Operational Security Plan

Hosted and Managed Services, United Kingdom

Document details

Title: Operational Security Plan

Client: Coordinate My Care

Author: Eugene Rudman

Version: 1.0

Document history

Version	Date	Author	Notes and updates
0.1	6 Mar 2020	Eugene Rudman	Initial draft
1.0	2 Feb 2021	Eugene Rudman	Approved release

Reviews and approvals

Version	Date	Reviewer / approver	Status
0.1	6 Mar 2020	Eugene Rudman	In review
1.0	2 Feb 2021	Julia Hopper (for Coordinate My Care)	Approved
1.0	2 Feb 2021	Eugene Rudman (InterSystems)	Approved

1 Contents

Document details 2
Document history 2
Reviews and approvals 2
1 Contents 3
2 Background, purpose and scope 5
3 Operational security objectives and controls 6
3.1 Information security policies (A5) 6
3.1.1 Management direction for information security 6
3.2 Organization of information security (A6) 6
3.2.1 Internal organization 6
3.2.2 Mobile devices and teleworking 6
3.3 Human resource security (A7) 7
3.3.1 Prior to employment 7
3.3.2 During employment 7
3.3.3 Termination and change of employment 7
3.4 Asset management (A8) 8
3.4.1 Responsibility for assets 8
3.4.2 Information classification 8
3.4.3 Media handling 8
3.5 Access control (A9) 9
3.5.1 Business requirements of access control 9
3.5.2 User access management 9
3.5.3 User responsibilities 9
3.5.4 System and application access control 9
3.6 Cryptography (A10) 10
3.6.1 Cryptographic controls 10
3.7 Physical and environmental security (A11) 11
3.7.1 Secure areas 11
3.7.2 Equipment 11
3.8 Operations security (A12) 12
3.8.1 Operational procedures and responsibilities 12
3.8.2 Protection from malware 12
3.8.3 Backup 12
3.8.4 Logging and monitoring 12

3.8.5 Control of operational software 13
3.8.6 Technical vulnerability management 13
3.8.7 Information systems audit considerations 13
3.9 Communications security (A13) 14
3.9.1 Network security management 14
3.9.2 Information transfer 14
3.10 System acquisition, development and maintenance (A14) 15
3.10.1 Security requirements of information systems 15
3.10.2 Security in development and support processes 15
3.10.3 Test data 15
3.11 Supplier relationships (A15) 16
3.11.1 Information security in supplier relationships 16
3.11.2 Supplier service delivery management 16
3.12 Information security incident management (A16) 17
3.12.1 Management of information security incidents and improvements 17
3.13 Information security aspects of business continuity management (A17) 18
3.13.1 Information security continuity 18
3.13.2 Redundancies 18
3.13.3 Compliance with legal and contractual requirements 18
3.13.4 Information security reviews 18
Appendix 1 – Information Security (ISO 27001) certificate 19
Appendix 2 – Business Continuity (ISO 22301) certificate 20

2 Background, purpose and scope

The purpose of this Operational Security Plan is to outline the policies and controls that are in place to ensure ongoing confidentiality, integrity and availability of confidential data stored, transmitted and/or processed by the Coordinate My Care solution.

InterSystems' hosted and managed services in the United Kingdom are certified to ISO 27001. The corresponding Statement of Applicability has no exclusions which means that all available security controls under ISO 27002 have been implemented and that these are externally audited on a regular basis to ensure they remain effective.

Rather than focusing on technical measures through which each control is implemented, and which may change over time, this document therefore focuses on the controls that are in place in order to ensure secure operation of the hosted and managed service provided to Coordinate My Care.

InterSystems' ongoing certification, as evidenced by the certificate included in Appendix 1, therefore provides independent evidence that the required controls continue to be in place to ensure security for operation of the Coordinate My Care solution.

3 Operational security objectives and controls

This section outlines the controls in place to ensure ongoing security for the Coordinate My Care solution.

Each sub-heading includes a control reference in brackets that maps to the corresponding ISO 27001 control as well as the corresponding details in the InterSystems Security Management System which contains details of how each control is implemented.

3.1 Information security policies (A5)

3.1.1 Management direction for information security

The objective is to provide management direction and support for information security to meet business requirements as well as relevant laws and regulations.

- A set of policies for information security is defined, approved by management, published and communicated to all InterSystems employees and relevant external parties.
- These policies are reviewed on a regular basis and when significant changes occur in order to ensure their continued suitability, adequacy and effectiveness.

3.2 Organization of information security (A6)

3.2.1 Internal organization

The objective is to establish a management framework to initiate and control the implementation and operation of information security within the organization.

