## ISO27001:2013

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Included</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
<th>Solution implemented</th>
<th>Evidence and deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1 Policies for information security</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1.2 Review of the policies for information security</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.1 Information security roles and responsibilities</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.2 Segregation of duties</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.3 Contact with authorities</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.4 Contact with special interest group</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.5 Information security in project management</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.1 Mobile device policy</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.2 Teleworking</td>
<td>Yes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.1 Human resource security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Information security policies

- **Policy**: A set of policies for information security shall be defined and approved by management, published, and communicated to employees and relevant external parties. It is reviewed annually and approved by the Cloud Services Department.
- **Review**: The policy for information security shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

### Organisation of information security

- **Establish a management framework to initiate and control the implementation and operation of information security within the organisation**

### Mobile devices and teleworking

- **Ensure the security of teleworking and use of mobile devices**

### Human resource security

- **Human Resources Security**

---

**SEPO016 - Cegid Cloud Factory information security policy**

- **Scope**: The Cegid Security Team maintains regular exchanges with the CNIL and the ANSSI, as well as all relevant authorities. It is hierarchically and operationally independent of the ISMS activities.
- **Objectives**: The employees of the Cegid Security Team are members of the following organisations:
  - Cloud/Dev internal services agreement
  - Secure development charter
  - Cloud/Dev external services agreement
  - Security of info projects

**SEPS4 - Management of governance, roles, and responsibilities of ISMS**

- **Scope**: The Group Security Team is organised cross-functionally and it is hierarchically and operationally independent of the ISMS activities.
- **Objectives**: The employees of the Cegid Security Team are members of the following organisations:
  - Cloud/Dev/CloudSEC
  - Cegid Security Team maintains regular exchanges with the CNIL and the ANSSI.

---

**SEPO7 - Mobile devices and teleworking**

- **Scope**: The Cegid Security Team maintains regular exchanges with the CNIL and the ANSSI, as well as all relevant authorities.
- **Objectives**: The employees of the Cegid Security Team are members of the following organisations:
  - Cloud/Dev/CloudSEC
  - Cegid Security Team maintains regular exchanges with the CNIL and the ANSSI.

**SEPO039 - Human Resources Security**

- **Scope**: The Cegid Security Team maintains regular exchanges with the CNIL and the ANSSI, as well as all relevant authorities.
- **Objectives**: The employees of the Cegid Security Team are members of the following organisations:
  - Cloud/Dev/CloudSEC
  - Cegid Security Team maintains regular exchanges with the CNIL and the ANSSI.
An access control policy shall be established, documented, and included in the organization's responsibilities for information security.

The allocation and use of privileged access rights shall be restricted to the employee or contractor and enforced.

Management of privileged access rights shall be reviewed based on business and information security requirements. The policy shall take into account the level of classification of assets associated with its level of importance to the organization.

Security training for new employees is systematically provided. It is communicated only when the employee's personnel number is assigned.

Access control policy reviewed annually. Privacy statements are considered.

The access rights of all employees and external party users to information and information processing facilities shall be removed through a formal management process.

Due to the nature of physical assets and the size of the organization.

A check of references (diplomas, criminal record, etc.) is conducted by the Group's recruitment team. Letter of commitment from Management.

All candidates for employment shall have appropriate background checks conducted.

Security training for new employees is systematically provided. It is communicated only when the employee's personnel number is assigned.

Security training for new employees is systematically provided. It is communicated only when the employee's personnel number is assigned.
9.4 System and application access control

- Prevent unauthorized access to systems and applications

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users shall be required to follow the organization's practices in the use of secure authorizations.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The use of sensitive or critical information processing systems and applications shall be controlled.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9.4.1 Information access restriction

Access to information and application system functions shall be restricted and monitored to ensure compliance with the access control policy.

- Rights matrix

9.4.2 Securing log on procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log on procedure.

- Rights matrix

9.4.3 Password management system

Password management systems shall be interactive and shall ensure that quality passwords are used.

- Rights matrix

9.4.4 Use of privileged utility programs

The use of privileged utility programs that might be capable of controlling system and application control access shall be restricted and tightly controlled.

