Energy & Utilities Sector Guide

Data Protection and Compliance

Stannp operates as a Data Processor under UK GDPR and Data Protection Act 2018 with ICO registration ZA134992. All customer account and billing data is classified as confidential with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating. Data is hosted exclusively in Ireland (EEA) on Microsoft Azure with no transfers outside the EEA. ISO 27001, Cyber Essentials, and PCI-DSS certifications ensure regulatory compliance.

High Availability Structure

The platform delivers 99%+ uptime SLA with 24/7 SIEM monitoring and 12-month audit log retention. Critical services maintain RTO 30 minutes and RPO 6 hours for databases. Multi-factor authentication is mandatory for all internal systems with 2-hour session timeouts. Access follows role-based access control with least privilege principles and unique user authentication.

Security Testing & Monitoring

Comprehensive security measures include:

•   Monthly vulnerability scans using Qualys and Security Scorecard

•   Annual penetration testing and security assessments

•   Automated GitHub vulnerability scanning for source code

•   OWASP Top 10 application security testing

•   Critical patches within 7 days, important within 14 days, moderate within 30 days

Document Management & Recovery

Critical data backups occur every 15 minutes with daily full backups retained for 30 days. All backups are encrypted and geographically separated within the EEA. Standard retention is 3 years (customisable) with 2-month processing retention. Secure disposal procedures include physical destruction of hard drives before equipment disposal, complying with WEEE legislation.
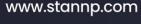
Incident Response & Business Continuity

Data breaches are reported to the ICO within 72 hours. The incident management framework classifies incidents by severity (Critical, Major, Minor) with structured response: detection, containment, investigation, eradication, recovery, and post-incident review. Comprehensive Business Continuity Plan covers all facilities with regular testing through recovery scenarios and tabletop simulations.

Physical Security & Staff Training

Facilities maintain 24/7 alarm monitoring and CCTV surveillance with controlled access. Clean desk policy and locked cabinets protect confidential materials. All staff receive annual security awareness training covering UK GDPR, phishing, social engineering, incident reporting, and authentication best practices. Role-specific training includes OWASP Top 10 for developers and risk management for security personnel.

Document Name:	TC02	Version No:	1	Date:	1st October 2025	Review Date:	1st October 2026

www.stannp.com

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ

01271 320 863
www.stannp.com

Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992