- Information security responsibilities are clearly defined and allocated.
- Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's information assets.
- Appropriate contacts with relevant authorities are maintained.
- Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.
- Information security is addressed in project management.

3.2.2 Mobile devices and teleworking

The objective is to ensure the security of teleworking and use of mobile devices.

- A policy and supporting security measures are in place to manage the risks introduced by the use of mobile devices.
- A policy and supporting security measures are in place to protect information accessed, processed or stored from remote sites.

3.3 Human resource security (A7)

3.3.1 Prior to employment

The objective is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

- Background checks are carried out in accordance with relevant laws, regulations and ethics and are proportional to the business requirements, the classification of the information to be accessed, contractual obligations and the perceived risks associated with the role.
- Contractual agreements with employees and contractors clearly state each party's obligations with respect to information security.

3.3.2 During employment

The objective is to ensure that employees and contractors are aware of and fulfil their information security.

- InterSystems management requires all employees and contractors to apply information security in accordance with established policies and procedures of the organization.
- All employees of the organization and, where relevant, contractors have received appropriate awareness education and training relevant for their job function.
- There is a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

3.3.3 Termination and change of employment

The objective is to protect the organization's interests as part of the process of changing or terminating employment.

- Information security responsibilities and duties that remain valid after termination or change of employment are defined, communicated to the employee or contractor and enforced.

3.4 Asset management (A8)

3.4.1 Responsibility for assets

The objective is to identify organizational assets and define appropriate protection responsibilities.

- Assets associated with information and information processing facilities are identified and an inventory of these assets is drawn up and maintained.
- Assets maintained in the inventory are assigned to a responsible owner.
- Rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.
- All employees and external party users are required to return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

3.4.2 Information classification

The objective is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

- Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
- An appropriate set of procedures for information labelling has been developed and implemented in accordance with the information classification scheme.
- Procedures for handling information assets have been developed and implemented in accordance with the information classification scheme adopted by the organization.

3.4.3 Media handling

The objective is to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

- Procedures have been implemented for the management of removable media in accordance with the classification scheme.
- Media is disposed of securely when no longer required, using formal procedures.
- Media containing information is protected against unauthorized access, misuse or corruption during transportation.

3.5 Access control (A9)

3.5.1 Business requirements of access control

The objective is to limit access to information and information processing facilities.

- An access control policy is established, documented and reviewed based on business and information security requirements.
- Users are only be provided with access to the network and network services that they have been specifically authorized to use.

3.5.2 User access management

The objective is to ensure authorized user access and to prevent unauthorized access to systems and services.

- A formal user registration and de-registration process has been implemented to enable assignment of access rights.
- A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services.
- The allocation and use of privileged access rights is restricted and controlled.
- The allocation of secret authentication information is controlled through a formal management process.
- Information asset owners review users' access rights at regular intervals.
- The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.

3.5.3 User responsibilities

The objective is to make users accountable for safeguarding their authentication information.

- Users are required to follow clearly defined practices in the use of secret authentication information.

3.5.4 System and application access control

The objective is to prevent unauthorized access to systems and applications.

- Access to information and application system functions is restricted in accordance with the access control policy.
- Where required by the access control policy, access to systems and applications is controlled by a secure log-on procedure.
- Password management systems are interactive and ensure quality passwords.
- The use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.
- Access to program source code is restricted.

3.6 Cryptography (A10)

3.6.1 Cryptographic controls

The objective is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

- A policy on the use of cryptographic controls for protection of information has been developed and is implemented.
- A policy on the use, protection and lifetime of cryptographic keys is developed and implemented through the whole key lifecycle.

3.7 Physical and environmental security (A11)

3.7.1 Secure areas

The objective is to prevent unauthorized physical access, damage and interference to the InterSystems information and information processing facilities.

- Security perimeters are defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
- Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
- Physical security for offices, rooms and facilities are designed and applied.
- Physical protection against natural disasters, malicious attack or accidents are in place.
- Procedures for working in secure areas are in place.
- Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

3.7.2 Equipment

The objective is to prevent loss, damage, theft or compromise of assets and interruption to the InterSystems operations.

- Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
- Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.
- Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage.
- Equipment is correctly maintained to ensure its continued availability and integrity.
- Equipment, information or software may not be taken off-site without prior authorization.
- Security is applied to off-site information assets taking into account the different risks of working outside of InterSystems' normal premises.
- All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
- Users are required to ensure that unattended equipment has appropriate protection.
- A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.

