Contenido

[5 Information security policies 6](#_Toc143846844)

[5.1 Management direction for information security 6](#_Toc143846845)

[5.1.1 Policies for information security 6](#_Toc143846846)

[5.1.2 Review of the policies for information security 6](#_Toc143846847)

[6 Organization of information security 6](#_Toc143846848)

[6.1 Internal organization 6](#_Toc143846849)

[6.1.1 Information security roles and responsibilities 6](#_Toc143846850)

[6.1.2 Segregation of duties 6](#_Toc143846851)

[6.1.3 Contact with authorities 6](#_Toc143846852)

[6.1.4 Contact with special interest groups 6](#_Toc143846853)

[6.1.5 Information security in project management 6](#_Toc143846854)

[6.2 Mobile devices and teleworking 6](#_Toc143846855)

[6.2.1 Mobile device policy 6](#_Toc143846856)

[6.2.2 Teleworking 6](#_Toc143846857)

[7 Human resource security 6](#_Toc143846858)

[7.1 Prior to employment 6](#_Toc143846859)

[7.1.1 Screening 6](#_Toc143846860)

[7.1.2 Terms and conditions of employment 6](#_Toc143846861)

[7.2 During employment 6](#_Toc143846862)

[7.2.1 Management responsibilities 6](#_Toc143846863)

[7.2.2 Information security awareness, education and training 7](#_Toc143846864)

[7.2.3 Disciplinary process 7](#_Toc143846865)

[7.3 Termination and change of employment 7](#_Toc143846866)

[7.3.1 Termination or change of employment responsibilities 7](#_Toc143846867)

[8 Asset management 7](#_Toc143846868)

[8.1 Responsibility for assets 7](#_Toc143846869)

[8.1.1 Inventory of assets 7](#_Toc143846870)

[8.1.2 Ownership of assets 7](#_Toc143846871)

[8.1.3 Acceptable use of assets 7](#_Toc143846872)

[8.1.4 Return of assets 7](#_Toc143846873)

[8.2 Information classification 7](#_Toc143846874)

[8.2.1 Classification of information 7](#_Toc143846875)

[8.2.2 Labelling of Information 7](#_Toc143846876)

[8.2.3 Handling of assets 7](#_Toc143846877)

[8.3 Media handling 7](#_Toc143846878)

[8.3.1 Management of removable media 7](#_Toc143846879)

[8.3.2 Disposal of media 7](#_Toc143846880)

[8.3.3 Physical media transfer 8](#_Toc143846881)

[9 Access control 8](#_Toc143846882)

[9.1 Business requirements of access control 8](#_Toc143846883)

[9.1.1 Access control Policy 8](#_Toc143846884)

[9.1.2 Access to networks and network services 8](#_Toc143846885)

[9.2 User access management 8](#_Toc143846886)

[9.2.1 User registration and de-registration 8](#_Toc143846887)

[9.2.2 User access provisioning 8](#_Toc143846888)

[9.2.3 Management of privileged access rights 8](#_Toc143846889)

[9.2.4 Management of secret authentication information of users 8](#_Toc143846890)

[9.2.4 Management of secret authentication information of users 8](#_Toc143846891)

[9.2.5 Review of user access rights 8](#_Toc143846892)

[9.2.6 Removal or adjustment of access rights 8](#_Toc143846893)

[9.3 User responsibilities 8](#_Toc143846894)

[9.3.1 Use of secret authentication information 8](#_Toc143846895)

[9.4 System and application access control 9](#_Toc143846896)

[9.4.1 Information access restriction 9](#_Toc143846897)

[9.4.2 Secure log-on procedures 9](#_Toc143846898)

[9.4.3 Password management system 9](#_Toc143846899)

[9.4.4 Use of privileged utility programs 10](#_Toc143846900)

[9.4.5 Access control to program source code 10](#_Toc143846901)

[10 Cryptography 10](#_Toc143846902)

[10.1 Cryptographic controls 10](#_Toc143846903)

[10.1.1 Policy on the use of cryptographic controls 10](#_Toc143846904)

[10.1.2 Key management 10](#_Toc143846905)

[11 Physical and environmental security 10](#_Toc143846906)

[11.1 Secure áreas 10](#_Toc143846907)

[11.1.1 Physical security perimeter 10](#_Toc143846908)

[11.1.2 Physical entry controls 10](#_Toc143846909)

[11.1.3 Securing offices, rooms and facilities 10](#_Toc143846910)

[11.1.4 Protecting against external and environmental threats 10](#_Toc143846911)

[11.1.5 Working in secure areas 10](#_Toc143846912)

