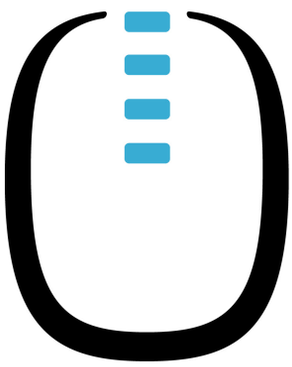

FENECON

FENECON Selbstauskunft Informationssicherheit

Inhaltsverzeichnis

1. Einleitung 2
2. Das Unternehmen 3
3. Unternehmens- und Organisationskontext 4
4. Informationssicherheit im Unternehmen 5
5. Informationssicherheit in den Produkten 7

1. Einleitung

Diese Selbstauskunft dient der Darstellung des aktuellen Stands der Informationssicherheit im Unternehmen.

Obwohl derzeit noch keine formalen Zertifizierungen nach ISO 27001:2024 und anderen Standards vorliegen, orientieren wir uns an den relevanten Normen und Best Practices. Die Umsetzung der Maßnahmen erfolgt schrittweise, mit dem Ziel einer kontinuierlichen Weiterentwicklung und möglicher zukünftiger Zertifizierung.

2. Das Unternehmen

FENECON ist ein führender Hard- und Softwarespezialist für Stromspeicherlösungen in den Segmenten Privathaushalt, Gewerbe und Industrie und der einzige deutsche Hersteller, der eine so umfangreiche Produktpalette an Batteriespeichersystemen in Deutschland fertigt und entwickelt.

Alle Speichermodelle zeichnet das selbst entwickelte Energiemanagementsystem FEMS aus, womit FENECON das weltweit erfolgreichste Open-Source-Energiemanagementsystem OpenEMS maßgeblich prägt. Die zahlreichen FEMS-Applikationen des Produktportfolios ermöglichen netz- und der Energiewende dienlichem Energiemanagement und intelligente Sektorenkopplung.

Als Experte für Stromspeicher und Energiemanagement zählt FENECON zu den stärksten Innovatoren in der Branche und setzt sich für eine Zukunft mit 100 Prozent erneuerbaren Energien ein. Die Leistungsfähigkeit, Flexibilität und Innovationskraft bestätigen auch zahlreiche Auszeichnungen:

- 3 x Innovator des Jahres (TOP 100-Wettbewerb für deutsche Mittelständler): 2023 bis 2025.
- 5 x The smarter E Award: 2020 bis 2025 für Stromspeichersysteme, Energiemanagement, herausragende Projekte und Geschäftsmodelle.
- Top Innovation Award (2025) und SolarProsumerAward von EUPD Research.
- Bayerischer Mittelstandspreis und BAYERNS BEST 50 (2024).

Als deutscher Hersteller, der seit 2011 im deutschen PV- und Energiemarkt etabliert ist, viel Erfahrung mit ausländischen Komponenten hat und Open-Source in vielen Aspekten lebt (beispielsweise mit dem hauseigenen Energiemanagement), liegen uns die Themen Informationssicherheit und Datenschutz sehr am Herzen. Wir begrüßen nationale, und besonders europäische Vorgaben, da sie einheitliche Regelungen zu diesen Themen schaffen.

3. Unternehmens- und Organisationskontext

Im Rahmen unserer Wachstums- und Professionalisierungsstrategie verfolgen wir aktiv die offizielle Zertifizierung unserer Prozesse und Maßnahmen.

- **ISO 9001:2015**

TÜV-zertifiziertes Qualitätsmanagement für alle FENECON-Standorte durch TÜV Süd.
(seit 07. Juli 2025)
Zertifikat als PDF-Download

- **ITQ Basisprüfung**

Initiierung eines Sicherheitsprozesses mit Auditierung und Prüfbericht durch externen IT-Dienstleister.
(seit 11.06.2025)

- **ISO 27001:2024**

Zertifizierung geplant und in Vorbereitung.

- **Beobachtung und Evaluierung zukünftiger relevanter Zertifizierungen im Rahmen Cyber Resilience Act (CRA), NIS2 und KRITIS - z. B.**

  ETSI EN 303 645 EU-Standard vernetzte Geräte

  RED 2014/53 EU-Standard für Cybersicherheit

  IEC 62443 Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme

- **Cloud-Services**

Hosting ausschließlich in Deutschland auf eigenen Servern und bei einem Hosting-Partner mit ISO-27001-Zertifizierung.

