oneAdvanced

Technical & Organisational Security Measures (TOMs)

Cyber Security

Table of Contents

Disclaimer 3

1. Executive Summary 4
2. Scope & Application 5
3. Information Security Governance 5
4. Security Operations & Monitoring 6
5. Security Information and Event Management (SIEM) 6
6. Vulnerability Management 7
7. Threat Detection and Prevention 7
8. Security Metrics and Reporting 8
9. Hosting & Infrastructure Resilience 8
10. Public Cloud Infrastructure 9
11. Geographic Redundancy & Disaster Recovery 9
12. Automated Failover & High Availability 10
13. Network Segmentation & Isolation 10
14. Supplier Due Diligence & Oversight 10
15. Annual Resilience & Failover Testing 11
16. Post-Incident Resilience Validation 11
17. Encryption in Transit & at Rest 12
18. Encryption Key Management 12
19. Backup Encryption 12
20. Access Control & Authentication 12
21. Audit Logging & Monitoring 13
22. Backup & Retention Schedule 14
23. Third-Party & Sub-Processor Controls 14
24. Certifications & Compliance 14
25. Vulnerability Management and Patching 16

26. Incident Response & Breach Notification.....16
27. Business Continuity & Disaster Recovery.....17
28. Change Control.....19

Disclaimer

This document contains confidential and / or proprietary information. The content must not be disclosed to third parties without the prior written approval of OneAdvanced Group Limited or one of its subsidiaries as appropriate (each referred to as "OneAdvanced"). External recipients may only use the information contained in this document for the purposes of evaluation of the information and entering into discussions with OneAdvanced and for no other purpose.

Whilst OneAdvanced endeavours to ensure that the information in this document is correct and has been prepared in good faith, the information is subject to change and no representation or warranty is given as to the accuracy or completeness of the information. OneAdvanced does not accept any responsibility or liability for errors or omissions or any liability arising out of its use by external recipients or other third parties.

No information set out or referred to in this document shall form the basis of any contract with an external recipient. Any external recipient requiring the provision of software and/or services shall be required to enter into an agreement with OneAdvanced detailing the terms applicable to the supply of such software and/or services and acknowledging that it has not relied on or been induced to enter into such an agreement by any representation or warranty, save as expressly set out in such agreement.

The software (if any) described in this document is supplied under licence and may be used or copied only in accordance with the terms of such a licence. Issue of this document does not entitle an external recipient to access or use the software described or to be granted such a licence.

The development of OneAdvanced software is continuous and the published information may not reflect the current status. Any particular release of the software may not contain all of the facilities described in this document and / or may contain facilities not described in this document.

OneAdvanced Group Limited is a company registered in England and Wales with registration number 05965280 whose registered office is at The Mailbox Level 3, 101 Wharfside Street, Birmingham, B1 1RF.

A full list of its trading subsidiaries is available at www.oneadvanced.com/privacy-policy/

1. Executive Summary

OneAdvanced Computer Software Group Limited and its subsidiaries (together “OneAdvanced”, “we”, “us”, “our”) act as a data processor for organisations across the United Kingdom, serving regulated sectors including healthcare, legal services, education, and local government. This document sets out the technical and organisational measures (TOMs) implemented pursuant to Article 32 of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and our obligations under Schedule 5 Data Protection of our Terms and Conditions with our customers.

These measures are designed to ensure a level of security appropriate to the risk of processing personal data, including special category data such as health information, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. Our security framework reflects the sensitivity of the data entrusted to us and the critical importance of service continuity across all sectors we serve.

OneAdvanced processes personal data solely on the documented instructions of our customers acting as Data Controllers. We implement comprehensive safeguards across people, processes, and technology to protect the Confidentiality, Integrity, and Availability (CIA) of all data entrusted to us. Our security posture is validated through independent certifications including ISO/IEC 27001:2022, Cyber Essentials Plus, and exceeding standards in the NHS Data Security and Protection Toolkit.

This document is reviewed annually and updated to reflect changes in our security posture, regulatory requirements, industry best practices, and feedback from customers and regulatory authorities. We are committed to continuous improvement in our data protection capabilities and transparent communication with our customers regarding our security measures.

All personnel at OneAdvanced, including employees, directors, contractors and sub-processors, are required to comply with these measures and our supporting information security and data protection policies.