[11.1.6 Delivery and loading áreas 10](#_Toc143846913)

[11.2 Equipment 11](#_Toc143846914)

[11.2.1 Equipment siting and protection 11](#_Toc143846915)

[11.2.2 Supporting utilities 11](#_Toc143846916)

[11.2.3 Cabling security 11](#_Toc143846917)

[11.2.4 Equipment maintenance 11](#_Toc143846918)

[11.2.5 Removal of assets 11](#_Toc143846919)

[11.2.6 Security of equipment and assets off-premises 11](#_Toc143846920)

[11.2.7 Secure disposal or reuse of equipment 11](#_Toc143846921)

[11.2.8 Unattended user equipment 11](#_Toc143846922)

[11.2.9 Clear desk and clear screen policy 11](#_Toc143846923)

[12 Operations security 11](#_Toc143846924)

[12.1 Operational procedures and responsibilities 11](#_Toc143846925)

[12.1.1 Documented operating procedures 11](#_Toc143846926)

[12.1.2 Change management 11](#_Toc143846927)

[12.1.3 Capacity management 11](#_Toc143846928)

[12.1.4 Separation of development, testing and operational environments 11](#_Toc143846929)

[12.2 Protection from malware 11](#_Toc143846930)

[12.2.1 Controls against malware 11](#_Toc143846931)

[12.3 Backup 12](#_Toc143846932)

[12.3.1 Information backup 12](#_Toc143846933)

[12.4 Logging and monitoring 12](#_Toc143846934)

[12.4.1 Event logging 12](#_Toc143846935)

[12.4.2 Protection of log Information 13](#_Toc143846936)

[12.4.3 Administrator and operator logs 13](#_Toc143846937)

[12.4.4 Clock synchronization 13](#_Toc143846938)

[12.5 Control of operational software 13](#_Toc143846939)

[12.5.1 Installation of software on operational systems 13](#_Toc143846940)

[12.6 Technical vulnerability management 13](#_Toc143846941)

[12.6.1 Management of technical vulnerabilities 13](#_Toc143846942)

[12.6.2 Restrictions on software installation 13](#_Toc143846943)

[12.7 Information systems audit considerations 13](#_Toc143846944)

[12.7.1 Information systems audit controls 13](#_Toc143846945)

[13 Communications security 13](#_Toc143846946)

[13.1 Network security management 13](#_Toc143846947)

[13.1.1 Network controls 13](#_Toc143846948)

[13.1.2 Security of network services 13](#_Toc143846949)

[13.1.3 Segregation in networks 14](#_Toc143846950)

[13.2 Information transfer 14](#_Toc143846951)

[13.2.1 Information transfer policies and procedures 14](#_Toc143846952)

[13.2.2 Agreements on information transfer 14](#_Toc143846953)

[13.2.3 Electronic messaging 14](#_Toc143846954)

[13.2.4 Confidentiality or non-disclosure agreements 14](#_Toc143846955)

[14 System acquisition, development and maintenance 14](#_Toc143846956)

[14.1 Security requirements of information systems 14](#_Toc143846957)

[14.1.1 Information security requirements analysis and specification 14](#_Toc143846958)

[14.1.2 Securing application services on public networks 14](#_Toc143846959)

[14.1.3 Protecting application services transactions 14](#_Toc143846960)

[14.2 Security in development and support processes 14](#_Toc143846961)

[14.2.1 Secure development policy 14](#_Toc143846962)

[14.2.2 System change control procedures 14](#_Toc143846963)

[14.2.3 Technical review of applications after operating platform changes 14](#_Toc143846964)

[14.2.4 Restrictions on changes to software packages 14](#_Toc143846965)

[14.2.5 Secure system engineering principles 14](#_Toc143846966)

[14.2.6 Secure development environment 14](#_Toc143846967)

[14.2.7 Outsourced development 14](#_Toc143846968)

[14.2.8 System security testing 15](#_Toc143846969)

[14.2.9 System acceptance testing 15](#_Toc143846970)

[14.3 Test data 15](#_Toc143846971)

[14.3.1 Protection of test data 15](#_Toc143846972)

[15 Supplier relationships 15](#_Toc143846973)

[15.1 Information security in supplier relationships 15](#_Toc143846974)

[15.1.1 Information security policy for supplier relationships 15](#_Toc143846975)

[15.1.2 Addressing security within supplier agreements 15](#_Toc143846976)

[15.1.3 Information and communication technology supply chain 15](#_Toc143846977)

[15.2 Supplier service delivery management 15](#_Toc143846978)

[15.2.1 Monitoring and review of supplier services 15](#_Toc143846979)

