Backup and Recovery Policy Guide

Overview

Our backup policy ensures the reduction of loss of critical company and customer information and minimises business downtime in the event of a data loss disaster. We maintain comprehensive backup procedures to protect all data processed through our platform.

Business Critical Data Protection

Automated Daily Backups Business critical data, including the Stannp platform database containing customer information, is automatically backed up daily. Critical data is backed up every 15 minutes to ensure minimal data loss in any scenario.

Secondary Backup System Weekly secondary backups provide an additional layer of protection for business critical data. This dual-backup approach ensures redundancy and increases data recovery options in the event of system failure.

Geographic Separation All backup data is stored in geographically separate server regions from the primary data location. This ensures that regional incidents or failures do not affect both primary and backup data simultaneously.

Backup Retention and Storage

Retention Period Daily backups are retained for 30 days, providing ample recovery options for any data loss scenarios. This retention period balances storage efficiency with comprehensive data recovery capabilities.

Secure Storage and Encryption All backups are encrypted using best cryptography methods as defined in our Cryptography Policy. Backup data is securely stored in accordance with our Data Transfer and Storage Policy, ensuring the same level of protection as live data.

Recovery Procedures

Backup Infrastructure Our backup architecture ensures critical data can be restored when required. Backups are encrypted and stored across separate availability zones, with 30 days of immediately available recovery points and 12 months total retention.

Automated Monitoring All automated backups are logged to verify successful completion. The Dev team receives immediate notification if any automated backup fails, allowing for rapid response and resolution.

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

High Availability and Uptime

Service Level Agreement We operate with a 99%+ uptime SLA supported by redundant systems and our comprehensive backup infrastructure. This ensures continuous service availability and rapid recovery capability.

Redundant Systems Multiple redundant systems work alongside our backup procedures to maintain service availability. This infrastructure is designed to handle failures without service interruption while backups provide additional recovery options.

Business Continuity Integration

Comprehensive Disaster Recovery Our backup policy integrates with comprehensive disaster recovery and business continuity procedures. These plans include both data recovery and operational continuity measures, ensuring service can be maintained or rapidly restored.

Manual Processing Fallback In addition to automated backup systems, we maintain manual processing fallback capabilities as part of our business continuity planning, providing multiple recovery pathways.

Non-Critical Data

Non-critical data is backed up at least monthly using cloud services with automated backup policies. Departments may implement more frequent backups based on their specific requirements.

Data Protection Assurance

Our backup policy ensures that customer data is protected with multiple layers of redundancy, encryption, and geographic separation. Combined with regular testing and monitoring, these procedures provide robust protection against data loss while maintaining the confidentiality and integrity of all backed-up information.