2. Scope & Application

2.1 Document Scope

This document outlines the technical and organisational measures (TOMs) that align with OneAdvanced policies applicable to our entire product range. These measures are regularly reviewed and enhanced to maintain a security standard appropriate for mitigating risk and meeting our legal, regulatory, and contractual obligations related to personal data processing.

These measures apply across the entire data lifecycle: collection, storage, processing, transmission, retention, and secure disposal. Where applications are hosted in a customer-managed Private Cloud or On-Premise configuration, OneAdvanced does not control all aspects of the hosting environment; the measures described in this document apply to the extent that OneAdvanced retains operational responsibility.

2.2 Regulatory Framework

OneAdvanced's TOMs are designed to ensure compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- NHS Scotland Information Governance Standards (NSS)
- NHS Records Management Code of Practice
- NHS Data Security and Protection Toolkit requirements
- NHS Digital Technology Assessment Criteria (DTAC)
- National Data Guardian's 10 Data Security Standards
- Medical Devices Regulations 2002 (where applicable)
- Cyber Essentials Plus scheme requirements.
- ISO27001:2022
- ISO42001:2023
- All other applicable data protection and information security legislation in force in the UK and other relevant local jurisdictions (Australia, New Zealand, Ireland).

3. Information Security Governance

3.1 Security Leadership and Accountability

OneAdvanced maintains executive-level accountability for information security through our Chief Information Security Officer (CISO), who reports directly to the Chief Technology Officer, with regular reporting to the CEO and the Board.

Information Security Management System (ISMS)

OneAdvanced operates a comprehensive ISMS certified to ISO/IEC 27001:2022 (Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems) by a UKAS-accredited certification body. The ISMS scope covers all OneAdvanced UK operations, infrastructure, and systems processing customer data. External surveillance audits are conducted annually, with full recertification audits every three years.

3.2 Information Security Strategy and Roadmap

Our information security strategy is reviewed and updated annually. The security roadmap is aligned with our product development roadmap and business growth strategy, ensuring security is integrated into all technology and commercial decisions. Security governance is overseen by the Chief Information Security Officer (CISO).

3.3 Security Policies

All personnel at OneAdvanced are required to comply with our comprehensive suite of information and cyber security policies.

Policies are regularly reviewed (according to individualised review cycle), approved by the control owner, and made available to all personnel via our internal policy management system. Compliance is monitored through regular audits, with non-compliance subject to disciplinary procedures.

4. Security Operations & Monitoring

4.1 Security Operations Centre (SOC)

OneAdvanced operates a 24/7/365 Security Operations Centre staffed by security analysts. The SOC provides:

Continuous Monitoring: Real-time monitoring of all infrastructure, applications, and endpoints across our estate.

Threat Detection: Automated correlation of security events using a Security Information and Event Management (SIEM) platform with threat intelligence feeds from a threat and vulnerability manager.

Incident Response: Immediate investigation and containment of security incidents according to documented playbooks.

Threat Intelligence: Consumption and analysis of threat intelligence from NCSC, CiSP (Cyber Security Information Sharing Partnership), and commercial sources

Security Metrics: Daily dashboards and weekly/monthly reporting on security posture, incident trends, and key risk indicators.

5. Security Information and Event Management (SIEM)

Our SIEM platform aggregates, correlates, and analyses security events from all systems. SIEM logs are retained for 12 months in write-once, tamper-evident storage, with integrity validation through cryptographic hashing.

6. Vulnerability Management

OneAdvanced operates a comprehensive vulnerability management program:

Continuous Vulnerability Scanning: Automated scanning of all infrastructure and applications using enterprise vulnerability management platforms.

Risk-Based Remediation: Vulnerabilities prioritised using CVSS (Common Vulnerability Scoring System) scores, exploitability, and asset criticality.

Patch Management: Structured patch deployment with defined Service Level Agreements.
Exception Management: Risk-based exception process for vulnerabilities that cannot be immediately remediated, with compensating controls documented.

Penetration Testing: Annual independent penetration testing by NCSC CHECK-approved providers.

Vulnerability Disclosure: Co-ordinated disclosure process for security researchers reporting vulnerabilities.
Vulnerability scan results and remediation status are reviewed by the Security Operations Team.

7. Threat Detection and Prevention

Multiple layers of security controls protect against cyber threats:

7.1 Endpoint Security:

- Endpoint detection and response (EDR) on workstations and servers.
- Anti-malware with machine learning detection.
- Full disk encryption on all user endpoints.

