Security Awareness & Training Guide

Overview

Stannp maintains a comprehensive security awareness and training programme to ensure all employees understand their information security responsibilities and actively contribute to protecting customer data. Technical security controls alone cannot secure information—effective security requires the awareness and proactive support of all employees.

Comprehensive Training Programme

All staff receive annual security awareness training covering information security policies and procedures, UK GDPR and data protection requirements, recognising and responding to security threats including phishing and social engineering, data handling and classification, physical security protocols, incident reporting procedures, and authentication best practices. Training commences upon joining the organisation and continues on a rolling basis to maintain awareness of current security issues and challenges.

Role-Specific Training

Beyond foundational awareness, employees with specific security responsibilities receive additional specialised training. Developers and system administrators receive training on secure coding practices, OWASP Top 10 security guidelines, and technical security controls. Information security, compliance, and operations personnel receive training on risk management, incident response, and security governance. All technical personnel receive specialised training appropriate to their roles, reflecting prior experience, qualifications, and job requirements.

Induction & Ongoing Development

Data protection training is provided upon induction with annual refreshers. Information security training is delivered during onboarding with annual updates covering evolving threats, new policies, and regulatory changes. HIPAA training is provided on induction for relevant personnel with annual updates. Regular communications keep employees informed of policy changes and emerging threats.

Diverse Delivery Methods

We deliver security awareness through multiple approaches to suit different learning preferences. Training courses provide focused, detailed instruction through classroom or online delivery. Workshops and case studies offer practical, interactive learning. Written materials including policies and guidelines provide reference resources. Our SharePoint site serves as the central repository for all security information, policies, and guidance materials accessible to all employees.

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

Threat Recognition & Response

Employees receive training on recognising and responding to common security threats including phishing emails and social engineering tactics, malware and suspicious attachments, unauthorised access attempts, data security breaches and incident indicators, and physical security concerns. Training includes proper use of multi-factor authentication, protecting authentication devices, and recognising credential phishing attempts. This addresses attacks targeting humans rather than technical systems.

Compliance & Accountability

All employees and third-party personnel must familiarise themselves with Stannp's security policies, standards, and guidelines. Training ensures understanding of obligations under information security policies, UK GDPR and data protection laws, PCI-DSS requirements, and contractual obligations. Employees are personally accountable for complying with applicable policies, laws, and regulations. Training includes incident reporting procedures, escalation paths, and the importance of prompt reporting.

Tailored Content

Security awareness and training materials are tailored to suit intended audiences. Non-technical employees receive awareness content focused on their responsibilities without overwhelming technical detail. Technical staff receive detailed information necessary to implement security controls properly. Managers receive training on their responsibilities for staff security and incident response coordination.

Continuous Improvement & Measurement

We regularly assess programme effectiveness through awareness test results, employee feedback, incident analysis identifying training gaps, compliance audit findings, and industry best practice reviews. Compliance measures include management oversight of training completion, reviews and audits of awareness levels, checking uptake of training opportunities, and incident analysis to identify training needs.

Universal Applicability

Our programme applies throughout the organisation regardless of whether employees use computer systems, as all employees are expected to protect all forms of information including computer data, written materials, and intangible knowledge. The programme also applies to third-party employees working for Stannp, whether bound by contractual terms or generally held standards of ethics and acceptable behaviour.

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

Commitment to Security Culture

Our comprehensive security awareness and training programme ensures all employees understand their security responsibilities and actively contribute to protecting customer data through ongoing training, diverse delivery methods, role-specific content, and continuous improvement, maintaining a strong security culture across the organisation.

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