, and continuous improvement of cybersecurity posture. Powin adopts AESCSF-aligned practices to help our customers in the Australian energy market achieve compliance and protect their operational environments.

Compliance Matrix

KEY INDUSTRY STANDARDS AND POWIN'S APPROACH

Below is a summary of how these standards can overlap across key cybersecurity topics and how Powin emphasizes cybersecurity in all aspects of our products and larger organization.

CORE SECURITY REQUIREMENT	SUMMARY	POWIN
Electronic and Physical Access Control	Control and monitor access to digital systems and physical infrastructure to prevent unauthorized entry.	• Leverages Zero Trust Architecture through items like: Least Privilege Access and Strong Identity Management (Multi Factor Authentication (MFA), Identify and Access Management (IAM)) • 24/7 surveillance and facility access management (performed through Powin Remote Operations Center)
Network Security	Protect IT and OT systems by securing networks and controlling access to them.	• Segmented defense of depth architecture • Third party audits • Constant automated system scanning for vulnerabilities • Network design follows industry-standard ISA/IEC 62443 framework and Purdue Reference Model
Risk Management	Identify, assess, and mitigate cybersecurity risks across IT/OT environments.	• StackOS Gatekeeper provides customer safeguards, preventing any bad actor from controlling system through the internet • All Powin software and firmware is engineered, designed, and managed within the U.S. and allied countries • Regular penetration testing by internal and external CISSP/ eCPPT certified professionals • Perpetual scanning of all Powin-created software to identify emerging and existing exploits
Incident Response and Recovery	Detect, respond to, and recover from cybersecurity incidents to minimize or eliminate disruption.	• Incident response plans tailored to customer needs • Routine exercises simulating security and major infrastructure emergencies
Data Protection	Prevent unauthorized access to all IT/OT data.	• Industry-standard encryption of all data both in transit and at rest • GDPR, UKGDPR, APP, CCPA compliant data management program
Asset and Change Management	Tracks and manages hardware and software assets, ensuring they are updated and protected. Controls and documents changes to systems, ensuring they are tested and authorized to prevent disruptions.	• StackOS Patch Management organization works with customers to safely update systems to minimize disruption • All patches automatically verified for malware and exploits • Comprehensive inventory and firmware management program of networked devices (switches/routers etc.)

By viewing cybersecurity through the lens of proven frameworks, we prove our commitment to ensuring that systems meet customer requirements and demonstrate our willingness to go above and beyond. We continuously refine our processes through regular audits, vulnerability assessments, and the adoption of new technologies, making sure our cybersecurity posture remains strong in the face of emerging threats. This proactive approach allows us to deliver secure, reliable energy storage solutions to our customers, safeguarding both their operations and their data.

For additional information about our Enterprise Cybersecurity Program, as well as sales and partnership inquiries, please reach out at www.powin.com