4. Informationssicherheit im Unternehmen

Die Informationssicherheit ist fester Bestandteil der Unternehmensstrategie von FENECON. Ziel ist es, Verfügbarkeit, Integrität und Vertraulichkeit von Informationen nachhaltig zu schützen und Risiken für Kunden, Partner und das Unternehmen zu minimieren.

- **Verantwortlichkeiten und Governance**

Die Gesamtverantwortung für Informationssicherheit liegt in der Geschäftsführung bei Stv. Geschäftsführer Stefan Feilmeier, Bachelor Wirtschaftsinformatik, Master Informatik (Embedded Systems).

Zur Umsetzung der Unternehmensstrategie im Bereich Informationssicherheit nutzen wir OKRs (Objectives and Key Results) und eine Delegationsmatrix. Der überwiegende Anteil der Aufgaben liegt zentral unternehmensübergreifend im Bereich „Shared Services“ in der Business Unit „Interne Dienste“.

Die Abteilungen des Bereichs (z. B. IT, Qualitätsmanagement, Strategie) setzen auf eigenes Personal und die Zusammenarbeit mit externen Experten um die langfristige Qualität und Weiterentwicklung sicherzustellen. Gesetzlich vorgeschriebene und Fachbeauftragte sind ernannt und durch interne Mitarbeiter oder Externe besetzt, z. B. Datenschutzbeauftragter, Qualitätsmanagementbeauftragter.

- **Basisprüfung ITQ**

Die Basisprüfung wurde Anfang 2025 durchgeführt und bildet den Grundstein für ein Informationssicherheitsmanagement (ISMS). Die Auditierung inkludierte die Bereiche Geschäftsführung, IT, Digitalisierung & ERP-System, FEMS (FENECON Energiemanagementsystem) und Marketing (z. B. Internetpräsenz).

Die Prüfung umfasst die Punkte IT-Sicherheitsmanagement, Virenschutz, Sicherheit von IT-Systemen, Vernetzung und Internet, VPN & WLAN, Inhaltssicherheit, Sicherheitserfordernisse, Patchmanagement, Passwörter und Verschlüsselung, Notfallvorsorge, Datensicherung, Infrastruktursicherung, Mobile Endgeräte, Lieferantenmanagement, Mobiles Arbeiten und Cloud.

Die im Audit identifizierten Aufgaben wurden an die betroffenen Abteilungen übergeben und werden in einer regelmäßigen IT-Security Taskforce überwacht.

- **Informationssicherheitsmanagement (ISMS)**

Eine Zertifizierung nach ISO 27001:2024 ist geplant und in Vorbereitung. Die konkreten Arbeiten daran wurden nach dem erfolgreichen Audit zur ISO 9001:2015 im Juni 2025 gestartet. Ein ISMS-Handbuch ist bereits im Aufbau, ein externes Beratungsunternehmen beauftragt und Workshops terminiert.

- **Awareness und Schulungen**

Über die interne E-Learning Plattformen „FENECON Academy“ und Sam Secova werden Mitarbeiterinnen und Mitarbeiter regelmäßig für Cybersecurity und Datenschutz sensibilisiert. Besondere Aufmerksamkeit gilt Software- und Hardwareentwicklern, Systemadministratoren und Service-Technikern mit erhöhten Berechtigungen.

- **Partnerschaften in Forschung & Entwicklung**

FENECON arbeitet seit jeher eng mit Universitäten, Forschungsinstituten und Marktbegleitern zusammen. Insbesondere die Zusammenarbeit in der OpenEMS Association e.V. und mit der aktiven Open-Source-Community rund um OpenEMS als Basis des FEMS ermöglicht unabhängige Kontrolle der Softwarequalität und Code-Sicherheit.
openems.io

5. Informationssicherheit in den Produkten

Informationssicherheit ist fester Bestandteil aller FENECON Hard- und Softwareprodukte und wird in der Gestaltung und Weiterentwicklung systematisch und einheitlich berücksichtigt.

Zentrales Element aller FENECON Stromspeichersysteme ist das FENECON Energiemanagementsystem (FEMS), das in allen Produkten eingesetzt wird. Es zeichnet sich im langjährigen Einsatz nachweislich durch seine hohe Stabilität und Skalierbarkeit aus.

Die FEMS-Plattform umfasst dabei sowohl das **lokale Energiemanagement** des Stromspeichersystems im Zusammenspiel mit weiterer Peripherie — wie z. B. Messeinrichtungen, analoge und digitale Ein- und Ausgänge, E-Auto-Ladestationen, etc. — als auch die durch FENECON betriebene **Cloud-Infrastruktur** — zur Fernüberwachung von Betriebszuständen in Echtzeit, zur Analyse historischer Daten, Fernwartung und die Bereitstellung von Software- und Firmwareupdates.