[15.2.2 Managing changes to supplier services 15](#_Toc143846980)

[16 Information security incident management 15](#_Toc143846981)

[16.1 Management of information security incidents and improvements 15](#_Toc143846982)

[16.1.1 Responsibilities and procedures 15](#_Toc143846983)

[16.1.2 Reporting information security events 15](#_Toc143846984)

[16.1.3 Reporting information security weaknesses 15](#_Toc143846985)

[16.1.4 Assessment of and decision on information security events 15](#_Toc143846986)

[16.1.5 Response to information security incidents 15](#_Toc143846987)

[16.1.6 Learning from information security incidents 16](#_Toc143846988)

[16.1.7 Collection of evidence 16](#_Toc143846989)

[17 Information security aspects of business continuity management 16](#_Toc143846990)

[17.1 Information security continuity 16](#_Toc143846991)

[17.1.1 Planning information security continuity 16](#_Toc143846992)

[17.1.2 Implementing information security continuity 16](#_Toc143846993)

[17.1.3 Verify, review and evaluate information security continuity 16](#_Toc143846994)

[17.2 Redundancies 16](#_Toc143846995)

[17.2.1 Availability of information processing facilities 16](#_Toc143846996)

[18 Compliance 16](#_Toc143846997)

[18.1 Compliance with legal and contractual requirements 16](#_Toc143846998)

[18.1.1 Identification of applicable legislation and contractual requirements 16](#_Toc143846999)

[18.1.2 Intellectual property rights 16](#_Toc143847000)

[18.1.3 Protection of records 16](#_Toc143847001)

[18.1.4 Privacy and protection of personally identifiable information 16](#_Toc143847002)

[18.1.5 Regulation of cryptographic controls 16](#_Toc143847003)

[18.2 Information security reviews 16](#_Toc143847004)

[18.2.1 Independent review of information security 16](#_Toc143847005)

[18.2.2 Compliance with security policies and standards 16](#_Toc143847006)

[18.2.3 Technical compliance review 17](#_Toc143847007)

# 5 Information security policies

## 5.1 Management direction for information security

### 5.1.1 Policies for information security

Does not apply.

### 5.1.2 Review of the policies for information security

Does not apply.

# 6 Organization of information security

## 6.1 Internal organization

### 6.1.1 Information security roles and responsibilities

Does not apply.

### 6.1.2 Segregation of duties

Does not apply.

### 6.1.3 Contact with authorities

Does not apply

### 6.1.4 Contact with special interest groups

Does not apply

### 6.1.5 Information security in project management

Does not apply

## 6.2 Mobile devices and teleworking

### 6.2.1 Mobile device policy

Does not apply

### 6.2.2 Teleworking

Does not apply

# 7 Human resource security

## 7.1 Prior to employment

### 7.1.1 Screening

Does not apply

### 7.1.2 Terms and conditions of employment

Does not apply

## 7.2 During employment

### 7.2.1 Management responsibilities

Does not apply

### 7.2.2 Information security awareness, education and training

Does not apply

### 7.2.3 Disciplinary process

Does not apply

## 7.3 Termination and change of employment

### 7.3.1 Termination or change of employment responsibilities

Does not apply

# 8 Asset management

## 8.1 Responsibility for assets

### 8.1.1 Inventory of assets

Does not apply

### 8.1.2 Ownership of assets

Does not apply

### 8.1.3 Acceptable use of assets

Does not apply

### 8.1.4 Return of assets

Does not apply

## 8.2 Information classification

### 8.2.1 Classification of information

Does not apply

### 8.2.2 Labelling of Information

All health information systems processing personal health information should inform users of the confidentiality of personal health information accessible from the system (e.g. at start-up or log-in) and should label hardcopy output as confidential when it contains personal health information.

### 8.2.3 Handling of assets

Does not apply

## 8.3 Media handling

### 8.3.1 Management of removable media

Does not apply

### 8.3.2 Disposal of media

Does not apply

### 8.3.3 Physical media transfer

Does not apply

# 9 Access control

## 9.1 Business requirements of access control

### 9.1.1 Access control Policy

Does not apply

### 9.1.2 Access to networks and network services

Does not apply

## 9.2 User access management

### 9.2.1 User registration and de-registration

Access to health information systems that process personal health information shall be subject to a formal user registration process. User registration procedures shall ensure that the level of authentication required of claimed user identity is consistent with the level(s) of access that will become available to the user.

### 9.2.2 User access provisioning

Does not apply

### 9.2.3 Management of privileged access rights

1. Health information systems should associate users (including health professionals, supporting staff and others) with the records of subjects of care and allow future access based on this association.

