Security Controls (Req/Rec)

epSOS baseline security catalog: Requirements and Recommendations

Report Description: This profile of ISO 27002 is tailored for the NCP of the epSOS large scape pilot.
It includes only those controls that were classified as required or recommended.

Field descriptions:
ID and title: from ISO 27002:2005
epSOS Reference: related to deliverables from WP 2.1, 3.7 etc.
Rel: Relevance (REQ: required, REC: recommended, TSE: to some extend; DIS: dispensible; N/A: not appicable
Status: edit status can be: draft, open, final, unknow + comment
Impl (implementation source): ISO if Implementation Guidance from ISO, otherwise an epSOS-specific Implementation is defined.
R/S (reason for selection): LR: legal reason, CO: contractual obligation, BR: business requirement, BP: best practice, ??: not decided
Description: objectives and controls from ISO 27002:2005
Other information: from ISO 27002:2005
Implementation: either ISO-default or epSOS-specific
Justification: epSOS-sepcific rationale for Implementation and reason for selection

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

5 Information security policy

A.5.1 Information security policy

A.5.1.1	Information security policy document	D3.7.2	REQ	final	epSOS	C

Description:
An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.

Edit Status:
D3.7.2/I (to be localized)

Other Information:
The information security policy might be a part of a general policy document. If the information security policy is distributed outside the organisation, care should be taken not to disclose sensitive information. Further information can be found in the ISO/IEC 13335-1:2004.

Implementation:
The epSOS security Policy document is D3.7.2/Section I.
Chapters 2.5 and 2.6 may be excluded, as they are covered by various other controls

D3.7.2-MS chapter 3.2 defines a framework for setting control objectives and controls, including the structure of risk assessment and risk management.

A.5.1.2	Review of the information security policy	REC	final	epSOS	C

Description:
The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

Implementation:
The security policy will be approved, implemented and periodically audited by epSOS partners represented by the PSB, through an independent party, e,g, through a contracted auditor.

6 Internal organization

A.6.1 Internal organization

A.6.1.1	Management commitment to information security	REC	final	ISO	BP

Description:
Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

Edit Status:
FWA or ISO27002 ??

Other Information:
Further information is contained in ISO/IEC 13335-1:2004.

Implementation Guidance:
Management should:
a) ensure that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes;
b) formulate, review, and approve information security policy;
c) review the effectiveness of the implementation of the information security policy;
d) provide clear direction and visible management support for security initiatives;
e) provide the resources needed for information security;
f) approve assignment of specific roles and responsibilities for information security across the organization;
g) initiate plans and programs to maintain information security awareness;
h) ensure that the implementation of information security controls is co-ordinated across the organization (see 6.1.2).
Management should identify the needs for internal or external specialist information security advice, and review and coordinate results of the advice throughout the organization.
Depending on the size of the organization, such responsibilities could be handled by a dedicated management forum or by an existing management body, such as the board of directors.

A.6.1.2	Information security co-ordination	REC	final	ISO	BP

Description:
Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.

Edit Status:
as per ISO27002

Implementation Guidance:

Typically, information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management. This activity should:
a) ensure that security activities are executed in compliance with the information security policy;
b) identify how to handle non-compliances;
c) approve methodologies and processes for information security, e.g. risk assessment, information classification;
d) identify significant threat changes and exposure of information and information processing facilities to threats;
e) assess the adequacy and co-ordinate the implementation of information security controls;
f) effectively promote information security education, training and awareness throughout the organization;
g) evaluate information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions in response to identified information security incidents.
If the organization does not use a separate cross-functional group, e.g. because such a group is not appropriate for the organization's size, the actions described above should be undertaken by another suitable management body or individual manager.

A.6.1.3	Allocation of Information security responsibilities	REC	final	ISO	BP

Description:
All information security responsibilities should be clearly defined

Edit Status:
as per ISO27002

Other Information:
In many organizations an information security manager will be appointed to take overall responsibility for the development and implementation of security and to support the identification of controls.
However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

Implementation Guidance:
Allocation of information security responsibilities should be done in accordance with the information security policy (see clause 4). Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly identified. This responsibility should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes, such as business continuity planning, should be clearly defined.
Individuals with allocated security responsibilities may delegate security tasks to others. Nevertheless they remain responsible and should determine that any delegated tasks have been correctly performed.
Areas for which individuals are responsible should be clearly stated; in particular the following should take place:
a) the assets and security processes associated with each particular system should be identified and clearly defined;
b) the entity responsible for each asset or security process should be assigned and the details of this responsibility should be documented (see also 7.1.2);
c) authorization levels should be clearly defined and documented./

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.6.1.4	Authorization process for information processing		REC	final	ISO	BP

Description:
A management authorization process for new information processing facilities should be defined and implemented.

Edit Status:
as per ISO27002

Implementation Guidance:
The following guidelines should be considered for the authorization process:
a) new facilities should have appropriate user management authorization, authorizing their purpose and use. Authorization should also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met;
b) where necessary, hardware and software should be checked to ensure that they are compatible with other system components;
c) the use of personal or privately owned information processing facilities, e.g. laptops, home-computers or hand-held devices, for processing business information, may introduce new vulnerabilities and necessary controls should be identified and implemented.

A.6.2 External parties

A.6.2.1	Identification of risks related to external parties		REC	final	epSOS	BP

Description:
The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

Edit Status:
need elaboration for PoC, services, vendors as per ISO27002

Other Information:
Information might be put at risk by external parties with inadequate security management. Controls should be identified and applied to administer external party access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements might be used.
Organizations may face risks associated with inter-organizational processes, management, and communication if a high degree of outsourcing is applied, or where there are several external parties involved.
The controls 6.2.2 and 6.2.3 cover different external party arrangements, e.g. including:
a) service providers, such as ISPs, network providers, telephone services, maintenance and support services;
b) managed security services;
c) customers;
d) outsourcing of facilities and/or operations, e.g. IT systems, data collection services, call centre operations;
e) management and business consultants, and auditors;
f) developers and suppliers, e.g. of software products and IT systems;
g) cleaning, catering, and other outsourced support services;

h) temporary personnel, student placement, and other casual short-term appointments.
Such agreements can help to reduce the risks associated with external parties.

Implementation:
The vendors delivering hardware, software and services to the NCP need to be identified and

Where there is a need to allow an external party access to the information processing facilities or information of an organization, following considerations should be taken into account:
a) if access to critical systems (NCP gateway, network infrastructure) is required;
b) the type of access:
1) physical access, e.g. to offices, computer rooms, filing cabinets;
2) logical access, e.g. to an organization's databases, information systems;
c) the controls necessary to protect information that is not intended to be accessible by external parties;
d) how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed;

Access by external parties to the organization's information should not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected by the agreement with the external party (see also 6.2.2 and 6.2.3).
It should be ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information processing facilities.

A.6.2.3	Addressing security in third party agreements	REC	final	ISO	BP

Description:
Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

Edit Status:
ISO profile

Other Information:
The security requirements related to customers accessing organizational assets can vary considerably depending on the information processing facilities and information being accessed. These security requirements can be addressed using customer agreements, which contain all identified risks and security requirements (see 6.2.1).
Agreements with external parties may also involve other parties. Agreements granting external party access should include allowance for designation of other eligible parties and conditions for their access and involvement.

Implementation Guidance:
The agreement should ensure that there is no misunderstanding between the organization and the third party. Organizations should satisfy themselves as to the indemnity of the third party.
Following parties of an NCP should be considered:

a) service providers, such as ISPs, network providers, telephone services, maintenance and support services;
b) managed security services;
d) outsourcing of facilities and/or operations, e.g. IT systems, data collection services, call centre operations;
e) management and business consultants, and auditors;
f) developers and suppliers of NCP gateway, audit repository, monitoring and other related software products and IT systems;
g) cleaning, catering, and other outsourced support services;
h) temporary personnel, student placement, and other casual short-term appointments.

The following terms should be considered for inclusion in the agreement in order to satisfy the identified security requirements (see 6.2.1):
a) the information security policy;
b) controls to ensure asset protection, including the relevant controls of this ISMS, and
1) controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the agreement;
2) confidentiality, integrity, availability, and any other relevant property (see 2.1.5) of the assets;
3) restrictions on copying and disclosing information, and using confidentiality agreements (see 6.1.5);
c) user and administrator training in methods, procedures, and security;
d) ensuring user awareness for information security responsibilities and issues;
e) provision for the transfer of personnel, where appropriate;
f) responsibilities regarding hardware and software installation and maintenance;
g) a clear reporting structure and agreed reporting formats;
h) a clear and specified process of change management;
i) access control policy, covering:
1) the different reasons, requirements, and benefits that make the access by the third party necessary;
2) permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
3) an authorization process for user access and privileges;
4) a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use;
5) a statement that all access that is not explicitly authorised is forbidden;
6) a process for revoking access rights or interrupting the connection between systems;
j) arrangements for reporting, notification, and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement;
k) a description of the product or service to be provided, and a description of the information to be made available along with its security classification (see 7.2.1);
l) the target level of service and unacceptable levels of service; m) the definition of verifiable performance criteria, their monitoring and reporting; n) the right to monitor, and revoke, any activity related to the organization’s assets;
o) the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;
p) the establishment of an escalation process for problem resolution;
q) service continuity requirements, including measures for availability and reliability, in accordance with an organization’s business priorities;
r) the respective liabilities of the parties to the agreement;
s) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries (see also 15.1);
t) ommited - covered by 6.1.5;

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
u) involvement of the third party with subcontractors, and the security controls these subcontractors need to implement; v) conditions for renegotiation/termination of agreements: (early termination, organizational change)						

7 Asset management

A.7.1 Responsibility for assets

A.7.1.1	Inventory of assets	REC	final	epSOS	BP

Description:
All assets should be clearly identified and an inventory of all important assets drawn up and maintained.