7.2 Email Security:

- Advanced email filtering with anti-spam, anti-phishing, and malware detection.
- Link sandboxing for suspicious URLs.
- User awareness training and simulated phishing campaigns.
- DMARC, SPF, and DKIM authentication to prevent spoofing.

7.3 Zero-Day Protection:

- Behaviour-based detection for unknown threats.
- Threat intelligence integration for emerging threats.
- Rapid deployment of out-of-band patches for critical zero-day vulnerabilities.

8. Security Metrics and Reporting

Security performance is tracked through comprehensive metrics reviewed by leadership:

- Number and severity of security incidents (by category and trend analysis).
- Vulnerability remediation metrics (SLA compliance, backlog, time-to-remediate).
- Patch compliance rates across infrastructure.
- Phishing simulation results and training completion rates.
- Mean time to detect and respond to incidents.
- Penetration test findings and remediation status.
- Access review completion rates.
- Security awareness training completion rates.

9. Hosting & Infrastructure Resilience

9.1 Data Centre Infrastructure

OneAdvanced operates from Tier III or equivalent UK data centres with enterprise-grade resilience features:

Tier III Design Characteristics include N+1 redundancy across all critical components, maintainable infrastructure (without service interruption), multiple independent distribution paths and 99.982% availability design target (1.6 hours maximum downtime per year).

Network Security:

- Firewalls with intrusion prevention systems (IPS).
- Network segmentation isolating customer environments and sensitive systems.
- DDoS (Distributed Denial of Service) mitigation at network edge.
- Web application firewalls (WAF) protecting internet-facing applications.

Physical Security: includes 24/7/365 security, access control card reader access with man-trap entry, CCTV, visitor escort and logging procedures.

Environmental Controls: includes precision cooling with temperature and humidity monitoring, early smoke detection and gas-based fire suppression, uninterruptible Power Supply (UPS) with N+1 configuration, generators with 48+ hours fuel capacity and automatic failover and environmental monitoring with 24/7 alerting.

Connectivity: includes diverse network connectivity from multiple Tier 1 carriers, physically diverse fibre routes, BGP routing for automatic failover between providers and DDoS mitigation at network edge.

All data centre providers maintain ISO/IEC 27001 certification and undergo annual audits.

10. Public Cloud Infrastructure

In addition to dedicated Tier III data centres, OneAdvanced operates from AWS (Amazon Web Services) and Microsoft Azure Public Cloud providers for specific products and services. Public cloud deployments utilise:

Virtual Private Clouds (VPCs): Isolated network environments with customer-specific segmentation.

Infrastructure as Code (IaC): Version-controlled infrastructure provisioned via Terraform or equivalent, ensuring consistency and auditability.

Equivalent Security Controls: Network isolation, encryption, access controls, logging, and monitoring equivalent to dedicated infrastructure.

Compliance Certifications: All cloud providers maintain ISO 27001, SOC 2 Type II and equivalent certifications relevant to healthcare data processing.

Restricted Access: Cloud infrastructure access is limited to authorised OneAdvanced engineering personnel with multi-factor authentication and just-in-time elevation.

Third-Party Access: Access to cloud environments by third parties (AWS/Azure support) requires prior approval, is logged, and is conducted under change control with OneAdvanced personnel oversight.

Public cloud security configurations are audited quarterly and align with Centre for Internet Security (CIS) benchmarks and NCSC Cloud Security Principles.

11. Geographic Redundancy & Disaster Recovery

Critical systems are deployed across geographically separate sites to ensure resilience:

Primary and Secondary Sites: Located at least 40 kilometres apart in compliance with ISO 22301 business continuity and ISO 27001 information security standards.

Independent Infrastructure: Separate power grids, network connectivity, and environmental systems to eliminate common failure modes.

Data Replication: Synchronous or asynchronous database replication between sites depending on application requirements.

Automated Failover: Health monitoring triggers automated failover for database and application tiers.

Failover Testing: Annual failover testing validates recovery capabilities.

Geographic separation ensures resilience against regional disruptions including power grid failures, natural disasters, and localised connectivity issues.

12. Automated Failover & High Availability

Systems are architected for high availability with automated recovery:

Database Clustering: Active-passive or active-active database clustering depending on application requirements.

Application Clustering: Load-balanced application servers with session persistence.

Health Monitoring: Real-time health checks at database, application, network, and infrastructure layers.

Automated Failover Triggers: Configurable health check thresholds trigger automatic failover without manual intervention.