- Rights matrix

9.4.5 Access control to program source code

Access to program source code shall be restricted.

- Rights matrix

10 Cryptography

10.1 Cryptographic controls

Ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>A policy on the use of cryptographic controls for protection of information shall be developed and implemented.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy or encryption of data and files</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>This policy is reviewed regularly to provide the necessary level of security in keeping with standard good practices.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10.2 Key management

A policy on the use of keys, lifetime of cryptographic keys shall be developed and implemented through a whole-life key lifecycle management process.

- Rights matrix

10.3 Security perimeters

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information systems.

- Rights matrix

11 Physical and environmental security

11.1 Secure areas

Prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information systems.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security for offices, rooms, and facilities shall be designed and applied.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical protection measures against natural disasters, malicious attacks or accidents should be designed and implemented.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures for working in secure areas shall be designed and applied.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to areas of the building shall be controlled and isolated.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11.2 Equipment

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power and telecommunications cabling carrying data or supporting information systems shall be protected from interception, interference, or damage.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment maintenance shall be correctly maintained to ensure its continued availability and integrity.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment shall be correctly maintained to ensure its continued availability and integrity.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment shall be locked when in use.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12 Operational security

12.1 Operational procedures and responsibilities

Ensure correct and secure operations of information processing facilities

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating procedures shall be documented and made available to all users who need them.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Change management

Changes to the organization's business processes, information processing facilities, and systems that affect information security shall be controlled. | X | X |

12.2 Secure disposal and re-use of equipment

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk encryption, retention, secure remote connection via access gateway, and/or VPNs</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evidence of data destruction through Cloud Contract</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12.3 Separation of development, testing and operational environments

Ensure that development and operational environments are separate and that separation is enforced.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segregation through automated workflows in Azure DevOps</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12.4 Security perimeters

Prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information systems.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security for offices, rooms, and facilities shall be designed and applied.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical protection measures against natural disasters, malicious attacks or accidents should be designed and implemented.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures for working in secure areas shall be designed and applied.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to areas of the building shall be controlled and isolated.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12.5 Security controls

Security controls shall be selected and applied.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
<tbody>
<tr>
<td>The use of secure authorizations shall be controlled.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The rights and access matrix defines access by business group and application.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Rights matrix

12.6 Access control to program source code

Access to program source code shall be restricted.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
</table>
| Rights matrix

12.7 Privileged utility programs

The use of privileged utility programs that might be capable of controlling system and application control access shall be restricted and tightly controlled.

<table>
<thead>
<tr>
<th>Rule</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
</table>
| Rights matrix
12.1.1 Controls against malware
Detection, prevention, and recovery controls to protect against malware must be implemented, combined with appropriate access controls.

12.2 Backup

12.2.1 Information backup
Backup copies of all information systems, software, and system images shall be taken and tested regularly in accordance with an agreed backup policy.

X YES

12.2.2 Log and monitoring

12.2.2.1 Event logging
Event logs recording user activities, excepting tasks, fail to, and information security events shall be produced, kept, and reviewed regularly.

X X X

12.2.2.2 Protection of log information
Logging facilities and log information shall be protected against tampering and unauthorised access.

X X

12.2.2.3 Administrator and operator logs
System administrator and system operator activities shall be logged against the associated risk.

X X

12.2.4 Time synchronisation
The use of all network information processing systems within an organisation or security domain shall be synchronised to a single reference time source.

X X

12.2.5 Network architecture documents
The backup policy takes into account the specific of each client offer.

X

12.2.6 System administrator and system operator activities shall be logged.

12.2.6.1 Service agreements
Service agreements shall include a policy for handling these vulnerabilities by scope of evolution mode.

X

12.2.6.2 Software installation
Software installation policies shall be established and implemented.

X

12.3 System security and management

12.3.1 Network security management
Ensure that information security is designed and implemented within the development lifecycle of information systems.

YES

12.3.1.1 Information security requirements analysis and specification
Ensure that information security is an integral part of all network services shall be identified and included in network services agreements when these services are provided to or on behalf of another entity.

X

12.3.1.2 Segregation of services
Groups of information services, users, and information systems shall be segregated on networks.