Edit Status:
as per ISO27002

Other Information:
There are many types of assets, including:
a) information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
b) software assets: application software, system software, development tools, and utilities;
c) physical assets: computer equipment, communications equipment, removable media, and other equipment;
d) services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;
e) people, and their qualifications, skills, and experience;
f) intangibles, such as reputation and image of the organization.
Inventories of assets help to ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons. The process of compiling an inventory of assets is an important prerequisite of risk management (see also Section 4).

Implementation:
The NCP Asset Inventory shall be compled considerung these topics:
a) Configuration and data for NCP gateway, audit repository and other systems
b) Contracts and agreements (with third parties), system documentation, operational procedures, recovery and fallback arrangements, audit trails, and archived information;
c) Software assets: Application software, system software, development tools, and utilities;
d) Physical assets: Computer equipment, communications equipment and other equipment;
d) Services: computing and communications services, server housing;
e) People, and their qualifications, skills, and experience;
f) Intangibles, such as reputation and image of the organization.
g) For key material see cryptographic controls

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.7.1.3	Acceptable use of assets		REC	final	epSOS	BP

Description:
Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.

Edit Status:
as per ISO27002

Implementation:
Employees, contractors and third party users using or having access to the organization’s assets may not use these for other purposes than within the organization's objectives, that is acting as NCP gateway. Use of assets for processing of private or otherwise unrelated data like eMails or web content is strictly prohibited.

8 Human resources security

A.8.1 Prior to employment

A.8.1.1	Roles and responsibilities	REC	final	epSOS	??

Description:
Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.

Edit Status:
set of roles may be defined in 3.8

Other Information:
Job descriptions can be used to document security roles and responsibilities. Security roles and responsibilities for individuals not engaged via the organization's employment process, e.g. engaged via a third party organization, should also be clearly defined and communicated.

Implementation:
CEO (executive level):
initialize and maintain information security managment and audit processes; sign security policy; assign other security roles

CISO (chief infosec officer):
- Act as the organization's representative with respect to inquiries from CIO, external auditors and partners regarding the organization's security strategy and management.
- Act as the organization's representative when dealing with law enforcement agencies while pursuing the sources of network attacks and information theft by employees.
- Balance security needs with the organization's strategic business plan, identify risk factors, and determine solutions to both.
- Develop security controls and procedures that provide adequate business application protection without interfering with core business requirements.
- Plan and test responses to security breaches, including the possibility for discussion of the event with partners or the general public.
- Oversee the selection testing, deployment, and maintenance of information security products and services
- Oversee a staff of employees responsible for organization's information security

System administrator (NCP):
- setup and maintain systems
- technical vulnerability management (see A.12.6.1)
- key management
- accept and deploy software from third parties
- act as liason to a CERT (computer emergency response team)

System administrator (audit repository): as with sysadmin NCP

Network administrator
- establish and maintain network connectivity
- IPSec administration
- firewall adminsitration

Internal auditor

A.8.1.2	Screening	REC	final	epSOS	BP

Description:
Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Implementation:
Check of identity, qualification and reliabilty is common practice, but might need documentation.
(add references to existing controls ...)

A.8.1.3	Terms and conditions of employment	REC	final	epSOS	BP

Description:
As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.

Edit Status:
as per ISO27002

Other Information:
A code of conduct may be used to cover the employee's, contractor's or third party user's responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. The contractor or third party users may be associated with an external organization that may in turn be required to enter in contractual arrangements on behalf of the contracted individual.

Implementation:
The terms and conditions of employment should reflect the organization's security policy in addition to clarifying and stating:
a) that all employees, contractors and third party users who are given access to sensitive information should sign a confidentiality agreement prior to being given access to information processing facilities (see D3.8.1/7.2.4 - nondisclosure agreement for system administrators);
b) the employee's, contractor's and any other user's legal responsibilities regarding data protection legislation;
c) responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third party user (see also A.7.2.1 and A.10.7.3);
d) responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties;

e) responsibilities of the organization for the handling of personal information, including personal information created as a result of, or in the course of, employment with the organization (see also A.15.1.4);
f) responsibilities that are extended outside the organization's premises and outside normal working hours, e.g. in the case of remote support (see also A.9.2.5 and A.11.7.1);
g) actions to be taken if the employee, contractor or third party user disregards the organization's security requirements (see also A.8.2.3).
The organization should ensure that employees, contractors and third party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

A.8.2 During employment

A.8.2.1	Management responsibilities		REC	final	ISO	BP

Description:
Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization

Edit Status:
as per ISO27002

Other Information:
If employees, contractors and third party users are not made aware of their security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause less information security incidents.
Poor management may cause personnel to feel undervalued resulting in a negative security impact to the organization. For example, poor management may lead to security being neglected or potential misuse of the organization's assets.

Implementation Guidance:
Management responsibilities should include ensuring that employees, contractors and third party users:
a) are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems;
b) are provided with guidelines to state security expectations of their role within the organization;
c) are motivated to fulfill the security policies of the organization;
d) achieve a level of awareness on security relevant to their roles and responsibilities within the organization (see also 8.2.2);
e) conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working;
f) continue to have the appropriate skills and qualifications.

A.8.2.2	Information security awareness, education, and training	NCP-Requ#3.7.21	REC	final	ISO	BP

Description:
All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

Edit Status:
as per ISO27002

Other Information:
The security awareness, education, and training activities should be suitable and relevant to the person's role, responsibilities and skills, and should include information on known threats, who to contact for further security advice and the proper channels for reporting information security incidents (see also 13.1). Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role.

Implementation Guidance:
Awareness training should commence with a formal induction process designed to introduce the organization's security policies and expectations before access to information or services is granted.
Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process (see 8.2.3).

A.8.2.3	Disciplinary process	REC	final	ISO	BP

Description:
There should be a formal disciplinary process for employees who have committed a security breach.

Edit Status:
as per ISO27002

Other Information:
The disciplinary process should also be used as a deterrent to prevent employees, contractors and third party users in violating organizational security policies and procedures, and any other security breaches.

Implementation Guidance:
The disciplinary process should not be commenced without prior verification that a security breach has occurred (see also 13.2.3 for collection of evidence). The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

A.8.3 Termination or change of employment

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.8.3.1	Termination responsibilities		REC	final	ISO	BP

Description:
Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.

Edit Status:
as per ISO27002

Other Information:
The Human Resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the security aspects of the relevant procedures. In the case of a contractor, this termination responsibility process may be undertaken by an agency responsible for the contractor, and in case of an other user this might be handled by their organization.
It may be necessary to inform employees, customers, contractors, or third party users of changes to personnel and operating arrangements.

Implementation Guidance:
The communication of termination responsibilities should include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement (see 6.1.5), and the terms and conditions of employment (see 8.1.3) continuing for a defined period after the end of the employee's, contractor's or third party user's employment.
Responsibilities and duties still valid after termination of employment should be contained in employee's, contractor's or third party user's contracts.
Changes of responsibility or employment should be managed as the termination of the respective responsibility or employment, and the new responsibility or employment should be controlled as described in clause 8.1.

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.8.3.2	Return of assets		REC	final	ISO	BP

Description:
All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

Edit Status:
as per ISO27002

Implementation Guidance:
The termination process should be formalized to include the return of all previously issued software, corporate documents, and equipment. Other organizational assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media also need to be returned.
In cases where an employee, contractor or third party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment (see also 10.7.1).
In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.8.3.3	Removal of access rights		REQ	final	epSOS	LR

Description:
The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Edit Status:
data protection directive

Other Information:
In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee, contractor or third party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees, contractors and third party users involved to no longer share this information with the person departing.
In cases of management-initiated termination, disgruntled employees, contractors or third party users may deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning, they may be tempted to collect information for future use.

Implementation:
Upon termination Human Resources (HR) has to revoke any access rights of an individual to assets.
Upon changes of an employment access rights need to be reconsidered.
The access rights that should be removed or adapted include:
- physical and logical access,
- physical keys,
- identification cards,
- system accounts,
- mobile devices,
- subscriptions, and
- removal from any documentation that identifies them as a current member of the organization.

If a departing employee, contractor or third party user has known passwords for accounts remaining active, CISO has to arrange its change.
Access rights for information assets and information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:
a) whether the termination or change is initiated by the employee, contractor or third party user, or by management and the reason of termination;
b) the current responsibilities of the employee, contractor or any other user;
c) the value of the assets currently accessible.

9 Physical and environmental security

A.9.1 Secure areas

A.9.1.1	Physical security perimeter	REQ	final	ISO	C

Description:
Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

Edit Status:
as per ISO27002

Other Information:
Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection, where the failure of a single barrier does not mean that security is immediately compromised.
A secure area may be a lockable office, or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter.
Special consideration towards physical access security should be given to buildings where multiple organizations are housed.

Implementation Guidance:
The following guidelines should be considered and implemented where appropriate for physical security perimeters:
a) security perimeters should be clearly defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;
b) perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks etc; doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;
c) a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only;
d) physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;
e) all fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards; they should operate in accordance with local fire code in a failsafe manner;
f) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;
g) information processing facilities managed by the organization should be physically separated from those managed by third parties.

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.9.1.2	Physical entry controls		REC	final	ISO	BP

Description:
Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Edit Status:
as per ISO27002

Implementation Guidance:
The following guidelines should be considered:
a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures.
b) access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only; authentication controls, e.g. access control card plus PIN, should be used to authorize and validate all access; an audit trail of all access should be securely maintained;
c) all employees, contractors and third party users and all visitors should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;
d) third party support service personnel should be granted restricted access to secure areas or sensitive information processing facilities only when required; this access should be authorized and monitored;
e) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary (see 8.3.3).