3.8 Operations security (A12)

3.8.1 Operational procedures and responsibilities

The objective is to ensure correct and secure operations of information processing facilities.

- Operating procedures are documented as required and made available to all users who need them.
- Changes to the organization, business processes, information processing facilities and systems that affect information security are controlled.
- The use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
- Development, testing, and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.

3.8.2 Protection from malware

The objective is to ensure that information and information processing facilities are protected against malware.

- Detection, prevention and recovery controls to protect against malware is implemented, combined with appropriate user awareness.

3.8.3 Backup

The objective is to protect against loss of data.

- Backup copies of information, software and system images are taken and tested regularly in accordance with agreed backup policies.

3.8.4 Logging and monitoring

The objective is to record events and generate evidence.

- Event logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed.
- Logging facilities and log information are protected against tampering and unauthorized access.
- System administrator and system operator activities are logged and the logs protected and regularly reviewed.
- The clocks of all relevant information processing systems within an organization or security domain are synchronised to a single reference time source.

3.8.5 Control of operational software

The objective is to ensure the integrity of operational systems.

- Procedures are implemented to control the installation of software on operational systems.

3.8.6 Technical vulnerability management

The objective is to prevent exploitation of technical vulnerabilities.

- Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organization's exposure to such vulnerabilities is evaluated and the appropriate measures are taken in a timely manner to address the associated risk.
- Rules governing the installation of software by users have been established and implemented.

3.8.7 Information systems audit considerations

The objective is to minimise the impact of audit activities on operational systems.

- Audit requirements and activities involving verification of operational systems are carefully planned and agreed to minimise disruptions to business processes.

3.9 Communications security (A13)

3.9.1 Network security management

The objective is to ensure the protection of information in networks and its supporting information processing facilities.

- Networks are managed and controlled to protect information in systems and applications.
- Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced.
- Groups of information services, users and information systems are segregated on networks.

3.9.2 Information transfer

The objective is to maintain the security of information transferred within an organization and with any external entity.

- Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities.
- Agreements are in place to address the secure transfer of business information between the organization and external parties.
- Information involved in electronic messaging is appropriately protected.
- Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information are identified, regularly reviewed and documented.

3.10 System acquisition, development and maintenance (A14)

3.10.1 Security requirements of information systems

The objective is to ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

- Information security related requirements are included in the requirements for new information systems or enhancements to and specification existing information systems.
- Information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
- Information involved in application service transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

3.10.2 Security in development and support processes

The objective is to ensure that information security is designed and implemented within the development lifecycle of information systems.

- Rules for the development of software and systems are established and applied to developments within the organization.
- Changes to systems within the development lifecycle are controlled by the use of formal change control procedures.
- When operating platforms are changed, critical applications are reviewed and where appropriate tested to ensure there is no adverse impact on organizational operations or security.
- Modifications to software packages are discouraged, limited to necessary changes and all changes are strictly controlled.
- Principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts.
- Secure development environments for system development and integration efforts that cover the entire system development lifecycle, have been implemented.
- Outsourced system development activity is supervised and monitored.
- Testing of security functionality is carried out during development.
- Acceptance testing programs and related criteria are established for new information systems, upgrades and new versions.

3.10.3 Test data

The objective is to ensure the protection of data used for testing.

- Test data is selected carefully, protected and controlled.

3.11 Supplier relationships (A15)

3.11.1 Information security in supplier relationships

The objective is to ensure protection of information assets accessible by suppliers.

- Information security requirements for mitigating the risks associated with supplier's access to information assets are agreed with the supplier and documented.
- All relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components.
- Agreements with suppliers include requirements to address the information security risks associated with information and supply chain communications technology services and product supply chain.

3.11.2 Supplier service delivery management

The objective is to maintain an agreed level of information security and service delivery in line with supplier agreements.

- InterSystems regularly monitors, reviews and audits suppliers.
- Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

3.12 Information security incident management (A16)

3.12.1 Management of information security incidents and improvements

The objective is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

- Management responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents.
- Information security events are reported through appropriate security events management channels as quickly as possible.
- Employees and contractors using InterSystems' information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.
- Information security events are assessed in order to decide if they are to be classified as information security incidents.
- Information security incidents are responded to in accordance with the documented procedures.
- Knowledge gained from analysing and resolving information security incidents are used to reduce the likelihood or impact of future incidents.
- The organization has defined and applied procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

3.13 Information security aspects of business continuity management (A17)

3.13.1 Information security continuity

The objective is for information security continuity to be embedded in the organization's business continuity management systems.