Failover Validation: Post-failover validation ensures service restoration before traffic resumption.

Rollback Capability: Ability to fail back to primary site after issue resolution.

Failover mechanisms are tested during annual resilience testing and periodically invoked during planned maintenance to validate operational readiness.

13. Network Segmentation & Isolation

Customer environments are logically segregated to prevent unauthorised cross-customer access:

Virtual Private Clouds (VPCs): Dedicated VPCs for each customer or customer group with network isolation.

VLAN Segmentation: Virtual LANs segment traffic at Layer 2 for additional isolation.

Network Access Control Lists (ACLs): Stateful firewall rules permitting only necessary inter-zone traffic.

Micro-segmentation: Application-tier segmentation (web, application, database) with least-privilege network access.

Zero Trust Architecture Principles: Network location alone does not confer trust; all connections authenticated and authorised

Network segmentation is validated during annual penetration testing and reviewed quarterly as part of security architecture reviews.

14. Supplier Due Diligence & Oversight

All infrastructure providers (data centre operators, cloud providers, network carriers) undergo rigorous due diligence:

Pre-Engagement Assessment: Security questionnaires, certification verification, and financial stability review.

Contractual Safeguards: Data protection terms, security requirements, audit rights, and liability provisions in all contracts.

Ongoing Monitoring: Annual re-assessment of security posture and compliance with contractual obligations.

Audit Rights: Reserved right to audit supplier security controls or request independent audit reports.

Certification Requirements: ISO/IEC 27001 or equivalent information security certification is required for all critical suppliers.

Incident Notification: Suppliers contractually needed to notify OneAdvanced of security incidents as soon as reasonably possible

Supplier security posture is reviewed annually, with findings reported to the Information Security Steering Committee and escalated for material concerns.

15. Annual Resilience & Failover Testing

15.1 Resilience Testing Program Overview

OneAdvanced operates a structured resilience testing program conducted on a defined annual schedule covering the OneAdvanced product portfolio. Testing activity is planned in advance, with specific products and scenarios identified throughout the year to ensure coverage is risk-informed, systematic, and aligned to our Organisational Resilience framework.

The testing program is designed to validate that recovery capabilities perform as intended under realistic conditions. Scenarios are selected to reflect credible disruption events relevant to each product's architecture, dependencies, and operational context.

15.2 Single Point of Failure (SPoF) Audit

Annual audits to identify and validate mitigation of SPoF across infrastructure and application tiers. The scope includes:

Hardware Components: Server hosts, storage arrays, network switches, firewalls, load balancers.
Software Components: Operating systems, database management systems (RDBMS), middleware, critical application services.

Network Components: Network uplinks, routers, switches, firewalls, VPN concentrators.
External Dependencies: Third-party APIs, cloud services, DNS providers, certificate authorities

16. Post-Incident Resilience Validation

Following any significant incident affecting availability, data integrity, or security, targeted resilience testing is conducted to validate the effectiveness of remediation measures, confirm that the specific failure cannot recur, test any new safeguards or procedural changes and rebuild system resilience.

17. Encryption in Transit & at Rest

17.1 Encryption in Transit

All personal data transmitted across networks is protected using industry-standard encryption - TLS 1.3 Encryption - all HTTPS connections use TLS 1.3 (or TLS 1.2 minimum where TLS 1.3 is not yet supported). TLS certificates issued by trusted Certificate Authorities (CAs).

17.2 Encryption at Rest

Personal data stored on OneAdvanced systems is encrypted at rest:

Database Encryption: AES-256 encryption for all database files, Transparent Data Encryption (TDE) for SQL Server and equivalent for other RDBMS platforms, full disk encryption on all database servers with keys rotated every 12 months.

File Storage Encryption: AES-256 encryption for all file storage (NAS, SAN, object storage), server-side encryption for cloud storage (AWS S3, Azure Storage) and client-side encryption for highly sensitive data before transmission to storage.

Application Data Encryption: Sensitive fields (passwords, API keys, credentials) encrypted at application layer using FIPS 140-2 validated cryptographic libraries.

18. Encryption Key Management

Cryptographic keys are managed according to industry best practices

Cryptographic standards and algorithms are reviewed annually against guidance from National Cyber Security Centre (NCSC), National Institute of Standards and Technology (NIST) and industry best practices and emerging post-quantum cryptography developments. Deprecated or weak algorithms are systematically phased out according to published timelines.