Y

12.3.1.3 Information transfer
Maintain the security of information transferred between an organisation and with any external entity.

Y

12.3.1.4 Agreements on information transfer
Agreements shall address the secure transfer of business information between the organisation and external parties.

Y

12.3.1.5 Electronic messaging
Information involved in electronic messaging shall be appropriately protected.

Y

12.3.1.6 Confidentiality or non-disclosure agreements
Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed, and documented.

X

12.4 System security in development and support processes

12.4.1 Security requirements of information systems
Ensure that information security is an integral part of all information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

YES

12.4.1.1 Security requirements analysis and specification
The information security-related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

Y

12.4.2 Security application services on public networks
Information involved in application services passing over public networks shall be protected from fraud activity, contract dispute, unauthorized disclosure, and unauthorized duplication.

Y

12.4.3 Protecting application services transactions
Information involved in application services transactions shall be protected to prevent capture, transmission, misuse, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Y

12.4.4 System change control procedures
Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

Y

12.4.5 Technical evaluation of applications after operating platform changes
X

13 Communications security

13.1 Network security management
Ensure the protection of information in networks and its supporting information processing facilities.

Included

13.1.1 Network controls
Networks shall be managed and controlled to protect information in systems and applications.

X X

13.1.2 Security of network services
Security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreements when these services are provided to or on behalf of another entity.

Y

13.1.3 Segregation in networks
Groups of information services, users, and information systems shall be segregated on networks.

Y

13.1.4 Information transfer
Maintain the security of information transferred between an organisation and with any external entity.

Y

13.1.5 Agreements on information transfer
Agreements shall address the secure transfer of business information between the organisation and external parties.

Y

13.1.6 Electronic messaging
Information involved in electronic messaging shall be appropriately protected.

Y

13.1.7 Confidentiality or non-disclosure agreements
Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed, and documented.

Y

14 Acquisition, development, and maintenance

14.1 Security requirements of information systems
Ensure that information security is an integral part of all information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

Included

14.1.1 Information security requirements analysis and specification
The information security-related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

X

14.1.2 Security application services on public networks
Information involved in application services passing over public networks shall be protected from fraud activity, contract dispute, unauthorized disclosure, and unauthorized duplication.

X

14.1.3 Protecting application services transactions
Information involved in application services transactions shall be protected to prevent capture, transmission, misuse, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

X

14.2 Security development and support processes
Ensure that information security is designed and implemented within the development lifecycle of information systems.

Included

14.2.1 Secure development policy
Assure the development of software and systems shall be established and applied to developments within the organisation.

Y

14.2.2 System change control procedures
Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

Y

14.2.3 Technical evaluation of applications after operating platform changes
X

15.1 Communications security

15.1.1 Network security management
Ensure the protection of information in networks and its supporting information processing facilities.

Included

15.1.2 Security of network services
Security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreements when these services are provided to or on behalf of another entity.

X

15.1.3 Segregation in networks
Groups of information services, users, and information systems shall be segregated on networks.

Y

15.1.4 Information transfer
Maintain the security of information transferred between an organisation and with any external entity.

Y

15.1.5 Agreements on information transfer
Agreements shall address the secure transfer of business information between the organisation and external parties.

Y

15.1.6 Electronic messaging
Information involved in electronic messaging shall be appropriately protected.

Y

15.1.7 Confidentiality or non-disclosure agreements
Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed, and documented.

Y

16.1 Security requirements of information systems
Ensure that information security is an integral part of all information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

Included

16.1.1 Information security requirements analysis and specification
The information security-related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

X

16.1.2 Security application services on public networks
Information involved in application services passing over public networks shall be protected from fraud activity, contract dispute, unauthorized disclosure, and unauthorized duplication.

Y

16.1.3 Protecting application services transactions
Information involved in application services transactions shall be protected to prevent capture, transmission, misuse, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Y

16.2 Security development and support processes
Ensure that information security is designed and implemented within the development lifecycle of information systems.

Included

16.2.1 Secure development policy
Assure the development of software and systems shall be established and applied to developments within the organisation.

Y

16.2.2 System change control procedures
Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

Y

16.2.3 Technical evaluation of applications after operating platform changes
X

17.1 Communications security

17.1.1 Network security management
Ensure the protection of information in networks and its supporting information processing facilities.