- **Betriebskonzept und Architektur der FEMS Plattform**

  Lokale Funktionalität

  FENECON Stromspeichersysteme und das FEMS Energiemanagementsystem arbeiten vollständig autark, auch ohne Cloud-Anbindung.

  Auch erweiterte Optimierungsfunktionen wie das KI-basierte Fahrplanmanagement funktionieren vollständig lokal.

  Visualisierung von Live-Daten, Analyse historischer Daten und lokale Anlagenfunktionen zu Wartungs- und Servicezwecken stehen über eine lokale Web-Applikation zur Verfügung.

  Cloud-Anbindung

  Das FEMS Energiemanagementsystem nutzt Cloud-Anbindungen zur Fernüberwachung, Datenanalyse, Wartung und Bereitstellung von Updates.

  FEMS verbindet sich über eine dauerhafte, TLS-verschlüsselte, bidirektionale Verbindung zur FENECON Cloud und gewährleistet darüber IT-sicheren und schnellen Datenaustausch.

  Komponenten des Stromspeichersystems (z. B. Batterie-Wechselrichter, Batterie-Managementsystem, Klimagerät, etc.) sind nicht direkt mit dem Internet verbunden. Sämtliche Kommunikation findet ausschließlich über FEMS statt.

  FEMS nutzt ausschließlich ausgehende (keine eingehenden) Verbindungen und erleichtert so die Verwaltung der betrieblichen Firewall. Ziel-Adressen und Ports sind klar dokumentiert: FEMS Technische Dokumentation.

  Die Web-Applikation nutzt moderne Technologien und ist optimiert für den Betrieb an PC und Smartphone. FENECON stellt native Apps für Android und iOS zur Verfügung.

  Konfigurierbare automatische Benachrichtigung im Falle eines Systemfehlers und bei

Ausfall der Internetverbindung.

- **Technische und organisatorische Maßnahmen**

  Softwareentwicklung der FEMS Plattform

  FEMS wird von einem eigenen in-house Team aus Softwareentwicklern und DevOps-Ingenieuren in Deutschland entwickelt und betrieben.

  Die „Software Bill of Materials" (SBOM) wird gepflegt; unnötige Abhängigkeiten werden vermieden.

  Weiterentwicklungen und Fehlerbehebungen sind lückenlos nachvollziehbar über das unternehmensweite Aufgabenmanagement, die Versionierung des Quellcodes und der Infrastruktur, eindeutige Markierung von Release-Versionen und verständliche Changelogs.

  Die Softwareentwicklung setzt auf eine moderne Entwicklungsinfrastruktur:

  Umfangreiches Continuous Integration (CI) System mit automatisierten Tests, automatisierter Überwachung der SBOM auf „known vulnerabilities and exposures" (CVE) und Weiterentwicklungen und statische Code-Analyse.

  Anwendung moderner Entwicklungsmethoden wie „Security by Design", „Test-Driven Development", strukturierter Code-Review-Prozess, Trunk Based Development.

  Betriebssicherheit

  Bereitstellung von kostenlosen Funktions-, sowie Sicherheits-Updates für alle Produkte über die gesamte Lebenszeit, auch nach Garantieende

  Durch FENECON betriebene Cloud-Infrastruktur ausschließlich in Deutschland auf eigenen Servern und bei einem Hosting-Partner mit ISO 27001-Zertifizierung.

  Zugriffskontrolle mit rollenbasiertem Rechtemanagement, personenbezogenen Zugangskonten („named users") und sicherer, nicht umkehrbarer Passwortverschlüsselung (PBKDF2-SHA512).

  Sämtliche Konfigurationsänderungen am Stromspeichersystem sind versioniert und mit Zeitstempel und durchführendem Zugangskonto nachvollziehbar (erfordert Cloud-Anbindung).

  Bevorzugter Einsatz von Komponenten aus deutscher oder europäischer Fertigung.

Obwohl noch keine formale Zertifizierung nach ISO 27001 vorliegt, entspricht die gelebte Praxis bereits in vielen Bereichen den Anforderungen dieser und weiterer Normen. Welche weiteren Normen wir zertifiziert haben möchten prüfen wir laufend. Wir als FENECON verpflichten uns zu einer kontinuierlichen Weiterentwicklung und Verbesserung der Informationssicherheit!