19. Backup Encryption

All backup media is encrypted to protect against unauthorised access.

Backup encryption keys are managed under the same framework as production encryption keys.

20. Access Control & Authentication

20.1 User Access Management

Access to systems and personal data is controlled through comprehensive access management:

Multi-Factor Authentication (MFA): Mandatory to access systems processing personal data, such as Time-based One-Time Password (TOTP) via an authenticator app.

20.2 Privileged Access Management

Privileged access rights are allocated only where the role requires it and/or a legitimate business need has been identified, in accordance with the Principle of Least Privilege (PoLP). OneAdvanced governs privileged access through formal approval workflows, periodic access reviews, timely revocation of rights when no longer required, and defined accountability for all privileged account usage. OneAdvanced is currently evaluating dedicated privileged access management technology to complement existing administrative controls with additional automation, session monitoring, and just-in-time access provisioning.

20.3 Password Management

OA password policy aligns with NCSC and NIST guidance to support minimum length, complexity requirements balanced against usability (prefer length over complexity) and encouragement of unique, randomly generated passwords.

21. Audit Logging & Monitoring

21.1 Centralised Security Information and Event Management (SIEM)

All security-relevant events are collected in our centralised SIEM platform:

Log Sources:

- Administrative actions (configuration changes, user management, privileged operations).
- System events (service starts/stops, errors, performance anomalies).
- Security tool alerts (firewall, IPS, anti-malware, EDR).
- Network traffic logs (firewall rules, VPN connections).
- Application logs.

21.2 Database Audit Logging

All data access at the database layer is comprehensively logged:

Database Audit: SELECT, INSERT, UPDATE, DELETE– Retention: 12 months.

Application Logs: User navigation, consent changes, clinical calculations – Retention: 6 months. Integrity: Encrypted, centralised.

Log Access: Restricted to authorised processor staff.

Logged Database Operations:

- SELECT queries on tables containing personal data (with query parameters)
- INSERT, UPDATE, DELETE operations on patient/customer data tables
- Schema changes (ALTER, CREATE, DROP statements)
- Privilege grants and revocations
- Failed access attempts and permission denials

Database audit logs are essential for demonstrating compliance with data protection principles and supporting investigations of unauthorised access.

22. Backup & Retention Schedule

22.1 Backup Strategy and Procedures

OneAdvanced implements comprehensive backup procedures to ensure data availability and recoverability with weekly backups (full), daily incremental backups and continuous replication of real-time or near real-time for critical systems with low RPO requirements.

22.2 Retention Policy Exceptions

Retention periods may be extended in specific circumstances such as legal proceedings, investigations or regulatory inquiries, security related incidents or upon customer request (subject to technical feasibility and commercial agreement.

All retention policy exceptions are documented, approved by legal counsel where appropriate, and tracked until resolution.

23. Third-Party & Sub-Processor Controls

23.1 Sub-Processor Management Framework

OneAdvanced engages sub-processors only where necessary for service delivery and subjects all sub-processors to rigorous controls:

Sub-Processor Notification: Comprehensive list of sub-processors maintained and published at Sub_Processors List.

Sub-Processor Contracts: All sub-processors bound by written contracts imposing equivalent data protection obligations to those in the Schedule 5 Data Protection to our Terms and Conditions between OneAdvanced and the customer.
Contracts include confidentiality obligations, security requirements, data location restrictions, audit rights, and liability provisions.

24. Certifications & Compliance

24.1 Security and Quality Certifications

OneAdvanced maintains the following independently audited certifications:

ISO 27001:2022 – Information Security, Cybersecurity and Privacy Protection - **Information Security Management Systems.** Certified by UKAS-accredited certification body with annual surveillance audits plus full recertification every 3 years.

ISO 9001:2015 – Quality Management Systems. Ensures consistent delivery of high-quality products and services. Continuous improvement framework embedded in operations.

ISO 14001:2015 – Environmental Management Systems. Commitment to environmental sustainability and minimising environmental impact.

ISO 20000-1:2018 – Information Technology - Service Management. Service management processes aligned to industry best practices.

ISO 42001:2023 – Information Technology - Artificial Intelligence - Management System. Responsible AI governance framework for AI-enabled products and services, providing customers with independently verified assurance over AI development, deployment, and risk management practices

24.2 Certificate Access:

All certification certificates and executive summaries of audit reports are available via the OneAdvanced Trust Centre at https://trust.oneadvanced.com

24.3 Healthcare-Specific Certifications and Accreditations

NHS Care Identity Service 2 (CIS2) – NHS England Identity and Access Management

- Integration with NHS national authentication infrastructure.
- Support for smartcard and modern authentication methods.