Included

17.1.2 Security of network services
Security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreements when these services are provided to or on behalf of another entity.

X

17.1.3 Segregation in networks
Groups of information services, users, and information systems shall be segregated on networks.

Y

17.1.4 Information transfer
Maintain the security of information transferred between an organisation and with any external entity.

Y

17.1.5 Agreements on information transfer
Agreements shall address the secure transfer of business information between the organisation and external parties.

Y

17.1.6 Electronic messaging
Information involved in electronic messaging shall be appropriately protected.

Y

17.1.7 Confidentiality or non-disclosure agreements
Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed, and documented.

Y

18 Acquisition, development, and maintenance

18.1 Security requirements of information systems
Ensure that information security is an integral part of all information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

Included

18.1.1 Information security requirements analysis and specification
The information security-related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

X

18.1.2 Security application services on public networks
Information involved in application services passing over public networks shall be protected from fraud activity, contract dispute, unauthorized disclosure, and unauthorized duplication.

Y

18.1.3 Protecting application services transactions
Information involved in application services transactions shall be protected to prevent capture, transmission, misuse, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Y

18.2 Security development and support processes
Ensure that information security is designed and implemented within the development lifecycle of information systems.

Included

18.2.1 Secure development policy
Assure the development of software and systems shall be established and applied to developments within the organisation.

Y

18.2.2 System change control procedures
Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

Y

18.2.3 Technical evaluation of applications after operating platform changes
X

19.1 Communications security

19.1.1 Network security management
Ensure the protection of information in networks and its supporting information processing facilities.

Included

19.1.2 Security of network services
Security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreements when these services are provided to or on behalf of another entity.

X

19.1.3 Segregation in networks
Groups of information services, users, and information systems shall be segregated on networks.

Y

19.1.4 Information transfer
Maintain the security of information transferred between an organisation and with any external entity.

Y

19.1.5 Agreements on information transfer
Agreements shall address the secure transfer of business information between the organisation and external parties.

Y

19.1.6 Electronic messaging
Information involved in electronic messaging shall be appropriately protected.

Y

19.1.7 Confidentiality or non-disclosure agreements
Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed, and documented.

Y

20.1 Security development and support processes
Ensure that information security is designed and implemented within the development lifecycle of information systems.

Included

20.1.1 Secure development policy
Assure the development of software and systems shall be established and applied to developments within the organisation.

Y

20.1.2 System change control procedures
Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

Y

20.1.3 Technical evaluation of applications after operating platform changes
X
18.2.4 Restrictions on changes to software packages
Modifications to software packages shall be discouraged, limited to
incorrectness, and all changes shall be strictly controlled.

18.2.5 Secure system engineering principles
Principles for engineering secure systems shall be established.

18.2.6 Secure development environment
Organizations shall establish and appropriately protect secure
development environments for system development and integration
efforts that cover the entire software development lifecycle.

18.2.7 Outsourced development
The organization shall supervise and oversee the
outsourced systems development.

18.3 System security testing
Testing of security functionality shall be carried out during development.

18.4 System acceptance testing
Acceptance tests are performed and related clauses shall be
established for new information systems, upgrades, and new revisions.

18.4.1 Test plans
Ensure the provision of test data.

18.5 Test data
Test data shall be selected carefully, protected, and controlled.

15 Supplier relationships
SEPO13: Supplier relationships

15.1 Information security in supplier relationships
Ensure protection of the organization's assets that are
accessible by suppliers.

15.1.1 Information security policy for supplier relationships
In all relevant information security requirements, including
documentation, the supplier shall be involved and documented.

15.1.2 Addressing security within supplier agreements
An agreement with suppliers shall include requirements to address
information security risks associated with information
communications infrastructure, software, or provision of IT
infrastructure components for the organization's information.

15.1.3 Information and communication technology supply chain
Agreements with suppliers shall include requirements to address
information security risks associated with information
communications infrastructure, software, or provision of IT
infrastructure components for the organization's information.

15.2 Supplier service delivery management
Maintain an agreed level of information security services in line with supplier agreements.