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.9.1.3	Securing offices, rooms, and facilities		REQ	final	ISO	C

Description:
Physical security for offices, rooms, and facilities should be designed and applied

Edit Status:
as per ISO27002

Implementation Guidance:
The following guidelines should be considered to secure offices, rooms, and facilities:
a) account should be taken of relevant health and safety regulations and standards;
b) key facilities should be sited to avoid access by the public;
c) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities;
d) directories and internal telephone books identifying locations of sensitive information processing facilities should not be readily accessible by the public.

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.9.1.5	Working in secure areas		REQ	final	ISO	C

Description:
Physical protection and guidelines for working in secure areas should be designed and applied.

Edit Status:
as per ISO27002

Implementation Guidance:
The following guidelines should be considered:
a) personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis;
b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;
c) vacant secure areas should be physically locked and periodically checked;
d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized;
The arrangements for working in secure areas include controls for the employees, contractors and third party users working in the secure area, as well as other third party activities taking place there.

A.9.2 equipment security

A.9.2.1	Equipment siting and protection	REQ	final	epSOS	C

Description:
Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Edit Status:
as per ISO27002

Implementation:
Equipment siting and protection guideline:
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.
a) equipment should be sited to minimize unnecessary access into work areas;
b) information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access;
c) items requiring special protection should be isolated to reduce the general level of protection required;
d) controls should be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;
e) Anouncements to prohibit eating, drinking, and smoking in server facilities should be established;
f) temperature and humidity should be monitored;
g) protection against surge should be applied to all incoming power and communications lines;

Justification:
adapted to server equipment in business environment

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.9.2.3	Cabling security		REQ	final	ISO	C

Description:
Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

Edit Status:
as per ISO27002

Other Information:
Options to achieve continuity of power supplies include multiple feeds to avoid a single point of failure in the power supply.

Implementation Guidance:
The following guidelines for cabling security should be considered:
a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;
b) network cabling should be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas;
c) power cables should be segregated from communications cables to prevent interference;
d) clearly identifiable cable and equipment markings should be used to minimise handling errors, such as accidental patching of wrong network cables;
e) a documented patch list should be used to reduce the possibility of errors;
f) for sensitive or critical systems further controls to consider include:
1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;
2) use of alternative routings and/or transmission media providing appropriate security;
3) use of fibre optic cabling;
4) use of electromagnetic shielding to protect the cables;
5) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;
6) controlled access to patch panels and cable rooms;

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.9.2.4	Equipment maintenance		REQ	final	ISO	C

Description:
Equipment should be correctly maintained to ensure its continued availability and integrity.

Edit Status:
as per ISO27002

Other Information:
Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location.
More information about other aspects of protecting mobile equipment can be found in 11.7.1.

Implementation Guidance:

The following guidelines for equipment maintenance should be considered:
a) equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;
b) only authorized maintenance personnel should carry out repairs and service equipment;
c) records should be kept of all suspected or actual faults, and all preventive and corrective maintenance;
d) appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, sensitive information should be cleared from the equipment, or the maintenance personnel should be sufficiently cleared;
e) all requirements imposed by insurance policies should be complied with.

A.9.2.5	Security of equipment off-premises	REQ	final	epSOS	C

Description:
Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.

Edit Status:
as per ISO27002

Implementation:
The key risk factors for off-premises access are prohibited:
- the use of fixed or removeable storage (like hard disk or backup tape) without data encryption
- the access to internal networks (teleworking, remote maintenance)
If exceptions to the latter case are unavoidable, the scope of the ISMS must encompass these external systems

A.9.2.6	Secure disposal or re-use of equipment	REQ	final	epSOS	C

Description:
All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Edit Status:
as per ISO27002

Other Information:
Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.
Information can be compromised through careless disposal or re-use of equipment (see also 10.7.2).

Implementation:
Disposal of storage devices that may contain (have containerd) sensitive data must assure, that data cannot be recovered by means available to typical attackers.
Devices containing sensitive information should be either
a) physically destroyed or
b) the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S

using the standard delete or format function.
As sensitive data never should be stored unencrypted (see also A.12.3.1), option b) is deemed sufficient

10 Communications and operations management

A.10.1 Operational procedures and responsibilities

A.10.1.1	Documented operating procedures	REQ	final	ISO	C

Description:
Operating procedures should be documented, maintained, and made available to all users who need them.

Edit Status:
as per ISO27002

Implementation Guidance:
Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back- up, equipment maintenance, media handling, computer room and mail handling management, and safety.
The operating procedures should specify the instructions for the detailed execution of each job including:
a) processing and handling of information;
b) backup (see A.10.5);
c) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
d) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (see 11.5.4);
e) support contacts in the event of unexpected operational or technical difficulties;
f) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs (see A.10.7.2 and A.10.7.3);
g) system restart and recovery procedures for use in the event of system failure;
h) the management of audit-trail and system log information (see A.10.10).
Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools, and utilities.

A.10.1.2	Change management	REQ	final	ISO	C

Description:
Changes to information processing facilities and systems should be controlled.

Edit Status:
as per ISO27002

Other Information:
Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to

the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications (see also 12.5.1).
Changes to operational systems should only be made when there is a valid business reason to do so, such as an increase in the risk to the system. Updating systems with the latest versions of operating system or application is not always in the business interest as this could introduce more vulnerabilities and instability than the current version. There may also be a need for additional training, license costs, support, maintenance and administration overhead, and new hardware especially during migration.

Implementation Guidance:
Operational systems and application software should be subject to strict change management control.
In particular, the following items should be considered:
a) identification and recording of significant changes;
b) planning and testing of changes;
c) assessment of the potential impacts, including security impacts, of such changes;
d) formal approval procedure for proposed changes;
e) communication of change details to all relevant persons;
f) fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures.
When changes are made, an audit log containing all relevant information should be retained.

A.10.1.3	Segregation of duties	REQ	final	epSOS	C

Description:
Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Implementation:
Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.
Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.
Particular controls are:
a) Separation of operation from test and development (see A.10.1.4)
b) Nodes containing the audit trail repository must not be accessible to system administrators of the NCP gateway nodes.
c) Procurement and deployment of cryptographic keys used for the operational NPC nodes (TLS and WS-Security) should be separated from those used for IPSec.

A.10.1.4	Separation of development, test, and operational	REQ	final	epSOS	C

Description:
Development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system.

Edit Status:
as per ISO27002

Other Information:
Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment, or system failure. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.
Where development and test personnel have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code, which can cause serious operational problems.
Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, test, and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data (see also 12.4.2 for the protection of test data).

Implementation:
Separation between operational, test, and development environments is achieved by following rules:
a) personnel involved in development and test must not have administrative rights to production systems or cryptographic key material used for NCP operation.
b) development and operational software must run on different physical or virtual nodes and in different security domains;
c) transfer of software from development to operational status needs formal and documented hand-over, authorized by the CISO;
d) the test system environment should emulate the operational system environment as closely as possible;
e) sensitive data and key material must not be copied into the test system environment (see A.12.4.2).

Justification:
re c): removal of tools is quite ineffective and cumbersome for the sysadmin
re e) n/a - no end users on NCP

A.10.3 System planning and acceptance

A.10.3.2	System acceptance	REQ	final	ISO	C

Description:
Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.

Edit Status:
as per ISO27002

Other Information:
Acceptance may include a formal certification and accreditation process to verify that the security requirements have been properly addressed.

Implementation Guidance:
Service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the organization should plan the necessary transitions (of information, information processing facilities, and anything else that needs to be moved), and should ensure that security is maintained throughout the transition period.
The organization should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see A.14.1).

A.10.4 Protection against malicious and mobile code

A.10.4.1	Controls against malicious code	REQ	final	epSOS	C

Description:
Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

Edit Status:
as per ISO27002

Other Information:
The use of two or more software products protecting against malicious code across the information processing environment from different vendors can improve the effectiveness of malicious code protection.
Software to protect against malicious code can be installed to provide automatic updates of definition files and scanning engines to ensure the protection is up to date. In addition, this software can be installed on every desktop to carry out automatic checks.
Care should be taken to protect against the introduction of malicious code during maintenance and emergency procedures, which may bypass normal malicious code protection controls.

Implementation:
Protection against malicious code should be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls. The following rules apply:
a) installation of software on servers and clients used for development, test and adminsitration needs to be authorized (see A.15.1.2);
b) files and software either from or via external networks, or on any other medium, should be taken from authentic sources; checksums and signatures must be verified if available;
c) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated;
d) installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the checks carried out should include:
1) checking any files on electronic or optical media, and files received over networks, for malicious code before use;
2) checking electronic mail attachments and downloads for malicious code before use; this check should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;
3) checking web pages for malicious code (on the client for encrypted traffic);
e) defining management procedures and responsibilities to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks (see A.13.1 and A.13.2);

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S

Justification:
rely on vendors for malware scanners, as NCP's focus is on server operation

A.10.4.2	Controls against mobile code		REQ	final	epSOS	C

Description:
Where the use of mobile code is authorized, the configuration should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.

Edit Status:
as per ISO27002

Other Information:
Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction. Mobile code is associated with a number of middleware services.
In addition to ensuring that mobile code does not contain malicious code, control of mobile code is essential to avoid unauthorised use or disruption of system, network, or application resources and other breaches of information security.

Implementation:
Mobile code is software code which transfers from one computer to another computer and then executes automatically.
It is prohibited to use any mobile code on server nodes.
For client workstations only signed plug-ins and applets from reliable sources may be used.

