Stannp.com
The Direct Mail Platform

Business Continuity and Incident Management Guide

Overview

Stannp maintains comprehensive Business Continuity and Disaster Recovery plans to ensure service availability and rapid recovery in the event of disruptions. Our structured approach minimises downtime and protects customer data whilst maintaining operational continuity.

Business Continuity Planning

Comprehensive Coverage Our Business Continuity Plan covers all processes, procedures, services, people, and resources across our office and warehouse facilities. The plan addresses potential incidents including fire, severe weather, technical failures, utility failures, loss of key personnel, and supplier disruptions.

Clear Objectives During any incident, our priorities are to ensure staff safety, maintain production output, preserve our assets, sustain business operations according to executive priorities, and return to normal operations as quickly as possible.

Defined Activation Criteria The plan can be activated by senior leadership team members, ensuring rapid response even if key personnel are unavailable. Clear assessment procedures determine when full business continuity arrangements should be invoked.

Incident Management

Structured Response Framework Our incident management policy provides detailed procedures for handling disruptions to critical technical or infrastructure services, equipment, or data. Incidents are classified by severity with corresponding response protocols and escalation procedures.

Clear Roles and Responsibilities The Chief Technical Officer maintains overall accountability, supported by dedicated senior technical and engineers who coordinate response, implement containment measures, and facilitate recovery. Business Impact Assessment and customer communication are managed by operations leadership.

Rapid Response Times Initial incident reports are logged within 15 minutes of detection. Recovery Time Objectives (RTOs) range from 30 minutes for critical platform services to 24 hours for non-critical systems, ensuring minimal service disruption.

Recovery Objectives

Platform and API Services Critical platform services maintain a Recovery Time Objective of 30 minutes with a Recovery Point Objective of 48 hours, ensuring rapid restoration with minimal data loss.

Database Protection Our platform database, which holds customer data, has a Recovery Time Objective of 30 minutes and a Recovery Point Objective of just 6 hours, providing robust protection for your information.

Website and Communications Website services maintain a 30-minute recovery target, whilst email and phone systems are restored within 4 hours, ensuring business communications remain available.

Backup Strategy

Frequent Database Backups Platform database backups occur automatically with full backups weekly, differential backups twice daily, and transaction log backups every five minutes. A replicated database provides additional protection with synchronisation every 6 hours.

Code and Configuration Protection All platform code, API services, and website configurations are backed up with every code change through our version control systems. This ensures immediate availability of all current and historical configurations.

Encrypted and Geographically Separated All backups are encrypted both in transit and at rest. Critical data is stored in geographically separate server regions within Azure's infrastructure, protecting against regional incidents or failures.

Regular Testing Backup systems are monitored and tested every 6 months to ensure reliability. Full recovery testing occurs annually to validate restoration procedures and identify any improvements needed.

Disaster Recovery Procedures

Multiple Recovery Options Our disaster recovery procedures include work-from-home capabilities for office staff, alternative facility arrangements for warehouse operations, and manual processing fallback capabilities to maintain service continuity.

Documented Recovery Processes All recovery procedures are fully documented with clear step-by-step instructions, ensuring any qualified team member can execute recovery operations effectively.

Testing and Preparedness

We conduct regular business continuity and incident management testing to ensure our plans remain effective and our teams are prepared to respond. This includes monthly tabletop exercises, periodic simulations, and annual full plan testing. Staff involved in incident management undergo regular training to maintain readiness and familiarity with procedures.

Communication During Incidents

Structured Communication Plan A comprehensive Incident Communication Plan ensures timely, accurate, and consistent communication with stakeholders during incidents. Clear communication phases, defined roles, and message templates maintain transparency throughout the incident lifecycle.

Stakeholder Updates Internal teams, customers, and relevant stakeholders receive appropriate updates based on incident severity and impact. Communication effectiveness is evaluated during post-incident reviews.

Continuous Improvement

Post-Incident Reviews Formal reviews are conducted for all major and critical incidents. Findings are documented, analysed, and used to update incident management policies and procedures, ensuring continuous improvement.

Regular Training and Simulations Staff involved in incident management undergo periodic training and simulations, including tabletop exercises, to ensure readiness and familiarity with procedures. Communication processes are tested as part of preparedness exercises.

Policy Updates Business Continuity and Disaster Recovery procedures are reviewed and updated regularly to incorporate lessons learned, industry best practices, and compliance with ISO 27001 standards.

High Availability

99%+ Uptime SLA We maintain a 99%+ uptime Service Level Agreement supported by redundant systems and infrastructure designed for high availability. Our platform operates across multiple server regions to ensure continuous service delivery.

Proactive Monitoring Continuous monitoring through automated systems tracks performance metrics, system health, and potential incidents, enabling rapid detection and response to any issues before they impact service.

Compliance and Legal Requirements

All incident management and business continuity practices comply with applicable legal and regulatory requirements including UK GDPR, PCI-DSS, and ISO 27001 standards.