15.2.1 Monitoring and review of supplier services
Organizations shall regularly monitor and review supplier services.

15.2.2 Managing changes to supplier services
Changes to the provision of services by suppliers, including
maintaining and improving existing information security policies,
procedures, and contracts, shall be managed to avoid the
criticality of business information, systems, and processes involved
and re-assessment of risks.

16 Information security incident management
SEPS3: Security incident management

16.1 Management of information security incidents and improvements
Ensure a consistent and effective approach to the
management of information security incidents, including
communication on security events and weaknesses.

16.1.1 Responsibilities and procedures
Management responsibilities and procedures shall be established to
ensure a quick, effective, and ongoing response to information security
incidents.

16.1.2 Reporting information security events
Information security events shall be reported through appropriate
management channels as quickly as possible.

16.1.3 Reporting information security weaknesses
Employees and contractors operating on the organization's
information systems and services shall be required to report any
observed or suspected information security weaknesses in systems or
services.

16.1.4 Reporting information security weaknesses
Information security events shall be recorded, and it shall be decided if
they are to be classified as information security incidents.

16.1.5 Response to information security incidents
Information security incidents shall be responded to in accordance with
the documented procedures.

16.1.6 Response to information security incidents
Information security incidents shall be responded to in accordance with
the documented procedures.

16.1.7 Collection of evidence
The organization shall define and apply procedures for the
investigation, collection, acquisition, and preservation of information,
which can serve as evidence.

17 Information security aspects of business continuity management
SEIT25: Business continuity management

17.3 Information security continuity
Information security continuity shall be embedded in the
organization's business continuity management systems.

17.3.1 Planning information security continuity
The organization shall determine its requirements for information
security and the continuity of information security management in
adverse situations, e.g., during a crisis or disaster.

17.3.2 Implementing information security continuity
The organization shall establish, document, implement, and maintain
guidelines, procedures, and controls to ensure the required level of
continuity for information security during an adverse situation.

17.3.3 Verify, review and evaluate information security continuity
The organization shall verify the established and implemented
information security continuity controls at regular intervals in order to
ensure that they are valid and effective during adverse situations.

17.3.4 Redundancy
Ensure availability of information processing facilities
in case of disaster, and these facilities shall be maintained with
redundancy sufficient to meet availability requirements.

17.8 Compliance
SEPO10: Compliance and audit management

17.8.1 Compliance with legal and contractual requirements
Avoid breaches of legal, statutory, regulatory, or contractual
obligations related to information security and any
corresponding requirements.

17.8.2 Identification of applicable legislation and contractual requirements
All relevant legislation, statutory, regulatory, contractual requirements
and the organization's approach to meet these requirements shall be
explicitly identified, documented, and kept up to date for each
information system and the organization.
18.1.2 Intellectual property rights

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.

<table>
<thead>
<tr>
<th>YES</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
</table>

Cegid Cloud Factory is committed to ensuring compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and the use of proprietary software products. Software is acquired from known and reputable sources to ensure that copyright is respected.

18.1.4 Privacy and protection of personally identifiable information

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

<table>
<thead>
<tr>
<th>YES</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
</table>

The General Data Protection Regulation has been applicable to the scope since 25 May 2018. In this context, Cegid has appointed a DPO in charge of monitoring the subject across the group.

18.2 Information security reviews

Ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

<table>
<thead>
<tr>
<th>Included</th>
<th>LO</th>
<th>CO</th>
<th>BC</th>
<th>BP</th>
<th>RA</th>
</tr>
</thead>
</table>

18.2.1 Independent review of information security

The organisation’s approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

<table>
<thead>
<tr>
<th>YES</th>
<th>X</th>
</tr>
</thead>
</table>

Cegid Cloud Factory conducts an internal audit of the information system at least once a year. A management review is planned at the end.

18.2.2 Compliance with security policies and standards

Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

<table>
<thead>
<tr>
<th>YES</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
</table>

18.2.3 Technical compliance review

Information systems shall be regularly reviewed for compliance with the organisation’s information security policies and standards.

<table>
<thead>
<tr>
<th>YES</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
</table>

A policy of pentests and technical auditing helps to identify deviations.

Scan Report