A.10.5 Back-up

A.10.5.1	Information back-up	NCP-Requ#3.7.30; NCP-	REQ	final	epSOS	C

Description:
Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Edit Status:
adopted from ISO27002;

Other Information:
Back up arrangements can be automated to ease the back-up and restore process. Such automated solutions should be sufficiently tested prior to implementation and at regular intervals.

Implementation:
Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.
The following items for information back up need be considered:
a) the minimum number of back-up levels is 3 for daily, monthly and yearly backups;
b) accurate and complete records of the back-up copies and documented restoration procedures should be produced;

c) yearly, monthly backups need to be full backups;
d) the back-ups should be stored in a fire section different from the original equipment;
e) additional off-premises backups need to be created in monthly and yearly intervals, and at major system changes, such as the significant changes in software, configuration or keys;
e) back-up information should be given an appropriate level of physical and environmental protection (see clause 9) consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the back-up site;
f) back-up media should be tested twice a year to ensure that they can be relied upon for emergency use when necessary;
g) restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery; at leat one a year and with major changes in the backup software.
h) back-ups must be protected by means of encryption.
For th NCP and audit repository nodes, the backup arrangements should cover all systems information, applications, and data necessary to recover the complete system in the event of a disaster.
The retention period is set to 3 years (see A.15.1.3) unless otherwise required by national regulation.

A.10.6 Network security management

A.10.6.1	Network controls	REQ	final	epSOS	C

Description:
Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Edit Status:
derived from ISO27002

Other Information:
Additional information on network security can be found in ISO/IEC 18028, Information technology – Security techniques – IT network security.

Implementation:
Network managers should implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. In particular, the following items should be considered:
a) operational responsibility for networks should be separated from computer operations where appropriate (see A.10.1.3);
b) responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established;
c) Network connectivity should be restricted to the specified epSOS roles NCP, HCP, NCP system administrator and auditor;
d) Access to service networks should be confined to the NCP's premises;
e) System administrators and auditors should use restriced networks (VPNs) for the access to the NCP and audit repository nodes, with acces to other networks turned off;
f) appropriate logging and monitoring should be applied to enable recording of security relevant actions on the network level.
g) Network media shall used wired infrastructure; the use of wireless media is discouraged.

Justification:
adapted to the needs of NCP operation

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.10.6.2	Security of network services		REQ	final	ISO	C

Description:
Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in- house or outsourced.

Edit Status:
as per ISO27002

Other Information:
Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.
Security features of network services could be:
a) technology applied for security of network services, such as authentication, encryption, and network connection controls;
b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;
c) procedures for the network service usage to restrict access to network services or applications, where necessary.

Implementation Guidance:
The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.
The security arrangements necessary for particular services, such as security features, service levels, and management requirements, should be identified.
The organization should ensure that network service providers implement these measures.

A.10.7 Media handling

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.10.7.1	Management of removable media		REQ	final	epSOS	C

Description:
There should be procedures in place for the management of removable media.

Edit Status:
as per ISO27002

Other Information:
Removable media include tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media.

Implementation:
Guidelines for the management of removable media like CD-ROM, USB-memory sticks, portable hard drives:
a) if no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable (see also A.9.2.6);

b) an audit trail needs to be kept for media containing critical data that is removed from the organization;
c) all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications;
d) any confidential data MUST be stored using strong encryption; either implied by the storage format (like PKCS#12), or with AES128 (using tools like openssl);
f) personal mobile devices like smart phones, iPods, cameras and the like must not be used to store confidential data.
g) media shall be labeld according to its classification level (see also A.10.7.3 - awareness and proper handling overrules secrecy)

A.10.7.3	Information handling procedures		REQ	final	epSOS	C

Description:
Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.

Edit Status:
derived from ISO27002

Other Information:
These procedures apply to information in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of facsimile machines and any other sensitive items, e.g. blank cheques, invoices.

Implementation:
Procedures should be drawn up for handling, processing, storing, and communicating information consistent with its classification (see 7.2). The following items should be considered:
a) All media should be handled and labeled according to its indicated classification level;
b) access restrictions to prevent access from unauthorized personnel (implemented by A.11.1.1);
c) maintenance of a formal record of the authorized recipients of data for critical meta data and audit trails;
d) keeping the distribution of data to a minimum;
e) clear marking of all copies of media for the attention of the authorized recipient;
f) review of distribution lists and lists of authorized recipients at regular intervals.

Justification:
removed redundancies

A. Monitoring

A.10.10.1	Audit logging	NCP-REQ 3.7.11-16,18,	REQ	final	epSOS	C

Description:
Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Other Information:

The audit logs may contain intrusive and confidential personal data. Appropriate privacy protection measures should be taken (see also 15.1.4). Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (see 10.1.3).

Implementation:
Audit trails regarding the epSOS business level functions are defined in D3.4.2/3.2.2, D3.4/4.5 and D3.7.2-S2/6. It also has to adhere to following Requirements and recommendations:

NCP-Req#3.7.11 (Accounting and Control): a NCP MUST have a mechanism to record every access request and disclosure of medical information and clinical data, together with the time and identity of the accessing User. Clinical data MUST NOT be included in accounted data. Accounting records MUST be maintained as long as the pilot project lasts, unless otherwise legally required.

NCP-Req#3.7.12 (Auditing): it MUST be ensured that each action which has an impact on security is recorded. If data to be recorded contain both medical and personal data, an anonymization or pseudo-anonymization process SHOULD be used if possible or reasonable. In any case the recorded data MUST not contain personal health care data, but can contain a unique identifier to a data object. Audit records MUST be maintained as long as the pilot project lasts, unless otherwise legally required.

NCP-Req#3.7.14 (Continuously Logging): logging on the NCP SHOULD be operational at all times. In case of failure, the NCP involved MUST inform all the other NCPs.

NCP-Req#3.7.15 (Securing Access to Audit/Account Logs): a NCP MUST secure the access to audit records to prevent misuse or compromise.

NCP-Req#3.7.16 (Logging Transactions): a secure audit record MUST be created each time a User asks to access medical information of a Patient or to send an e-prescription dispensation's notification.

NCP-Req#3.7.18 (Minimum Content of Accounting Logs): the logs SHOULD contain:
- the user ID of the accessing User;
- the role the User is exercising;
- the organisation of the accessing User (at least in those cases where an individual accesses information on behalf of more - than one organisation);
- the unique Patient ID;
- the function performed by the accessing User;
- the NCP-id of the Originator/Target;
- a time stamp including time zone used.

NCP-Req#3.7.19 (Reporting Every Access medical information, notifications included): it SHOULD be possible to identify all requests to access to any Patient's record(s) (dispensations and modifications included) over a given period of time according to different parameters (Users, Patients' records,...)

System audit logs regarding the operating system should include, when relevant:
a) userIDs;
b) dates, times, and details of key events, e.g. log-on and log-off, or start and stop of system services;
c) terminal identity or location if possible;
d) records of successful and rejected system access attempts;

e) records of successful and rejected data and other resource access attempts;
f) changes to system configuration;
g) use of privileges;
h) use of system utilities and applications;
i) files accessed and the kind of access;

Segregation of duties (see A.10.1.2.3) shall apply to both business level audit trail and system audit logs.
j) network addresses and protocols;
k) alarms raised by the access control system;
,l) activation and de-activation of protection systems, such as intrusion detection systems.

A.10.10.2	Monitoring system use	NCP-Requ#3.7.13	REQ	final	epSOS	C

Description:
Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.

Edit Status:
epSOS

Other Information:
Usage monitoring procedures are necessary to ensure that users are only performing activities that have been explicitly authorized.
A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of information security incidents are given in 13.1.1.

Implementation:
Monitoring to prevent the abuse of confidential data is required by NCP-Req#3.7.13 (fraud detection); An appropriate monitoring facility must be established, to trigger alarms if an unreasonable high number or invalid combination of requests is dedected.

Definition of what is an abuse shall be defined in the access control policy (see A.11.1.1)

A.10.10.3	Protection of log information	D.3.7.2-S2/6.7; NCP-	REQ	final	epSOS	LR

Description:
Logging facilities and log information should be protected against tampering and unauthorized access.

Edit Status:
as per ISO27002

Other Information:
System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security.

Implementation:
Controls should aim to protect against unauthorized changes and operational problems with the auditing and logging facility including:
a) alterations to the message types that are recorded;
b) log files being edited or deleted;
c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events;
d) segregation of duties as required by D3.7.2-S2/6.6 (see A.10.1.3);
e) audit logs need to be retained for evidence as specified in A.10.10.1

Justification:
extended to encompass both system logs and audit trails

A.10.10.4	Administrator and operator logs	REC	final	ISO	BP

Description:
System administrator and system operator activities should be logged.

Edit Status:
as per ISO27002

Other Information:
An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

Implementation Guidance:
Logs should include:
a) the time at which an event (success or failure) occurred;
b) information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken);
c) which account and which administrator or operator was involved;
d) which processes were involved.
System administrator and operator logs should be reviewed on a regular basis.

A.10.10.5	Fault logging	REC	final	ISO	BP

Description:
Faults should be logged, analysed, and appropriate action taken.

Edit Status:
as per ISO27002

Other Information:

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S

Logging of errors and faults can impact the performance of a system. Such logging should be enabled by competent personnel, and the level of logging required for individual systems should be determined by a risk assessment, taking performance degradation into account.

Implementation Guidance:
Faults reported by users or by system programs related to problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:
a) review of fault logs to ensure that faults have been satisfactorily resolved;
b) review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.
It should be ensured that error logging is enabled, if this system function is available.