NHS Data Security and Protection Toolkit (DSPT) – Standards Exceeded (2025/2026)

- Annual self-assessment externally audited.
- Publicly published DSPT submission available at https://www.dsptoolkit.nhs.uk.

NHS Digital Technology Assessment Criteria (DTAC)

- Assessment of clinical safety, data protection, technical security, interoperability, and usability for NHS deployments

24.4 Government and Industry Certifications

Cyber Essentials Plus

- UK Government-backed scheme certifying implementation of essential cybersecurity controls
- Annual independent assessment by accredited assessor
- Required for UK public sector contracts

EU Artificial Intelligence Pact

- Voluntary commitment to responsible AI development and deployment in anticipation of EU AI Act requirements

Social Value Quality Mark (Bronze)

- Recognition of commitment to social value including employment, skills development, and community benefit

24.5 Penetration Testing

OneAdvanced conducts regular independent security assessments:

- Annual Penetration Testing conducted annually by NCSC CHECK-approved provider.
- Scope includes internet-facing applications, APIs, infrastructure, and internal network (where applicable).

- Testing methodology aligned to OWASP Testing Guide, PTES (Penetration Testing Execution Standard), and NCSC guidance.
- Attestation summary of penetration test results available to customers upon request.

25. Vulnerability Management and Patching

Continuous Vulnerability Scanning:

- Automated vulnerability scanning of all infrastructure and applications.
- Integration with threat intelligence feeds for zero-day vulnerability detection.

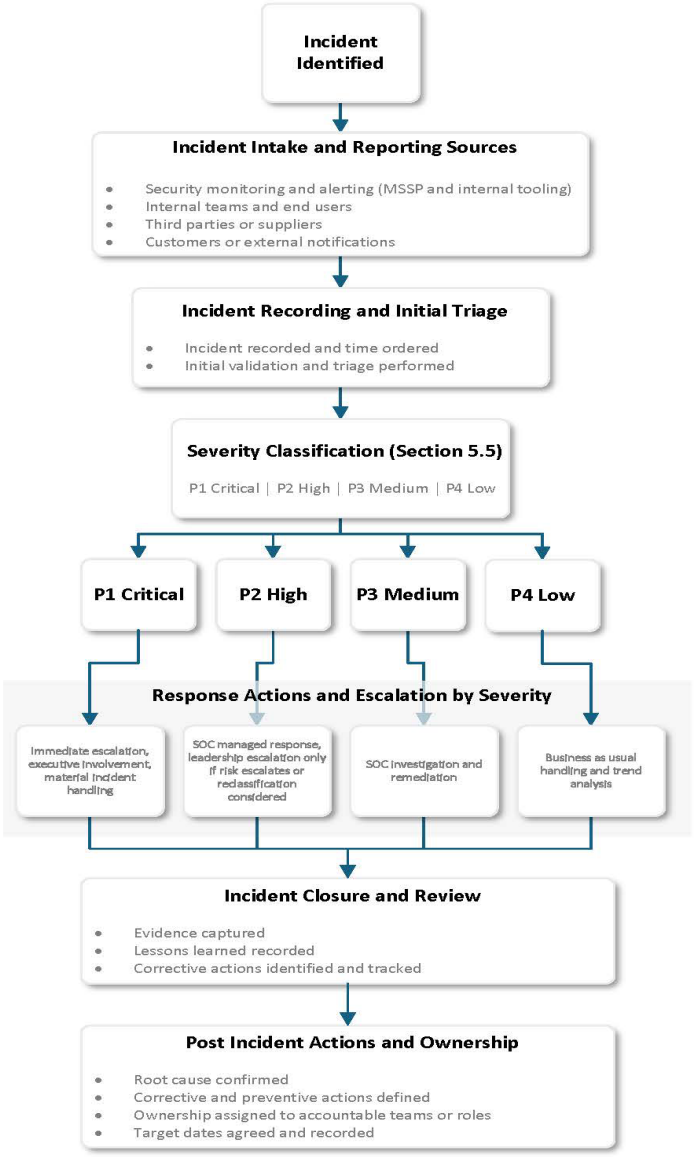
Risk-Based Patching Policy:

- Critical vulnerabilities: Patched within 15 days.
- High vulnerabilities: Patched within 15 days.
- Medium vulnerabilities: Patched within 30 days.
- Low vulnerabilities: Scheduled maintenance windows.

