IT Security Concept for the nPro SaaS Platform

Status: November 2025

---

1. Overview

nPro Energy is committed to ensuring the **confidentiality, integrity, and availability** of all customer data. Security is an integral part of our software development, our cloud infrastructure, and all operational processes. This document summarizes relevant technical and organizational measures, audits, and security concepts. We are happy to provide additional information upon request.

2. Infrastructure & Hosting

Our cloud platform is operated on servers of an external service provider (*Akamai Technologies*) and follows proven principles of **software security**, **encryption**, and **access control**.

2.1 Server Location

Hosting is carried out exclusively on servers located in **Germany** (Frankfurt am Main), **Europe**. The entire technical infrastructure is located within the European Union. The server operations are currently provided by Akamai Technologies, an internationally certified data center provider.

2.2 Data Center – Certifications & Compliance

Akamai Technologies meets all essential security and compliance requirements for operating critical cloud infrastructures. These include, among others:

- **ISO/IEC 27001,** ISO/IEC 27017, ISO/IEC 27018
- **German BSI certification** in accordance with §8a BSIG for operators of critical infrastructures
- Regular external audits by independent auditors
- All certifications can be accessed at the following link: https://www.akamai.com/legal/compliance

---

3. Data Transmission Security & Encryption

- All communication takes place exclusively via **HTTPS**.
- **TLS 1.3** is used for this purpose.
- Sensitive information is stored exclusively in **encrypted** form.

---

4. Security Tests and Audits

nPro Energy has successfully completed an **Acunetix security audit**. The test confirmed that no critical or high-severity vulnerabilities were found. The audit covered, among other things:

- SQL injection and database exposure
- Cross-site scripting (XSS)
- Authentication and session management
- Insecure file paths or file inclusions
- SSL/TLS and HTTP configurations
- Outdated components with known security vulnerabilities

nPro Energy regards these successful audits as part of an ongoing security process, which is complemented by **manual penetration tests** and code reviews.

In addition, we conduct:

- Automated vulnerability monitoring for all software dependencies (**CVE scanning**)
- Code reviews before every release

---

5. Access Control and Operations

Access to production systems is restricted to **authorized team members** only. All access is protected by strong authentication and role-based permissions. All administrative access is **logged** and **reviewed** regularly. Customer data **is not shared with third parties under any circumstances** without explicit written consent.

---

6. Operational Security and Emergency Preparedness

Primary backups are stored **redundantly** by the data center operator. In addition, nPro Energy creates its own **daily, encrypted data backups**, which are archived externally and for the long term. This multi-layered strategy ensures **high fault tolerance** and **rapid recoverability** in the event of an emergency.

---

7. Compliance and Security Strategy

nPro Energy is continuously working on further developing its security measures.
Planned next steps:

- Annual **external penetration tests**
- Expansion of the documentation for the **incident response process**
- Preparation for **ISO 27001 certification**

---

8. Access, Login & Single Sign-On

Administrative access to the servers is carried out via **SSH** using cryptographic keys. Password-based logins are completely disabled. Access is restricted to a small group of authorized users.

User accounts of the SaaS platform are protected by passwords. Passwords are stored exclusively as secure **hash values** (no plaintext).

If desired, login via **SSO (Single Sign-On)** using existing Microsoft accounts is available. This allows companies to use their existing Azure AD / Microsoft Entra policies (e.g., MFA, Conditional Access).

---

9. Control Over Input Data

Our platform processes only the data that **users themselves enter or upload**. This generally includes technical parameters such as:

- Energy demand values
- Load profiles
- Performance data
- Parameters for the technical design of systems

Key security principles:

- No external data sources are automatically imported that could contain classified or critical information.
- Users retain full control over the type of data they upload.
- In security-sensitive contexts, **approximated or synthetic load profiles** can easily be used, ensuring that no conclusions can be drawn about critical infrastructure.
- Upon request, the **complete and irreversible deletion** of all project data can be initiated at any time.

---

10. Company Structure & Independence

nPro Energy GmbH is **fully economically independent**. There are no financial or organizational dependencies on external companies, energy providers, or institutions. The development and operation of the SaaS platform are carried out **independently** and without any external influence.

---

11. References

Our software is successfully used in production by a wide range of professional users. These include:

- Energy suppliers and **companies operating critical infrastructure** (explicit references available upon request, as some may not be publicly named), for example ***Veolia S.A.*** or ***ENGIE S.A.***
- **60 municipal utilities** in Germany, including *Stadtwerke München*, *Stadtwerke Leipzig*, and *Berliner Stadtwerke*.
- **State authorities** in Germany, such as *Gebäudemanagement Schleswig-Holstein AöR*.
- More than **250 engineering firms**, consulting companies, and private planning organizations.
- Additional references available at https://www.npro.energy/main/en/references