A.10.10.6	Clock synchronization	D3.7.2-S2/1.3.3	REQ	final	epSOS	C

Description:
The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.

Edit Status:
as specified in epSOS

Other Information:
The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol can be used to keep all of the servers in synchronisation with the master clock.

Implementation:
Time synchronization is required by epSOS to keep drift below 1 second. See D3.4.2/4.2 for implementaiton details.

N10. Non-Repudiation

11 Access control

A.11.1 Business requirement for access control

A.11.1.1	Access control policy	D3-4	REQ	final	epSOS	C

Description:
An access control policy should be established, documented, and reviewed based on business and security requirements for access.

Other Information:
Care should be taken when specifying access control rules to consider:
a) differentiating between rules that must always be enforced and guidelines that are optional or conditional;
b) establishing rules based on the premise “Everything is generally forbidden unless expressly permitted” rather than the weaker rule “Everything is generally permitted unless expressly forbidden”;
c) changes in information labels (see 7.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;
d) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;
e) rules, which require specific approval before enactment, and those which do not.
Access control rules should be supported by formal procedures and clearly defined responsibilities (see, for example, 6.1.3, 11.3, 10.4.1, 11.6).

Implementation:
Access control policy (needs to be detailed by NCP)
Access controls are both logical and physical (see also section A.9) and these should be considered together.
Auxiliary systems (like administrative workstations) are not in the scope of this profile, but need to managed with and adequate protection level.

The policy should take account the business and system level users.
A) The business level policy has to include:
a) the epSOS actors as defined in D3.6.2 (3.1 epSOS LSP entities)
b) patient consent according to D3.6.2 (3.3)
c) than national policy (e.g. patient consent must be given in country of affiliation, prescriptions not valid if signed by nurse, or othe rlimitations due to national law)

B) The system level policy shoud take into account the following:
a) access control requirements of business transations as defined in D3.4 in the functional specification for each use case;
b) Default policy is to deny all access;
c) standard user access profiles for common job roles in the organization:
1) CIO
2) CISO
3) System administrator (operation/NCP)
4) System administrator (operation/audit repository, monitoring)

5) System administrator (test, development)
6) Network adminsitrator
7) Auditor
8) .....
d) requirements for formal authorization of access requests (see A.11.2.1);
e) requirements for periodic review of access controls (see A.11.2.4);
f) removal of access rights (see A.8.3.3).

Justification:
simplify for server-type system's needs

A.11.2 User access management

A.11.2.1	User registration	REC	final	ISO	BP

Description:
There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

Edit Status:
as per ISO27002

Other Information:
Consideration should be given to establish user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews (see 11.2.4) are easier managed at the level of such roles than at the level of particular rights.
Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or service agents (see also 6.1.5, 8.1.3 and 8.2.3).

Implementation Guidance:
The access control procedure for user registration and de-registration should include:
a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons, and should be approved and documented;
b) checking that the user has authorization from the system owner for the use of the information system or service; separate approval for access rights from management may also be appropriate;
c) checking that the level of access granted is appropriate to the business purpose (see 11.1) and is consistent with organizational security policy, e.g. it does not compromise segregation of duties (see 10.1.3);
d) giving users a written statement of their access rights;
e) requiring users to sign statements indicating that they understand the conditions of access;
f) ensuring service providers do not provide access until authorization procedures have been completed;
g) maintaining a formal record of all persons registered to use the service;
h) immediately removing or blocking access rights of users who have changed roles or jobs or left the organization;
i) periodically checking for, and removing or blocking, redundant user IDs and accounts (see 11.2.4);

j) ensuring that redundant user IDs are not issued to other users.

A.11.2.2	Privilege management	NCP-Requ#3.7.04	REQ	final	epSOS	C

Description:
The allocation and use of privileges should be restricted and controlled.

Edit Status:
as per ISO27002

Other Information:
Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems.

Implementation:
Privilege management is to be considered on application and system level.

For the application level refere to D3.4

For the system the allocation of privileges should be controlled through a formal authorization process. The following steps should be considered:
a) the access privileges associated with each system product, e.g. operating system, database management system and each system application, and the users to which they need to be allocated should be identified;
b) privileges should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (see A.11.1.1), i.e. the minimum requirement for their functional role only when needed;
c) an authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete;
d) the development and use of system routines should be promoted to avoid the need to grant privileges to users;
e) the development and use of programs which avoid the need to run with privileges should be promoted;
f) privileges should be assigned to a different user ID (or separated usage context) from those used for normal business use.

A.11.2.3	User password management	REC	final	epSOS	BP

Description:
The allocation of passwords should be controlled through a formal management process.

Edit Status:
as per ISO27002

Other Information:
Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization. Other technologies for user identification and authentication, such as biometrics, e.g. finger-print verification, signature

verification, and use of hardware tokens, e.g. smart cards, are available, and should be considered if appropriate.

Implementation:
Authentication by knowledge and possession is preferable over authentication by knowledge (password). (See A.11.4.2)
Authentication protocols over networks MUST be resistant against spoofing and MITM-attacks. E.g. ssh-connections should be established with keys that are distributed out-of-band.

If password are being used, following requirements should be fulfilled:
a) users should be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group; this signed statement could be included in the terms and conditions of employment (see A.8.1.3);
b) when users are required to maintain their own passwords they should be provided initially with a secure temporary password (see A.11.3.1), which they are forced to change immediately;
c) establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;
d) temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided;
e) temporary passwords should be unique to an individual and should not be guessable;
f) users should acknowledge receipt of passwords;
g) passwords should never be stored on computer systems in an unprotected form;
h) default vendor passwords should be altered following installation of systems or software.

A.11.2.4	Review of user access rights	REC	final	ISO	??

Description:
Management should review users' access rights at regular intervals using a formal process.

Edit Status:
as per ISO27002

Other Information:
It is necessary to regularly review users' access rights to maintain effective control over access to data and information services.

Implementation Guidance:
The review of access rights should consider the following guidelines:
a) users' access rights should be reviewed at regular intervals, e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment (see 11.2.1);
b) user access rights should be reviewed and re-allocated when moving from one employment to another within the same organization;
c) authorizations for special privileged access rights (see 11.2.2) should be reviewed at more frequent intervals, e.g. at a period of 3 months;
d) privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;
e) changes to privileged accounts should be logged for periodic review.

A.11.3 User responsibilities

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.11.3.1	Password use		REC	final	ISO	BP

Description:
Users should be required to follow good security practices in the selection and use of passwords.

Edit Status:
as per ISO27002

Other Information:
Management of the help desk system dealing with lost or forgotten passwords needs special care as this may also be a means of attack to the password system.

Implementation Guidance:
All users should be advised to:
a) keep passwords confidential;
b) avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;
c) change passwords whenever there is any indication of possible system or password compromise;
d) select quality passwords with sufficient minimum length which are:
1) easy to remember;
2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
4) free of consecutive identical, all-numeric or all-alphabetic characters;
e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;
f) change temporary passwords at the first log-on;
g) not include passwords in any automated log-on process, e.g. stored in a macro or function key;
h) not share individual user passwords;
i) not use the same password for business and non-business purposes.
If users need to access multiple services, systems or platforms, and are required to maintain multiple separate passwords, they should be advised that they may use a single, quality password (see d) above) for all services where the user is assured that a reasonable level of protection has been established for the storage of the password within each service, system or platform.

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.11.3.2	Unattended user equipment		REC	final	ISO	BP

Description:
Users should ensure that unattended equipment has appropriate protection.

Edit Status:
as per ISO27002

Other Information:

Equipment installed in user areas, e.g. workstations or file servers, may require specific protection from unauthorized access when left unattended for an extended period.

Implementation Guidance:
All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:
a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
b) log-off mainframe computers, servers, and office PCs when the session is finished (i.e. not just switch off the PC screen or terminal);
c) secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use (see also 11.3.3).

A.11.3.3	Clear desk and clear screen policy	REC	final	ISO	BP

Description:
A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

Edit Status:
as per ISO27002

Other Information:
A clear desk/clear screen policy reduces the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion. Consider the use of printers with pin code function, so the originators are the only ones who can get their print outs, and only when standing next to the printer.

Implementation Guidance:
The clear desk and clear screen policy should take into account the information classifications (see 7.2), legal and contractual requirements (see 15.1), and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:
a) sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;
b) computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;
c) incoming and outgoing mail points and unattended facsimile machines should be protected;
d) unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented;
e) documents containing sensitive or classified information should be removed from printers immediately.

A.11.4 Network access control

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.11.4.4	Remote diagnostic and configuration port protection		REC	final	epSOS	BP

Description:
Physical and logical access to diagnostic and configuration ports should be controlled.

Edit Status:
as per ISO27002

Other Information:
Many computer systems, network systems, and communication systems are installed with a remote diagnostic or configuration facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access.

Implementation:
Access to diagnostic and configuration functions have to be covered by third-party agreements, that extend the controls of this profile to the external party (see A.6.3.2). Part of that agreement must be the use of strong authentication (see A.11.4.2) or at least strong passwords (see also A.11.2.3 and A.11.3.1), network service security (see A.10.6.2) and controlled physical access (see A.9.1.2).

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.11.4.5	Segregation in networks		REQ	final	epSOS	BP

Description:
Groups of information services, users, and information systems should be segregated on networks.

Other Information:
Networks are increasingly being extended beyond traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorized access to existing information systems that use the network, some of which may require protection from other network users because of their sensitivity or criticality.