- InterSystems has determined requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
- InterSystems has established, documented, implemented and continues to maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
- InterSystems verifies established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

3.13.2 Redundancies

The objective is to ensure availability of information processing facilities.

- Information processing facilities are implemented with redundancy sufficient to meet availability requirements.

3.13.3 Compliance with legal and contractual requirements

The objective is to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

- All relevant legislative statutory, regulatory, contractual requirements and InterSystems' approach to meet these requirements are explicitly identified, documented and kept up to date.
- Appropriate procedures are implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
- Records are protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legal, regulatory, contractual and business requirements.
- Privacy and protection of personally identifiable information are ensured as required in relevant legislation and regulation where applicable.
- Cryptographic controls are used in compliance with all relevant agreements, legislation and regulations.

3.13.4 Information security reviews

The objective is to ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

- InterSystems' approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures) are reviewed independently at planned intervals or when significant changes occur.
- Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
- Information systems are regularly reviewed for compliance with the organization's information security policies and standards.

Appendix 1 – Information Security (ISO 27001) certificate

CERTIFICATION EUROPE™

This is to certify that the

Information Security Management System

Of

InterSystems

At

InterSystems House, Tangier Lane, Eton, Windsor, Berkshire, SL4 6BB
Felstead House, 2-6 Frances Road, Windsor, Berkshire, SL4 3AA
Data Centre, Birmingham , Studley, B80 7BG
Data Centre, Coriander Avenue, London, E14 2AA
Holyrood Park House, 106 Holyrood Road, Edinburgh, EH8 8AS

Has been assessed by Certification Europe (UK) Ltd and deemed to comply with the requirements of

ISO 27001:2013

This certificate is valid for the activities specified below:

The sale, delivery and support of software systems, including all IT services from InterSystems UK & Ireland offices and services hosted at third-party data centres.

Certification to the standard is made under the Statement of Applicability (version 1.0) and Certification Europe has adjudged that the exclusions under this Statement do not compromise the integrity of the ISMS.

Certification of Registration remains the property of Certification Europe (UK) Ltd.
The validity of this Certificate is maintained on the condition that the Management System is assessed through an on-going surveillance programme and continues to adequately meet the requirements of the standard.
To verify this certificate validity please contact us at info@certificationeurope.co.uk

Date of Initial Certification: 20th April 2016

This Certificate is valid until: 19th April 2022

Chief Executive: Michael Brophy

Signature:

Chairman: Padraic A. White

Signature:

Client Registration No.: 2016/2270
Certificate Reference No.: B/2

Date of certificate issue: 1st July 2019

ISO 27001 CERTIFICATION EUROPE™

UKAS MANAGEMENT SYSTEMS 0219

Certification Europe (UK) Ltd Boundary House, Cricket Field Road, Uxbridge UB8 1QG, United Kingdom

Appendix 2 – Business Continuity (ISO 22301) certificate

CERTIFICATION EUROPE™

ORIGINAL DIGITAL COPY

This is to certify that the

Business Continuity Management System

Of

InterSystems

At

Tangier Lane, Eton, Windsor, Berkshire SL4 6BB England

Has been assessed by Certification Europe (UK) Ltd and deemed to comply with the requirements of

ISO 22301:2012

This certificate is valid for the activities specified below:

The Business Continuity Management System of InterSystems UKI supporting the sales, delivery and support of software systems and services to customers from InterSystems' united Kingdom and Ireland sites in accordance with the Service Catalogue and all related activities.

Certification of Registration remains the property of Certification Europe (UK) Ltd.
The validity of this Certificate is maintained on the condition that the Management System is assessed through an on-going surveillance programme and continues to adequately meet the requirements of the standard.
To verify this certificate validity please contact us at info@certificationeurope.co.uk

Date of Initial Certification: 26th April 2017 This Certificate is valid until: 30th October 2022

Chief Executive: Michael Brophy

Signature:

Client Registration No.: 2017/2496
Certificate Reference No.: A/2

Date of certificate issue: 4th May 2020

ISO 22301 CERTIFICATION EUROPE™

UKAS MANAGEMENT SYSTEMS 0219

Certification Europe (UK) Ltd Boundary House, Cricket Field Road, Uxbridge UB8 1QG, United Kingdom

InterSystems UK & Ireland

InterSystems House
70 Tangier Lane, Eton
Windsor, SL4 6BB
Tel: +44 (0)1753 855450

InterSystems.co.uk

InterSystems Corporation
World Headquarters

One Memorial Drive
Cambridge, MA 02142-1356
Tel: +1.617.621.0600

InterSystems.com