IT-Sicherheitskonzept für die SaaS-Plattform nPro

Stand: November 2025

---

1. Überblick

nPro Energy verpflichtet sich, die **Vertraulichkeit, Integrität und Verfügbarkeit** aller Kundendaten sicherzustellen. Sicherheit ist ein integraler Bestandteil unserer Softwareentwicklung, unserer Cloud-Infrastruktur und sämtlicher Betriebsprozesse. Dieses Dokument fasst relevante technische und organisatorische Maßnahmen, Audits und Sicherheitskonzepte zusammen. Weitere Informationen stellen wir auf Anfrage gerne zur Verfügung.

---

2. Infrastruktur & Hosting

Unsere Cloud-Plattform wird auf Servern eines externen Dienstleisters (*Akamai Technologies*) betrieben und folgt bewährten Prinzipien der **Softwaresicherheit**, **Verschlüsselung** und **Zugriffskontrolle**.

2.1 Serverstandort

Hosting erfolgt ausschließlich auf Servern in **Deutschland** (Frankfurt a. M.). Die gesamte technische Infrastruktur befindet sich innerhalb der EU. Der Serverbetrieb erfolgt derzeit durch Akamai Technologies, einen international zertifizierten Rechenzentrumsanbieter.

2.2 Rechenzentrum – Zertifizierungen & Compliance

Akamai Technologies erfüllt alle wesentlichen Sicherheits- und Compliance-Anforderungen für den Betrieb kritischer Cloud-Infrastrukturen. Dazu gehören unter anderem:

- **ISO/IEC 27001**, ISO/IEC 27017, ISO/IEC 27018
- **BSI-Zertifizierung** gemäß §8a BSIG für Betreiber Kritischer Infrastrukturen
- Regelmäßige externe Audits durch unabhängige Prüfer
- Alle Zertifizierungen sind unter folgendem Link abrufbar: https://www.akamai.com/legal/compliance

---

3. Sicherheit der Datenübertragung & Verschlüsselung

- Sämtliche Kommunikation erfolgt ausschließlich über **HTTPS**.
- Hierfür wird der Standard **TLS 1.3** verwendet.
- Sensible Informationen werden ausschließlich **verschlüsselt** gespeichert

---

4. Sicherheitstests und Audits

nPro Energy hat erfolgreich einen **Acunetix-Sicherheitsaudit** durchlaufen. Der Test bestätigte, dass keine kritischen oder hochgradigen Schwachstellen gefunden wurden. Geprüft wurden unter anderem:

- SQL-Injection und Datenbank-Exposition
- Cross-Site-Scripting (XSS)
- Authentifizierungs- und Sitzungsmanagement
- Unsichere Dateipfade oder -einbindungen
- SSL/TLS- und HTTP-Konfigurationen
- Veraltete Komponenten mit bekannten Sicherheitslücken

nPro Energy betrachtet diese Art von erfolgreichen Audits als Teil eines kontinuierlichen Sicherheitsprozesses, der durch manuelle Penetrationstests und Code-Reviews ergänzt wird.

Darüber hinaus führen wir durch:

- Automatisches Schwachstellen-Monitoring für alle Software-Abhängigkeiten (**CVE-Scanning**)
- Code-Reviews vor jedem Release

---

5. Zugriffskontrolle und Betrieb

Zugriff auf Produktionssysteme haben ausschließlich **autorisierte Teammitglieder**. Zugriffe sind durch starke Authentifizierung und rollenbasierte Berechtigungen geschützt. Alle administrativen Zugriffe werden **protokolliert** und regelmäßig **überprüft**. Kundendaten werden ohne ausdrückliche, schriftliche Zustimmung **unter keinen Umständen an Dritte weitergegeben**.

---

6. Betriebssicherheit und Notfallvorsorge

Primäre Backups werden durch den Rechenzentrumsbetreiber **redundant gespeichert**. Zusätzlich erstellt nPro Energy eigene **tägliche, verschlüsselte Datensicherungen**, die extern und langfristig archiviert werden. Diese mehrschichtige Strategie gewährleistet eine **hohe Ausfallsicherheit** und **schnelle Wiederherstellbarkeit** im Notfall.

---

7. Compliance- und Sicherheitsstrategie

nPro Energy arbeitet kontinuierlich an der Weiterentwicklung seiner Sicherheitsmaßnahmen. Geplante nächste Schritte:

- Jährliche **externe Penetrationstests**
- Erweiterung der Dokumentation zum **Incident-Response-Prozess**
- Vorbereitung auf eine **ISO 27001-Zertifizierung**

---

8. Zugriff, Login & Single Sign-On

Administrative Zugriffe auf die Server erfolgen über **SSH** mit kryptographischen Schlüsseln. Passwortbasierte Logins sind vollständig deaktiviert. Der Zugriff ist auf einen kleinen, autorisierten Nutzerkreis beschränkt.

Benutzerkonten der SaaS-Plattform sind passwortgeschützt. Passwörter werden ausschließlich als sichere **Hash-Werte** gespeichert (kein Klartext).

Auf Wunsch ist die Anmeldung über **SSO (Single Sign-On)** über bestehende Microsoft-Konten möglich. Damit können Unternehmen ihre bestehenden Azure AD / Microsoft Entra Policies (z. B. MFA, Conditional Access) nutzen.

---

9. Kontrolle über Eingabedaten

Unsere Plattform verarbeitet ausschließlich die Daten, die Nutzer **selbst eingeben oder hochladen**. Hierzu zählen in der Regel technische Kenngrößen wie:

- Energiebedarfe
- Lastprofile
- Leistungsdaten
- Parameter zur technischen Auslegung von Anlagen

Wichtige Sicherheitsprinzipien:

- Es werden keine externen Datenquellen automatisch importiert, die klassifizierte oder kritische Informationen enthalten könnten.
- Nutzer behalten volle Kontrolle über die Art der hochgeladenen Daten.
- In sicherheitssensiblen Kontexten können problemlos **approximierte oder synthetische Lastprofile** genutzt werden, die keine Rückschlüsse auf kritische Infrastruktur zulassen.
- Auf Wunsch kann jederzeit die **vollständige und irreversible Löschung** aller Projektdaten veranlasst werden.

---

10. Unternehmensstruktur & Unabhängigkeit

Die nPro Energy GmbH ist **wirtschaftlich vollständig unabhängig**. Es bestehen keine finanziellen oder organisatorischen Abhängigkeiten zu externen Unternehmen, Energieversorgern oder Institutionen. Die Entwicklung und der Betrieb der SaaS-Plattform erfolgen **eigenständig** und ohne Einflussnahme Dritter.

---

11. Referenzen

Unsere Software ist erfolgreich im produktiven Einsatz bei einer Vielzahl professioneller Anwender. Dazu gehören:

- Energieversorger und **Unternehmen der kritischen Infrastruktur** (explizite Referenzen auf Anfrage, da diese teilweise nicht öffentlich benannt werden dürfen).
- **60 Stadtwerke** in Deutschland, darunter u. a. die Stadtwerke München, Stadtwerke Leipzig, und die Berliner Stadtwerke.
- **Landesbehörden**, z. B. die Gebäudemanagement Schleswig-Holstein AöR (GMSH).
- **Kommunen**, die nPro für Energie- und Infrastrukturplanung einsetzen.
- Mehr als **250 Ingenieurbüros**, Beratungsunternehmen und private Planungsunternehmen.