Implementation:
NCPs should define network connectivity per service. The defined connections are:
a) other epSOS NCPs, optionally via SOAP proxy
b) national epSOS participants (HCP)
c) audit repository and monitoring services
d) management network

Each connection implies specific firewall settings. Whether firewalls, network switches etc. are locally, dedicated or virtualized is to be defined, but IPSec-services should be on a separated device (see A.10.1.3 - segregation of duties).
The management network may be used to manage other systems, but should be restricted to system adminsitrators having at least the authentication quality and and other security restrictions that are required by this profile.

Justification:
D3.7.2-S2/5, best practice

A.11.5 Operating system access control

A.11.5.1	Secure log-on procedures	REC	final	epSOS	BP

Description:
Access to operating systems should be controlled by a secure log-on procedure.

Edit Status:
generalize from password-based to general authentication mechanism

Other Information:
If passwords are transmitted in clear text during the log-on session over a network, they may be captured by a network ‘sniffer’ program on the network.

Implementation:
This procedures apply primarily to password-based authentication; secure log-on procedures for other technologies need to be specified accordingly.

The procedure for logging into an operating system should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance. A good log-on procedure should:
a) not display system or application identifiers until the log-on process has been successfully completed;
b) display a general notice warning that the computer should only be accessed by authorized users;
c) not provide help messages during the log-on procedure that would aid an unauthorized user;
d) 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;
e) limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, and consider:
 1) recording unsuccessful and successful attempts;
 2) forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization;
 3) disconnecting data link connections;
 4) sending an alarm message to the system console if the maximum number of log-on attempts is reached;
 5) setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected;
f) limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on;
g) 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;
h) not display the password being entered or consider hiding the password characters by symbols;
i) not transmit passwords in clear text over a network.

Justification:
only for password-base authentication

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.11.5.2	User identification and authentication	NCP-Requ#3.7.1b	REQ	final	ISO	C

Description:
All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

Edit Status:
as per ISO27002

Other Information:
Passwords (see also 11.3.1 and 11.5.3) are a very common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user identification and authentication should be suitable to the sensitivity of the information to be accessed.
Objects such as memory tokens or smart cards that users possess can also be used for identification and authentication. Biometric authentication technologies that use the unique characteristics or attributes of an individual can also be used to authenticate the person's identity. A combination of technologies and mechanisms securely linked will result in stronger authentication.

Implementation Guidance:
This control should be applied for all types of users (including technical support personnel, operators, network administrators, system programmers, and database administrators).
User IDs should be used to trace activities to the responsible individual. Regular user activities should not be performed from privileged accounts.
In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented for such cases. Additional controls may be required to maintain accountability.
Generic IDs for use by an individual should only be allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g. read only access), or where there are other controls in place (e.g. password for a generic ID only issued to one staff at a time and logging such instance).
Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

A.11.5.3	Password management system		REC	final	ISO	BP

Description:
Systems for managing passwords should be interactive and should ensure quality passwords.

Edit Status:
as per ISO27002

Other Information:
Passwords are one of the principal means of validating a user's authority to access a computer service.
Some applications require user passwords to be assigned by an independent authority; in such cases, points b), d) and e) of the above guidance do not apply.
In most cases the passwords are selected and maintained by users. See section 11.3.1 for guidance on the use of passwords.

Implementation Guidance:
A password management system should:
a) enforce the use of individual user IDs and passwords to maintain accountability;
b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
c) enforce a choice of quality passwords (see 11.3.1);
d) enforce password changes (see 11.3.1);
e) force users to change temporary passwords at the first log-on (see 11.2.3);
f) maintain a record of previous user passwords and prevent re-use;
g) not display passwords on the screen when being entered;
h) store password files separately from application system data;
i) store and transmit passwords in protected (e.g. encrypted or hashed) form.

Justification:
relevant if passwords are being used to authenticate NCP staff

A.11.5.5	Session time-out	REC	final	epSOS	BP

Description:
Inactive sessions should shut down after a defined period of inactivity.

Edit Status:
as per ISO27002

Other Information:
This control is particularly important in high risk locations, which include public or external areas outside the organization's security management. The sessions should be shut down to prevent access by unauthorized persons and denial of service attacks.

Implementation:
Session timeouts of system level users should enforce re-authentication after 15 minutes of inactivity.

A.11.5.6	Limitation of connection time	REC	final	epSOS	BP

Description:
Restrictions on connection times should be used to provide additional security for high-risk applications.

Edit Status:
as per ISO27002

Other Information:
Limiting the period during which connections to computer services are allowed reduces the window of opportunity for unauthorized access. Limiting the duration of active sessions prevents users from holding sessions open to prevent re-authenticating.

Implementation:

Connection time for system level users must not exceed 10 hours for standard administrative accounts without reauthentication.

A. Sensitive system isolation

A.11.6.2	Sensitive system isolation	REC	final	epSOS	BP

Description:
Sensitive systems should have a dedicated (isolated) computing environment.

Other Information:
Some application systems are sufficiently sensitive to potential loss that they require special handling. The sensitivity may indicate that the application system:
a) should run on a dedicated computer; or
b) should only share resources with trusted applications systems. Isolation could be achieved using physical or logical methods (see also 11.4.5).

Implementation:
NCPs and audit repository should run on dedicated systems.

Justification:
The NCP and audit repository are dedicated systems; beyond that there is no subsystem processing sensitive data.

A.11.7 Mobile computing and teleworking

A.11.7.1	Mobile computing and communications	REC	final	epSOS	BP

Description:
A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

Edit Status:
see 11.7

Other Information:
Mobile network wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are
a) some wireless security protocols are immature and have known weaknesses;
b) information stored on mobile computers may not be backed-up because of limited network bandwidth and/or because mobile equipment may not be connected at the times when back-ups
are scheduled.

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S

Implementation:
NCPs should only be accessed from on-premises devices using wired network conenctions.

A.11.7.2	Teleworking		REC	final	epSOS	BP

Description:
A policy, operational plans and procedures should be developed and implemented for teleworking activities.

Edit Status:
see 11.7

Other Information:
Teleworking uses communications technology to enable personnel to work remotely from a fixed location outside of their organization.

Implementation:
Teleworking for system administrators is discouraged.

12 Correct processing in applications

A.12.2 Correct processing in applications

A.12.2.1	Input data validation	REC	final	epSOS	BP

Description:
Data input to applications should be validated to ensure that this data is correct and appropriate.

Edit Status:
as per ISO 27002

Other Information:
Automatic examination and validation of input data can be considered, where applicable, to reduce the risk of errors and to prevent standard attacks including buffer overflow and code injection.

Implementation:
epSOS testing is based on standard IHE-tests, and covered by WP 3.9. Parts of the NCP-gateway that need locally developed test cases should consider following ISO-27002-guidelines for input data validation:
Checks should be applied to the input of business transactions, standing data (e.g. names and addresses, credit limits, customer reference numbers), and parameter tables (e.g. sales prices, currency conversion rates, tax rates). The following guidelines should be considered:
a) dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
1) out-of-range values;
2) invalid characters in data fields;
3) missing or incomplete data;
4) exceeding upper and lower data volume limits;
5) unauthorized or inconsistent control data;
b) periodic review of the content of key fields or data files to confirm their validity and integrity;
c) inspecting hard-copy input documents for any unauthorized changes (all changes to input documents should be authorized);
d) procedures for responding to validation errors;
e) procedures for testing the plausibility of the input data;
f) defining the responsibilities of all personnel involved in the data input process;
g) creating a log of the activities involved in the data input process (see A.10.10.1).

A.12.2.2	Control of internal processing	REC	final	epSOS	BP

Description:
Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

Other Information:
Data that has been correctly entered can be corrupted by hardware errors, processing errors or through deliberate acts. The validation checks

required will depend on the nature of the application and the business impact of any corruption of data.

Implementation:
epSOS testing is based on standard IHE-tests, and covered by WP 3.9. Parts of the NCP-gateway that need locally developed test cases should consider following ISO-27002-guidelines for the design and implementation of applications to ensure that the risks of processing failures leading to a loss of integrity are minimized:
a) the use of add, modify, and delete functions to implement changes to data;
b) the procedures to prevent programs running in the wrong order or running after failure of prior processing (see also A.10.1.1);
c) the use of appropriate programs to recover from failures to ensure the correct processing of data;
d) protection against attacks using buffer overruns/overflows.
An appropriate checklist should be prepared, activities documented, and the results should be kept secure. Examples of checks that can be incorporated include the following:
a) session or batch controls, to reconcile data file balances after transaction updates;
b) balancing controls, to check opening balances against previous closing balances, namely:
1) run-to-run controls;
2) file update totals;
3) program-to-program controls;
c) validation of system-generated input data (see A.12.2.1);
d) checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers;
e) hash totals of records and files;
f) checks to ensure that application programs are run at the correct time;
g) checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved;
h) creating a log of the activities involved in the processing (see A.10.10.1).

A.12.2.3	Message integrity	REC	final	epSOS	C

Description:
Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.

Other Information:
Cryptographic techniques (see 12.3) can be used as an appropriate means of implementing message authentication.

Implementation:
epSOS message integrity in between NCPs is enforced using digital signatures on the SOAP message level (see D3.7.2-S2/Chapter 3 Data Integrity Security Service). Integrity between NCPs and HCP/HCO must also be enforced by appropriate means.

A.12.2.4	Output data validation	REC	final	epSOS	BP

Description:
Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the

circumstances.

Other Information:
Typically, systems and applications are constructed on the assumption that having undertaken appropriate validation, verification, and testing, the output will always be correct. However, this assumption is not always valid; i.e. systems that have been tested may still produce incorrect output under some circumstances.