26. Incident Response & Breach Notification

26.1 Incident Classification and Severity

All security incidents are classified by severity to ensure appropriate response. See below diagram for process flow.



27. Business Continuity & Disaster Recovery

27.1 Business Continuity Management Framework

OneAdvanced operates a comprehensive Business Continuity Management (BCM) framework aligned to ISO 22301 standards:

Business Continuity Policy: Executive-approved policy defining objectives, scope, and responsibilities, commitment to maintaining business operations during disruptions.

Business Impact Analysis (BIA): Conducted every 2 years (or upon significant business change), identifies critical business functions, dependencies, recovery priorities, and maximum tolerable downtime and assessment of financial, operational, reputational, and regulatory impact of disruptions.

Risk Assessment: Identification of threats to business continuity (natural disasters, cyber-attacks, supply chain failures, pandemics, etc.), likelihood and impact assessment for each threat

Treatment Strategies: prevention, mitigation, transfer, acceptance.

Business Continuity Plans (BCPs): Documented plans for maintaining or rapidly resuming critical functions during disruptions covering incident activation criteria, roles and responsibilities, communication procedures, recovery procedures, alternative work arrangements. Department-level BCPs owned by Heads of Department and annual plan review and update.

27.2Disaster Recovery Planning

Disaster Recovery Plans (DRPs) ensure rapid recovery of IT systems and data. Product / service-specific DRPs documenting recovery procedures, including data restoration, system rebuilding, testing, validation and return to normal operations. DRPs are maintained by VP Platform Engineering and product owners.

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined for each critical system.

27.3Business Continuity Testing

Business continuity and disaster recovery plans are regularly tested including DR invocation tests, achievement validations, testing and restoration.

27.4 Alternative Working Arrangements

Plans ensure critical personnel can continue working during site unavailability with remote working capabilities with secure remote access, cloud-based collaboration tools – validated during Covid-19 pandemic response.

27.5Incident and Crisis Management

OneAdvanced operates a tiered incident management framework that escalates from Incident, through Major Incident, to Crisis Management, ensuring a proportionate and structured response at every level of severity. This is underpinned by formal Root Cause Analysis (RCA) and continuous improvement logs, both subject to internal audit, providing assurance that lessons are captured, embedded, and independently verified. The approach aligns with recognised best practice and international standards, including ISO 22301 (Business Continuity Management), ISO 22361 (Crisis Management), and ITIL incident management principles, reinforced by a Plan-Do-Check-Act cycle of continual improvement.

27.6 Return to Normal Operations

Following a business continuity event, structured procedures ensure safe return to normal. Procedures include verification of root cause of disruption has been resolved, system testing, phased monitored restoration and post-event review. All BCPs and DRPs are updated based on lessons learned.

28. Change Control

28.1 Change Control Framework

All changes to systems processing personal data are managed through formal change control:

Standard Changes: Pre-approved, low-risk, routine changes (e.g., password resets, minor configuration changes).

Normal Changes: Require assessment, approval, and scheduling (e.g., software patches, configuration updates)

Emergency Changes: Urgent changes to address critical security or availability issues (expedited approval with post-implementation review).

Documented change request including description, justification, impact assessment, rollback and testing plan. All requests are risk assessed considering data protection, security, availability, and operational impact for approval by the Change Advisory Board (CAB). Changes tested in non-production environment before deployment; rollback procedures documented and tested. Advance notification is sent to affected customers (minimum 7 days for planned maintenance). Changes are logged and audit trails are available for compliance reviews.

28.2 Regulatory Engagement

Information Commissioner's Office (ICO):

- Proactive engagement with ICO on data protection matters.
- Cooperation with ICO audits and investigations.
- Implementation of ICO recommendations and guidance

NHS Digital and NHS England:

- Engagement with NHS Digital on security standards, DSPT, and national cybersecurity initiatives.
- Alignment with NHS England's digital transformation strategy and data standards.

oneAdvanced

Powering the world of work

Our business software and IT services are the trusted choice for critical sectors, including healthcare, legal services, and education. We keep the world of work moving.

Speak to our expert consultants for personalised advice & recommendations, & get support on the products you are interested in.

Contact us

+44(0) 330 343 4000 www.oneadvanced.com hello@oneadvanced.com