2. Systems containing personal health information should support role-based access control capable of mapping each user to one or more roles and each role to one or more system functions.

3. A user of a health information system containing personal health information shall access its services in a single role.

### 9.2.4 Management of secret authentication information of users

Does not apply

### 9.2.4 Management of secret authentication information of users

Does not apply

### 9.2.5 Review of user access rights

Does not apply

### 9.2.6 Removal or adjustment of access rights

Does not apply

## 9.3 User responsibilities

### 9.3.1 Use of secret authentication information

Does not apply

## 9.4 System and application access control

### 9.4.1 Information access restriction

Health information systems processing personal health information shall authenticate users and should do so by means of authentication involving at least two factors.

Access to information and application system functions related to the processing personal health information should be isolated from (and separate to) access to information processing infrastructure that is unrelated to the processing of personal health information.

### 9.4.2 Secure log-on procedures

ISO/IEC 27002:2013, 9.4.2 applies. Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.

A good log-on procedure should:

1. not display system or application identifiers until the log-on process has been successfully completed;
2. display a general notice warning that the computer should only be accessed by authorized users;
3. not provide help messages during the log-on procedure that would aid an unauthorized user;
4. validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;
5. protect against brute force log-on attempts;
6. log unsuccessful and successful attempts;
7. raise a security event if a potential attempted or successful breach of log-on controls is detected;
8. display the following information on completion of a successful log-on:

1) date and time of the previous successful log-on;

2) details of any unsuccessful log-on attempts since the last successful log-on;

1. not display a password being entered;
2. not transmit passwords in clear text over a network;
3. terminate inactive sessions after a defined period of inactivity, especially in high-risk locations such as public or external areas outside the organization's security management or on mobile devices;
4. restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

### 9.4.3 Password management system

1. Does not apply

### 9.4.4 Use of privileged utility programs

Does not apply

### 9.4.5 Access control to program source code

Does not apply

# 10 Cryptography

## 10.1 Cryptographic controls

### 10.1.1 Policy on the use of cryptographic controls

Does not apply

### 10.1.2 Key management

Does not apply

# 11 Physical and environmental security

## 11.1 Secure areas

### 11.1.1 Physical security perimeter

Does not apply

### 11.1.2 Physical entry controls

Does not apply

### 11.1.3 Securing offices, rooms and facilities

Does not apply

### 11.1.4 Protecting against external and environmental threats

Does not apply

### 11.1.5 Working in secure areas

Does not apply

### 11.1.6 Delivery and loading areas

Does not apply

## 11.2 Equipment

### 11.2.1 Equipment siting and protection

Does not apply

### 11.2.2 Supporting utilities

Does not apply

### 11.2.3 Cabling security

Does not apply

### 11.2.4 Equipment maintenance

Does not apply

### 11.2.5 Removal of assets

Does not apply

### 11.2.6 Security of equipment and assets off-premises

Does not apply

### 11.2.7 Secure disposal or reuse of equipment

Does not apply

### 11.2.8 Unattended user equipment

Does not apply

### 11.2.9 Clear desk and clear screen policy

Does not apply

# 12 Operations security

## 12.1 Operational procedures and responsibilities

### 12.1.1 Documented operating procedures

Does not apply

### 12.1.2 Change management

Does not apply

### 12.1.3 Capacity management

Does not apply

### 12.1.4 Separation of development, testing and operational environments

Does not apply

## 12.2 Protection from malware

### 12.2.1 Controls against malware

Does not apply

## 12.3 Backup

### 12.3.1 Information backup

Does not apply

## 12.4 Logging and monitoring

### 12.4.1 Event logging

Control

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Event logs should include, when relevant:

1. user IDs;
2. system activities;
3. dates, times and details of key events, e.g. log-on and log-off;
4. device identity or location if possible and system identifier;
5. records of successful and rejected system access attempts;
6. records of successful and rejected data and other resource access attempts;
7. changes to system configuration;
8. use of privileges;
9. use of system utilities and applications;
10. files accessed and the kind of access;
11. network addresses and protocols;
12. alarms raised by the access control system;
13. activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems;
14. records of transactions executed by users in applications.

Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

In addition to following the guidance given by ISO/IEC 27002, health information systems processing personal health information should create a secure audit record each time a user accesses, creates, updates or archives personal health information via the system. The audit log should uniquely identify the user, uniquely identify the data subject (i.e. the subject of care), identify the function performed by the user (record creation, access, update, etc.), and note the time and date at which the function was performed.

When personal health information is updated, a record of the former content of the data and the associated audit record (i.e. who entered the data on what date) should be retained.

