Energy & Utilities Sector Guide

Customer Billing & Transactional Mail Security

Energy suppliers and utilities operate in a highly regulated environment with continuous operational demands. Stannp operates under applicable US privacy regulations including state data protection laws, providing the secure infrastructure necessary for processing customer billing communications and consumption data.

All customer account and billing data receives confidential classification with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating. ISO 27001 and PCI-DSS certifications ensure regulatory compliance with regulatory requirements.

Supporting energy suppliers and utilities with secure transactional mail processing for billing statements, account notifications, and regulatory communications. Our production facilities operate enhanced confidentiality protocols specifically designed for processing sensitive customer billing data and consumption information, maintaining customer trust in energy communications.

Operational Resilience for Billing Cycles

The platform delivers 99%+ uptime SLA supporting the continuous processing requirements essential for billing cycles and regulatory deadline management. Critical database services maintain RTO 30 minutes and RPO 6 hours, ensuring billing communications continue without interruption during incidents.

Organizations manage their own user accounts and access controls within the platform, enabling role-based access control with least privilege principles. Multi-factor authentication is available for enhanced account security. Production facilities maintain segregated processing environments for transactional mail, with dedicated staff trained in handling confidential billing communications and customer consumption data.

Security Testing & Infrastructure Monitoring

Monthly vulnerability scans using Qualys and Security Scorecard assess infrastructure and application security across all systems processing customer billing data. These third-party security tools provide independent validation of our security posture.

OWASP Top 10 application security testing protects against common web application vulnerabilities that could compromise billing systems. Automated GitHub vulnerability scanning monitors source code continuously, identifying security issues during development.

CVSS-based patch management ensures timely remediation with critical vulnerabilities addressed within 7 days, important patches within 14 days, and moderate patches within 30 days. This risk-based approach prioritizes patches according to severity while minimizing operational disruption to billing processes.

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

Billing Data Protection & Recovery

Critical billing data receives backup every 15 minutes with daily full backups retained for 30 days. All backup data is encrypted and stored in zonally separated locations, ensuring recovery capability during peak billing periods.

Organizations manage their own data retention policies within the platform. The system supports appropriate data retention periods in compliance with applicable privacy regulations. Secure disposal procedures include physical destruction of hard drives before equipment disposal.

Incident Response & Business Continuity

Data breaches are reported to relevant authorities within 72 hours. The incident management framework classifies incidents by severity (Critical, Major, Minor) with structured response processes including 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, ensuring continuous operations during peak billing periods including winter demand and regulatory reporting deadlines.

Data Security & Staff Training

All staff receive annual security awareness training covering applicable US privacy regulations, phishing, social engineering, incident reporting, and authentication best practices. Staff handling transactional mail receive additional training on confidentiality protocols for billing communications and customer consumption data, ensuring appropriate handling throughout the production process.

All new employees are subject to background checks before commencing employment, providing appropriate vetting for personnel handling confidential customer billing data.

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