Implementation:
epSOS testing is based on standard IHE-tests, and covered by WP 3.9. Parts of the NCP-gateway that need locally developed test cases should consider following ISO-27002-guidelines for 0utput validation:
a) plausibility checks to test whether the output data is reasonable;
b) reconciliation control counts to ensure processing of all data;
c) providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;
d) procedures for responding to output validation tests;
e) defining the responsibilities of all personnel involved in the data output process;
f) creating a log of activities in the data output validation process.

A.12.3 Cryptographic controls

A.12.3.1	Policy on the use of cryptographic controls	NCP-Requ#3.7.03a, 03b,	REQ	final	epSOS	C

Description:
A policy on the use of cryptographic controls for protection of information should be developed and implemented.

Edit Status:
need detailed implementation according to NCP-requ.

Other Information:
Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.
A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques, and to avoid inappropriate or incorrect use. When using digital signatures, consideration should be given to any relevant legislation, in particular legislation describing the conditions under which a digital signature is legally binding (see 15.1).
Specialist advice should be sought to identify the appropriate level of protection and to define suitable specifications that will provide the required protection and support the implementation of a secure key management system (see also 12.3.2).
ISO/IEC JTC1 SC27 has developed several standards related to cryptographic controls. Further information can also be found in IEEE P1363 and the OECD Guidelines on Cryptography.

Implementation:
Purpose

A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques, and to avoid inappropriate or incorrect use.

Assets to be protected and controls to be applied
The following enumeration shows assets and their appropriate control:
- Message: :signature
Transport (NCP web service, web portal): encryption, node authentication with NCP, HCP (required on epSOS and national levels)
- Network: IPSec encryption and network authentication (required on epSOS, recommended on national level)
- Configuration data: signature
- SAML assertions: signature
- Audit trail: segregation of operation; signature of single messages plus daily batches; (optional)
- Medical data for storage in NCP: no need in current project phase.
- NCP key material: physical security and organizational procedures

Responsibilities
1) CISO : for the implementation of the policy;
2) named system administrators: for the key management, including key generation (see also A.12.3.2);

Specifications for crypto-controls
- Trusted Node Infrastructure (D3.4 §4.1)
- epSOS Trust Service Lists (D3.4 §4.4)
- Message Signature (D3.4 §4.3.5.2)
- Cryptographic Keys and Algorithms (D3.4 §5.1)
- epSOS Certificate Profiles (D3.4 §5.4)

Root certificates
The acknowledgement of root certificates of other MS is handled according to the Commission's decision based on Directive 2006/123/EC. The EC publishes a document with a list of URLs pointing to the national Trust Lists; its location is
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
That XML-document references the national trust lists, like http://www.signatur.rtr.at/currenttsl.xml in case of Austria.
Participants can be from EU or EWR; Inclusion of other countries must be investigated.

Justification:
profiled for NCP

A.12.3.2	Key management	REQ	final	epSOS	BP

Description:
Key management should be in place to support the organization’s use of cryptographic techniques.

Other Information:
The management of cryptographic keys is essential to the effective use of cryptographic techniques. ISO/IEC 11770 provides further information on key management. The two types of cryptographic techniques are:

a) secret key techniques, where two or more parties share the same key and this key is used both to encrypt and decrypt information; this key has to be kept secret since anyone having access to the key is able to decrypt all information being encrypted with that key, or to introduce unauthorized information using the key;
b) public key techniques, where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which has to be kept secret); public key techniques can be used for encryption and to produce digital signatures (see also ISO/IEC 9796 and ISO/IEC 14888).
There is a threat of forging a digital signature by replacing a user's public key. This problem is addressed by the use of a public key certificate.
Cryptographic techniques can also be used to protect cryptographic keys. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information may need to be made available in an unencrypted form as evidence in a court case.

Implementation:
Trust bootstrapping shall be conforming to the epSOS Circle of Trust setup procedures

Cryptographic keys are stored on the NCP (and routers for IPSec) and accessible to system tasks without human intervention. Without that measure operation (outside a pilot) is not feasible, as recovery would be very slow. Therefore the nodes containing cryptographic material need to be protected - that is the objective of this profile.

Key management should:
a) obtain public key certificates from reliable CAs (see D3.7.2-S2/8) and uderstand the certificate policy;
b) change or update certificates in regular intervals (dependent on expire intervals);
c) deal with compromised keys;
d) log key management related activities;
e) implement the root certificates in the NCP Trusted Service List (see D3.4.2/4.4)

Justification:
profiled for NCP

A.12.4 Security of system files

A.12.4.1 Control of operational software	REC	final	ISO	BP

Description:
There should be procedures in place to control the installation of software on operational systems.

Edit Status:
as per ISO 27002

Other Information:
Operating systems should only be upgraded when there is a requirement to do so, for example, if the current version of the operating system no longer supports the business requirements. Upgrades should not take place just because a new version of the operating system is available. New versions of operating systems may be less secure, less stable, and less well understood than current systems.

Implementation Guidance:

To minimize the risk of corruption to operational systems, the following guidelines should be considered to control changes:
a) the updating of the operational software, applications, and program libraries should only be performed by trained administrators upon appropriate management authorization (see A.12.4.3);
b) operational systems should only hold approved executable code, and not development code or compilers;
c) applications and operating system software should only be implemented after extensive and successful testing; the tests should include tests on usability, security, effects on other systems and user-friendliness, and should be carried out on separate systems (see also 10.1.4); it should be ensured that all corresponding program source libraries have been updated;
d) a configuration control system should be used to keep control of all implemented software as well as the system documentation;
e) a rollback strategy should be in place before changes are implemented;
f) an audit log should be maintained of all updates to operational program libraries;
g) previous versions of application software should be retained as a contingency measure;
h) old versions of software should be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive.
Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software.
Any decision to upgrade to a new release should take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses (see also A.12.6.1).
Physical or logical access should only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities should be monitored.
Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

A.12.4.2	Protection of system test data	REC	final	epSOS	BP

Description:
Test data should be selected carefully, and protected and controlled.

Other Information:
System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data.

Implementation:
epSOS test data must not contain references to living or recently deceased persons.

Justification:
take no risk with sensitive data in testing

A.12.4.3	Access control to program source code	REC	final	ISO	BP

Description:
Access to program source code should be restricted.

Implementation Guidance:

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries. The following guidelines should then be considered (see also 11) to control access to such program source libraries in order to reduce the potential for corruption of computer programs:
a) where possible, program source libraries should not be held in operational systems;
b) the program source code and the program source libraries should be managed according to established procedures;
c) support personnel should not have unrestricted access to program source libraries;
d) the updating of program source libraries and associated items, and the issuing of program sources to programmers should only be performed after appropriate authorization has been received;
e) program listings should be held in a secure environment (see 10.7.4);
f) an audit log should be maintained of all accesses to program source libraries;
g) maintenance and copying of program source libraries should be subject to strict change control procedures (see 12.5.1).

Justification:
profiled for NCP

A.12.5 Security in development and support processes

A.12.5.1	Change control procedures	REC	final	epSOS	BP

Description:
The implementation of changes should be controlled by the use of formal change control procedures.

Other Information:
Program source code is code written by programmers, which is compiled (and linked) to create executables. Certain programming languages do not formally distinguish between source code and executables as the executables are created at the time they are activated.
The standards ISO 10007 and ISO/IEC 12207 provide further information about configuration management and the software lifecycle process.

Implementation:
Formal change control procedures should be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control, and managed implementation.
This process should include a risk assessment, analysis of the impacts of changes, and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.
Wherever practicable, application and operational change control procedures should be integrated (see also A.10.1.2). The change procedures should include:
a) maintaining a record of agreed authorization levels;
b) ensuring changes are submitted by authorized users;
c) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;
d) identifying all software, information, database entities, and hardware that require amendment;

e) obtaining formal approval for detailed proposals before work commences;
f) ensuring communication patners (other NCPs national participants) accept changes prior to implementation;
g) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;
h) maintaining a version control for all software updates;
i) maintaining an audit trail of all change requests;
j) ensuring that operating documentation (see A.10.1.1) and user procedures are changed as necessary to remain appropriate;
k) ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

A.12.5.2	Technical review of applications after operating system	REC	final	epSOS	BP

Description:
When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Other Information:
Changing software can impact the operational environment.
Good practice includes the testing of new software in an environment segregated from both the production and development environments (see also A.10.1.4). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs, and other updates. Automated updates should not be used on critical systems as some updates may cause critical applications to fail (see A.12.6).

Implementation:
This process should cover:
a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;
b) ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;
c) ensuring that notification of operating system changes is provided in time to allow appropriate tests and reviews to take place before implementation;
A specific group or individual should be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes (see A.12.6).

Justification:
profiled for epSOS

A.12.5.3	Restrictions on changes to software packages	REC	final	ISO	BP

Description:
Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.

Edit Status:
as per ISO 27002

Implementation Guidance:

As far as possible, and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified the following points should be considered:
a) the risk of built-in controls and integrity processes being compromised;
b) whether the consent of the vendor should be obtained;
c) the possibility of obtaining the required changes from the vendor as standard program updates;
d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes.
If changes are necessary the original software should be retained and the changes applied to a clearly identified copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software (see 12.6). All changes should be fully tested and documented, so that they can be reapplied if necessary to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

A.12.5.5	Outsourced software development	REC	final	epSOS	BP

Description:
Outsourced software development should be supervised and monitored by the organization.

Implementation:
Where software development is outsourced, the following points should be considered:
a) licensing arrangements, code ownership, and intellectual property rights (see A.15.1.2);
b) contractual requirements for liabilty;
c) escrow arrangements in the event of failure of the third party;
d) rights of access for audit of the quality and accuracy of work done;

Justification:
adapted to risk level (informal estimation)

13 Information security incident management

A.13.1 Reporting information security events and weaknesses

A.13.1.1	Reporting information security events		REQ	final	epSOS	BP

Description:
Information security events should be reported through appropriate management channels as quickly as possible.