Messaging systems used to transmit messages containing personal health information should keep a log of message transmissions (such a log should contain the time, date, origin and destination of the message, but not its content).

The organization should carefully assess and determine the retention period for these audit logs, with particular reference to clinical professional standards and legal obligations, in order to enable

investigations to be carried out when necessary and to provide evidence of misuse where necessary.

The health information system’s audit logging facility should be operational at all times while the health information system being audited is available for use.

Health information systems containing personal health information should be provided with facilities for analyzing logs and audit trails that:

1. allow the identification of all system users who have accessed or modified a given subject of care’s record(s) over a given period of time;
2. allow the identification of all subjects of care whose records have been accessed or modified by a given system user over a given period of time.

### 12.4.2 Protection of log Information

Audit records shall be secure and tamper-proof. Access to system audit tools and audit trails shall be safeguarded to prevent misuse or compromise.

### 12.4.3 Administrator and operator logs

Does not apply

### 12.4.4 Clock synchronization

Does not apply

## 12.5 Control of operational software

### 12.5.1 Installation of software on operational systems

Does not apply

## 12.6 Technical vulnerability management

### 12.6.1 Management of technical vulnerabilities

Does not apply

### 12.6.2 Restrictions on software installation

Does not apply

## 12.7 Information systems audit considerations

### 12.7.1 Information systems audit controls

Does not apply

# 13 Communications security

## 13.1 Network security management

### 13.1.1 Network controls

Does not apply

### 13.1.2 Security of network services

Does not apply

### 13.1.3 Segregation in networks

Does not apply

## 13.2 Information transfer

### 13.2.1 Information transfer policies and procedures

Does not apply

### 13.2.2 Agreements on information transfer

Does not apply

### 13.2.3 Electronic messaging

Does not apply

### 13.2.4 Confidentiality or non-disclosure agreements

Does not apply

# 14 System acquisition, development and maintenance

## 14.1 Security requirements of information systems

### 14.1.1 Information security requirements analysis and specification

Does not apply

### 14.1.2 Securing application services on public networks

Does not apply

### 14.1.3 Protecting application services transactions

Does not apply

## 14.2 Security in development and support processes

### 14.2.1 Secure development policy

Does not apply

### 14.2.2 System change control procedures

Does not apply

### 14.2.3 Technical review of applications after operating platform changes

Does not apply

### 14.2.4 Restrictions on changes to software packages

Does not apply

### 14.2.5 Secure system engineering principles

Does not apply

### 14.2.6 Secure development environment

Does not apply

### 14.2.7 Outsourced development

Does not apply.

### 14.2.8 System security testing

Does not apply.

### 14.2.9 System acceptance testing

Does not apply.

## 14.3 Test data

### 14.3.1 Protection of test data

Does not apply

# 15 Supplier relationships

## 15.1 Information security in supplier relationships

### 15.1.1 Information security policy for supplier relationships

Does not apply

### 15.1.2 Addressing security within supplier agreements

Does not apply

### 15.1.3 Information and communication technology supply chain

Does not apply

## 15.2 Supplier service delivery management

### 15.2.1 Monitoring and review of supplier services

Does not apply

### 15.2.2 Managing changes to supplier services

Does not apply

# 16 Information security incident management

## 16.1 Management of information security incidents and improvements

### 16.1.1 Responsibilities and procedures

Does not apply

### 16.1.2 Reporting information security events

Does not apply

### 16.1.3 Reporting information security weaknesses

Does not apply

### 16.1.4 Assessment of and decision on information security events

Does not apply

### 16.1.5 Response to information security incidents

Does not apply

### 16.1.6 Learning from information security incidents

Does not apply

### 16.1.7 Collection of evidence

Does not apply

# 17 Information security aspects of business continuity management

## 17.1 Information security continuity

### 17.1.1 Planning information security continuity

Does not apply

### 17.1.2 Implementing information security continuity

Does not apply

### 17.1.3 Verify, review and evaluate information security continuity

Does not apply

## 17.2 Redundancies

### 17.2.1 Availability of information processing facilities

Does not apply

# 18 Compliance

## 18.1 Compliance with legal and contractual requirements

### 18.1.1 Identification of applicable legislation and contractual requirements

Does not apply

### 18.1.2 Intellectual property rights

Does not apply

### 18.1.3 Protection of records

Does not apply

### 18.1.4 Privacy and protection of personally identifiable information

Does not apply

### 18.1.5 Regulation of cryptographic controls

Does not apply

## 18.2 Information security reviews

### 18.2.1 Independent review of information security

Does not apply

### 18.2.2 Compliance with security policies and standards

Does not apply

### 18.2.3 Technical compliance review

Does not apply