Incident Management Guide

Overview

Stannp maintains a comprehensive incident management framework to ensure rapid response to any disruption of IT services or compromise of systems and data. Our structured approach ensures swift return to normal operations with minimal business impact. We are committed to continuously improving our incident management processes through regular reviews and alignment with ISO 27001 best practices.

What is an Incident?

An incident is any unplanned event that disrupts or threatens to disrupt normal operations, affects service quality, or compromises security. This includes system outages, security breaches, data corruption, infrastructure failures, and service degradation.

Incident Classification

Incidents are classified by severity to ensure appropriate response:

Severity Level	Impact	Examples
Critical	Immediate and severe risk to security, operations, or data integrity	• Data breach with unauthorised access • System-wide outage • Server compromise • Critical software bugs causing data loss
Major	Potential threat to operations or important data but not immediately critical	• Significant software bugs • Unauthorised access attempts • Security patch failures • Configuration exposures
Minor	Minimal impact with no significant compromise of data or security	• Policy violations • Minor configuration errors • Non-sensitive information exposure

Recovery Objectives

We maintain defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical services to ensure rapid restoration:

Service	Maximum Data Loss (RPO)	Maximum Downtime (RTO)
Platform Dashboard & API	48 hours	30 minutes
Platform Database	6 hours	30 minutes
Website	48 hours	30 minutes
Email Systems	48 hours	4 hours
Office Infrastructure	N/A	4 hours

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

Incident Response Process

Detection & Reporting

Incidents are detected through automated monitoring, user reports, or security alerts and logged immediately upon detection.

Classification & Prioritization

Initial assessment determines incident severity and potential impact, ensuring appropriate resource allocation.

Containment

Immediate actions are taken to limit the spread and impact of the incident, protecting unaffected systems.

Investigation

Technical teams investigate root causes and assess the full scope of impact.

Eradication

Measures are implemented to remove the root cause and prevent recurrence.

Recovery

Normal services are restored with validation of system integrity following documented procedures.

Post-Incident Review

Formal reviews identify lessons learned and drive continuous improvement.

Communication

We maintain a comprehensive communication plan ensuring timely, accurate updates to stakeholders throughout any incident. Regular status updates are provided to affected parties, with clear resolution notifications once services are restored.

Backup & Recovery Strategy

Platform Database

Regular full backups, differential backups, and continuous transaction log backups with database replication.

Platform & API Code

Continuous backup on every code change through secure repository management.

Email Systems

Daily backups with redundant storage.

Website

Continuous backup on every code change through secure repository management.

All backups are encrypted both in transit and at rest to protect against unauthorised access. Automated monitoring verifies successful backup completion with immediate notification for any failures.

Testing & Continuous Improvement

Our incident management capabilities are regularly tested and validated through:

- Periodic recovery scenario testing
- Staff training and readiness exercises
- Tabletop simulations
- Post-incident reviews and process updates

Compliance & Standards

Our incident management practices comply with:

- ISO 27001 information security management standards
- UK GDPR data protection requirements
- PCI-DSS payment card industry standards

Commitment to Service Resilience

Through clearly defined procedures, regular testing, continuous training, and lessons learned processes, we maintain the resilience and reliability our customers depend on whilst minimising the impact of any incidents that occur.