Implementation:
D3.8.1/6.2.1.1 defines incident management. Information security incident management is a subordinate function of general incident management, but the responsibility to process or escalate an infosec incident may be different. (see A.8.1.1)
Beyond the guidelines in D3.8.1/6.2.1.1 following considerations apply:
A report of an incident should note if is a information security event. A point of contact should be established for the reporting of information security events. It should be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.
All employees, contractors and third party users should be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact. The reporting procedures should include:
a) information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event;
b) the correct behaviour to be undertaken in case of an information security event, i.e.
1) noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behaviour) immediately;
2) not carrying out any own action, but immediately reporting to the point of contact;

Justification:
profiled for epSOS

A.13.1.2	Reporting security weaknesses	NCP-Requ#3.7.23,	REQ	final	ISO	C

Description:
All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

Edit Status:
as per ISO 27002

Implementation Guidance:
All employees, contractors and third party users should report these matters either to their management or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible, and available as

possible. They should be informed that they should not, in any circumstances, attempt to prove a suspected weakness.

A.13.2 Management of information security incidents and improvements

A.13.2.1	Responsibilities and procedures	REC	final	ISO	BP

Description:
Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.

Edit Status:
as per ISO 27002

Other Information:
Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate.Employees, contractors and third party users should be advised not to attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

Implementation Guidance:
In addition to reporting of information security events and weaknesses (see also A.13.1), the monitoring of systems, alerts, and vulnerabilities (A.10.10.2) should be used to detect information security incidents. The following guidelines for information security incident management procedures should be considered:
a) procedures should be established to handle different types of information security incident, including:
1) information system failures and loss of service;
2) malicious code (see A.10.4.1);
3) denial of service;
4) errors resulting from incomplete or inaccurate business data;
5) breaches of confidentiality and integrity;
6) misuse of information systems;
b) in addition to normal contingency plans (see A.14.1.3), the procedures should also cover (see also A.13.2.2):
1) analysis and identification of the cause of the incident;
2) containment;
3) planning and implementation of corrective action to prevent recurrence, if necessary;
4) communication with those affected by or involved with recovery from the incident;
5) reporting the action to the appropriate authority;
c) audit trails and similar evidence should be collected (see A.13.2.3) and secured, as appropriate, for:
1) internal problem analysis;
2) use as forensic evidence in relation to a potential breach of contract or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
3) negotiating for compensation from software and service suppliers;

d) action to recover from security breaches and correct system failures should be carefully and formally controlled; the procedures should ensure that:
1) only clearly identified and authorized personnel are allowed access to live systems and data (see also A.6.2 for external access);
2) all emergency actions taken are documented in detail;
3) emergency action is reported to management and reviewed in an orderly manner;
4) the integrity of business systems and controls is confirmed with minimal delay.
The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

A.13.2.2	Learning from information security incidents	REC	final	ISO	BP

Description:
There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

Edit Status:
as per ISO 27002

Other Information:
The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process (see 5.1.2).The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process (see 5.1.2).

Implementation Guidance:
The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

A.13.2.3	Collection of evidence	REC	final	ISO	BP

Description:
Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Edit Status:
as per ISO 27002

Other Information:
When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required.
Evidence may transcend organizational and/or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions.When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness

of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required. Evidence may transcend organizational and/or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions.

Implementation Guidance:
Internal procedures should be developed and followed when collecting and presenting evidence for the purposes of disciplinary action handled within an organization.
In general, the rules for evidence cover:
a) admissibility of evidence: whether or not the evidence can be used in court;
b) weight of evidence: the quality and completeness of the evidence.
To achieve admissibility of the evidence, the organization should ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence.
The weight of evidence provided should comply with any applicable requirements. To achieve weight of evidence, the quality and completeness of the controls used to correctly and consistently protect the evidence (i.e. process control evidence) throughout the period that the evidence to be recovered was stored and processed should be demonstrated by a strong evidence trail. In general, such a strong trail can be established under the following conditions:
a) for paper documents: the original is kept securely with a record of the individual who found the document, where the document was found, when the document was found and who witnessed the discovery; any investigation should ensure that originals are not tampered with;
b) for information on computer media: mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory should be taken to ensure availability; the log of all actions during the copying process should be kept and the process should be witnessed; the original media and the log (if this is not possible, at least one mirror image or copy) should be kept securely and untouched.
Any forensics work should only be performed on copies of the evidential material. The integrity of all evidential material should be protected. Copying of evidential material should be supervised by trustworthy personnel and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilized should be logged.

15 Compliance

A.15.1 Compliance with legal requirements

A.15.1.3	Protection of organizational records	REQ	final	ISO	BP

Description:
Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

Other Information:
Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organization operates within statutory or regulatory rules, to ensure adequate defense against potential civil or criminal action, or to confirm the financial status of an organization with respect to shareholders, external parties, and auditors. The time period and data content for information retention may be set by national law or regulation.
Further information about managing organizational records can be found in ISO 15489-1.

Implementation Guidance:
Records should be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keying material and programs associated with encrypted archives or digital signatures (see 12.3), should also be stored to enable decryption of the records for the length of time the records are retained.
Consideration should be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations. For long term storage, the use of paper and microfiche should be considered.
Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change.
Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.
The system of storage and handling should ensure clear identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.
To meet these record safeguarding objectives, the following steps should be taken within an organization:
a) guidelines should be issued on the retention, storage, handling, and disposal of records and information;
b) a retention schedule should be drawn up identifying records and the period of time for which they should be retained;
c) an inventory of sources of key information should be maintained;
d) appropriate controls should be implemented to protect records and information from loss, destruction, and falsification.

ID	Title	epSOS Reference	Rel	Status	Impl.	R/S
A.15.1.4	Data protection and privacy of personal information	NCP-REQ 3.7.05, 07; D3.	REQ	final	epSOS	LR

Description:
Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

Other Information:
A number of countries have introduced legislation placing controls on the collection, processing, and transmission of personal data (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing, and disseminating personal information, and may restrict the ability to transfer that data to other countries.

Implementation:
This topic is covered by D3.8.1/chapter 5. It is a responsibility to be fulfilled when localizing the framework agreement (FWA).

A.15.1.5	Prevention of misuse of information processing facilities	REC	final	epSOS	BP

Description:
Users should be deterred from using information processing facilities for unauthorized purposes.

Other Information:
The information processing facilities of an organization are intended primarily or exclusively for business purposes.
Intrusion detection, content inspection, and other monitoring tools may help prevent and detect misuse of information processing facilities.
Many countries have legislation to protect against computer misuse. It may be a criminal offence to use a computer for unauthorized purposes.
The legality of monitoring the usage varies from country to country and may require management to advise all users of such monitoring and/or to obtain their agreement. Where the system being entered is used for public access (e.g., a public web server) and is subject to security monitoring, a message should be displayed saying so.

Implementation:
As defined in A.7.1.3, epSOS-equipment is dedicated and may not be used for any other purpose.

A.15.2 Compliance with security policies and standards, and technical compliance

A.15.2.1	Compliance with security policies and standards	REC	final	ISO	C

Description:
Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

Other Information:
Operational monitoring of system use is covered in A.10.10.

Implementation Guidance:

Managers should regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements.
If any non-compliance is found as a result of the review, managers should:
a) determine the causes of the non-compliance;
b) evaluate the need for actions to ensure that non-compliance do not recur;
c) determine and implement appropriate corrective action;
d) review the corrective action taken.
Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out the independent reviews (see A.6.1.8), when the independent review takes place in the area of their responsibility.

A.15.2.2	Technical compliance checking	REC	final	ISO	BP

Description:
Information systems should be regularly checked for compliance with security implementation standards.

Other Information:
Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical expertise.
Compliance checking also covers, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities.
Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s). Penetration testing and vulnerability assessments are not a substitute for risk assessment.

Implementation Guidance:
Technical compliance checking should be performed either manually (supported by appropriate software tools, if necessary) by an experienced system engineer, and/or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist.
If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable.
Any technical compliance check should only be carried out by competent, authorized persons, or under the supervision of such persons.

A.15.3 Information systems audit considerations

A.15.3.1	Information systems audit controls	REC	final	ISO	C

Description:
Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.

Edit Status:

audit poicy needs to be specified

Implementation Guidance:
The following guidelines should be observed:
a) audit requirements should be agreed with appropriate management;
b) the scope of the checks should be agreed and controlled;
c) the checks should be limited to read-only access to software and data;
d) access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;
e) resources for performing the checks should be explicitly identified and made available;
f) requirements for special or additional processing should be identified and agreed;
g) all access should be monitored and logged to produce a reference trail; the use of time- stamped reference trails should be considered for critical data or systems;
h) all procedures, requirements, and responsibilities should be documented;
i) the person(s) carrying out the audit should be independent of the activities audited.

A.15.3.2	Protection of information systems audit tools	REC	final	epSOS	BP

Description:
Access to information systems audit tools should be protected to prevent any possible misuse or compromise.

Other Information:
If third parties are involved in an audit, there might be a risk of misuse of audit tools by these third parties, and information being accessed by this third party organization. Controls such as 6.2.1 (to assess the risks) and 9.1.2 (to restrict physical access) can be considered to address this risk, and any consequences, such as immediately changing passwords disclosed to the auditors, should be taken.

Implementation:
Information systems audit tools, e.g. software or data files, should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.
Other controls like A.10.1.3 (segregation of duties) and A.11.6.2 (isolation of sensitive systems) help to enforce this.