

Cybersecurity Statement

Executive Summary

Energy Vault is a global leader in sustainable energy storage solutions, including proprietary gravity, battery, and green hydrogen energy storage hardware technologies, supported by a technology-agnostic energy management system software and integration platform. The company's mission is to accelerate the clean energy transition through innovative, cost-effective, and scalable storage technologies.

Digital Security Program

Energy Vault's Digital Security Program (DSP) is a comprehensive framework aligned with ISO 27001, SOX 404, and NIST SP 800-37. It governs all data, systems, and infrastructure across the enterprise and its partners.

Key elements include:

- Role-based access control, MFA, and least-privilege principles.
- Endpoint protection, encryption, and mobile device management.
- Network segmentation, firewalls
- Threat and vulnerability monitoring, management, and intrusion detection.
- Data integrity, durability, protection, and monitoring.
- Annual cybersecurity training and phishing simulations.
- Continuous improvement, annual standards, policy, and procedure reviews
- Third party evaluation, information security requirements and risk management
- Continuously monitored through internal and external third-party auditing

Incident Response and Disaster Recovery

Energy Vault's Incident Response Plan (IRP) and Disaster Recovery Plan (DRP) follow NIST SP 800-61 guidelines and ensure business continuity.

Incident Response Phases:

1. Preparation
2. Detection and Analysis

3. Containment, Eradication, and Recovery
4. Post-Incident Review
5. Lessons Learned Captured for Improvement

Roles and Responsibilities:

- CIO / CISO: Communicates material incidents.
- Director of IT & Assurance: Leads response and ensures compliance.
- InfoOps & Department Key Stakeholders: Executes containment and recovery.
- All employees: Report incidents and follow policies.

All incidents must be reported immediately to InfoOps with relevant details.

Employee Responsibilities

All Energy Vault personnel must:

- Complete annual cybersecurity training.
- Read, acknowledge, and comply with company policies and procedures
- Use strong, unique passwords and enable MFA.
- Avoid public Wi-Fi unless using VPN.
- Report suspicious emails, system behavior, and security events immediately.

Safety and Quality

Energy Vault integrates safety and quality into every project phase, including real-time monitoring, predictive analytics, and fire suppression systems.

Certifications include:

- ISO 9001 – Quality Management
- ISO 45001 – Occupational Health & Safety
- ISO 27001 – Information Security

Compliance and Governance

Energy Vault's compliance framework includes:

- ISO 14001 – Environmental Management

- ISO 37001 – Anti-Bribery Management
- SOX 404 – Internal Controls over Financial Reporting

Corporate Governance Policies:

- Code of Conduct
- Corporate Governance Guidelines
- Committee Charters (Audit, Nominating & Corporate Governance, Compensation)
- Anti-Bribery
- Global Labor and Human Rights
- Insider Trading
- Occupational Health & Safety
- Quality & Environmental Management
- Supplier Code of Conduct

Sustainability and ESG Commitments/Statements:

- Annual Corporate Sustainability Report
- AA1000 third-party assurance
- Task Force on Climate-related Financial Disclosures
- Biodiversity
- No-Deforestation
- Modern Slavery Management
- Procurement & Supply Chain ESG