Access Control Guide

Overview

Stannp implements comprehensive physical and logical access controls across all networks, IT systems, and services to provide authorised, granular, auditable, and appropriate user access. Our controls ensure the confidentiality, integrity, and availability of all data in accordance with our Information Security Policy.

Core Principles

Least Privilege & Need-to-Know

Access rights are granted following strict least privilege and need-to-know principles. Users receive only the access necessary to perform their specific job functions, ensuring customer data is accessed only when required.

Unique User Authentication

Access control is implemented via individual user accounts secured by passwords. Generic or shared identities are never used to access customer data or personally identifiable information. Every user is individually identifiable and accountable.

Customer Data Protection

All customer data is classified as confidential and protected with the highest level of security controls including multi-layered firewall protection, network segregation, role-based access control (RBAC), encryption at rest and in transit, and comprehensive access logging and monitoring.

Access Control Implementation

Role-Based Access Control (RBAC)

Users receive permissions appropriate to their role. RBAC ensures employees can only access data specifically required for their job responsibilities, with access controlled through firewalls, network segregation, secure authentication, and access control list restrictions.

Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is mandatory for all internal systems, providing an additional layer of security beyond username and password authentication using time-based one-time passwords (TOTP) or authentication applications. MFA is available as an optional security enhancement for customer accounts.

Session Management

Session timeouts of 2 hours for all users to ensure inactive sessions cannot be exploited. Screen-locking systems and authentication device protection provide additional security layers.

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

Privileged Access Management

Restricted Privileges

Administrator and privileged access is managed through access control procedures.

Enhanced Controls

Privileged access receives additional security with session timeouts of 2 hours, comprehensive logging and monitoring, segregation from standard operations, and restrictions preventing use for routine activities.

Administrative Segregation

Administrative duties are segregated between development, test, and production environments. This segregation of duties prevents any single person from having end-to-end control and ensures appropriate checks and balances.

Customer Data Segregation

Complete Isolation

Each customer's data is completely segregated and accessible only to authorised users within that customer account. Our multi-tenancy architecture ensures complete data isolation through unique account IDs, logical data separation, network-based tenant separation, and regional separation capabilities.

Customer Platform Controls

The Stannp platform uses role-based user accounts enabling customers to have granular control over their data. Customers can define which users have access and what permissions each user has, providing complete control over who within their organisation can access their data.

Remote Access Security

Controlled Access

Remote access is controlled through authentication and connection security measures.

Physical Access Control

Access to network infrastructure is controlled through restricted key access, with keys provided only to authorised personnel. This prevents unauthorised physical access to systems and equipment.

Access Provisioning & De-provisioning

New User Access

Access is granted following strict authorisation processes based on job role and responsibilities. New users receive only the minimum access necessary for their specific functions, following least privilege principles.

Access Removal

Access is promptly de-provisioned when employees leave or change roles. Regular access reviews ensure former employees cannot retain system access and that current employees have only appropriate access for their current role.

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

Monitoring & Auditing

Comprehensive Logging

All access to systems and data is logged and monitored. These logs provide complete visibility into who accessed what data, when, and from where, ensuring accountability and enabling investigation of any security concerns.

Continuous Monitoring

Our SIEM system provides automated monitoring of access logs for suspicious activity. Alerts automatically trigger in-person security reviews, and access controls are monitored regularly through audits to ensure policy compliance.

Regular Testing

Access control measures are regularly tested through penetration testing to validate effectiveness and identify any vulnerabilities. Testing includes our own infrastructure and, where applicable, our cloud service providers.

Cloud & System Security

Cloud System Controls

All cloud-based systems meet our rigorous access control standards. Every employee accessing cloud systems uses unique credentials with complex passwords and mandatory multi-factor authentication to maintain secure access control at all times.

Access Control Methods

Access is controlled through multiple methods including explicit device logon, file and folder permissions, user account privilege limitations, server and workstation access rights, firewall permissions, network access control lists (ACLs), authentication requirements, database access rights, and encryption at rest and in transit.

Compliance & Standards

Regulatory Compliance

Our access control measures comply with UK GDPR, PCI-DSS, and ISO 27001 requirements. Regular audits verify ongoing compliance with these standards and industry best practices.

Commitment to Access Security

We maintain strict access controls to ensure your data remains secure and is accessed only by authorised personnel for legitimate business purposes. All access is logged, monitored, and regularly audited for compliance, ensuring the highest standards of data protection.

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