cegid

Statement of applicability ISO27001:2013

Version of 23/02/2023
Classification: Public

Modified by: Security Team

ISO27001:2013

		Solution implemented	Evidence and deliverables
4	**Context of the organisation**		
4.1	Understanding the organisation and its context	Scope of the SaaS Security Management System (SEPO12)	SELI030 - SOA
4.2	Understanding the needs and expectations of interested parties		
4.3	Determining the scope of the information security management system		
4.4	Information security management system		
5	**Leadership**		
5.1	Leadership and commitment	Management of governance, roles, and responsibilities of ISMS (SEPS4)	Letter of commitment from Management
5.2	Policy		Minutes of meetings of information security structures
5.3	Organisational roles, responsibilities, and authorities		
6	**Planning**		
6.1	Actions to address risks and opportunities	Risk Assessment and Treatment Process (SEPS5)	Results of risk analysis and RTP
6.2	Information security objectives and planning to achieve them		
7	**Support**		
7.1	Resources	Human Resources Security (SEPO9)	HR process and document
7.2	Competence		
7.3	Awareness		
7.4	Communication	ISMS Communication Process (SEPO11)	Security Committee meeting minutes
7.5	Documented information	Documentation management process (SEPS2)	Electronic Document Management process
8	**Operation**		
8.1	Operational planning and control	Control, monitoring, and improvement policy (SEPO17)	Security Committee meeting minutes
8.2	Informational security risk assessment	Risk management process (SEPS5)	Results of risk analysis and risk treatment plan
8.3	Informational security risk treatment		
9	**Performance evaluation**		
9.1	Monitoring, measurement, analysis, and evaluation	Control, monitoring, and improvement policy (SEPO17)	Security Committee meeting minutes
9.2	Internal audit	Compliance and audit management (SEPO10)	Audit planning
9.3	Management review	Management of governance, roles, and responsibilities of ISMS (SEPS4)	Management review
10	**Improvement**		
10.1	Nonconformity and corrective actions	Compliance and audit management (SEPO10)	Audit planning
10.2	Continual improvement	Control, monitoring, and improvement policy (SEPO17)	Security Committee meeting minutes Management review minutes

LO = Legal Obligations
CO = Contractual Obligations
BC = Business Commitment
BP = Best Practices
RA = Risk Analysis

The implementation of the security controls defined in the statement of applicability are intended to reduce the security risks that may exist in the ISMS.

ISO27001:2013 Annex A

	Requirements		Included	LO	CO	BC	BP	RA	Solution implemented	Evidence and deliverables
5	**Information security policies**									**SEPO16 - Cegid Cloud Factory information security policy**
5.1	**Management direction for information security**	**Provide management direction and support for information security in accordance with business requirements and relevants laws and regulations**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties.	YES				X	X	An information security policy has been drafted It is reviewed annually and approved by the Cloud Services Department	Letter of commitment from Management
5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	YES				X			
6	**Organisation of information security**									**SEPS4 - Management of governance, roles, and responsibilities of ISMS**
6.1	**Internal organisation**	**Establish a management framework to initiate and control the implementation and operation of information security within the organisation**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	YES				X		The Group Security Team is organised cross-functionally. It is hierarchically and operationally independent of the ISMS activities	Presentation of the missions and organisation of the teams dedicated to information security
6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce the opportunities for unauthorised or unintentional modification or misuse of any of the organisation's assets.	YES				X		DevOps-type organisation of assignments and teams	Organisation of AzurDevOps teams
6.1.3	Contact with authorities	Appropriate contacts with relevant authorities must be maintained.	YES	X			X		Cegid's Security Team maintains regular exchanges with the CNIL and the ANSSI	Email/Message Exchange
6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	YES				X		The employees of the Cegid Security Team are members of the following organisations: CLUSIR / CLUSIF /Club ISO 27001	Justification for subscribing to the Clusir/Clusif/
6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	YES				X	X	Organisation of teams and processes in agile mode (Azure DevOps) for consideration of security in infrastructure and development in all projects related to ISMS	Organisation of AzurDevOps teams Secure development charter Cloud/Dev internal services agreement Security of infra projects
6.2	**Mobile devices and teleworking**	**Ensure the security of teleworking and use of mobile devices**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		**SEOP7- Mobile devices and teleworking**
6.2.1	Mobile device policy	A policy and supporting security measures shall adopted to manage the risks introduced by using mobile devices	YES				X	X	Encryption of employee laptop disks Privacy filters MFA and VPN in mobility situations	
6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed, or stored at teleworking sites.	YES			X		X		
7	**Human resource security**									**SEPO9-Human Resources Security**

7.1	**Prior to employment**	**Ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations, and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks	YES			X		X	A check of references (diplomas, criminal record, etc.) is conducted by the Group's recruitment team	Group HR recruitment procedures SaaS/HR services agreement
7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security	YES			X		X	The employment contract signed by the new employees includes a confidentiality clause and a non-competition clause	
7.2	**During employment**	**Ensure that employees and contractors are aware of and fulfil their information security responsibilities**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	YES				X		Formal commitment of the Cloud Services Department through the various committees, meetings, and communications around security and ISMS	Letter of commitment from Management
7.2.2	Information security awareness, education, and training	All employees of the organisation and, where relevant, contractors shall receive appropriate learning and awareness training and regular updates in organisational policies and procedures, as relevant for their job function.	YES			X	X	X	Security training for new employees is systematically provided An annual awareness plan is developed	Training plans and contents Awareness-raising content and results
7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	YES			X	X	X	A disciplinary process may be initiated in the event of a breach of the ISSP or the IT tool use charter and equipment	Internal regulations Employment contract Enhanced confidentiality clause
7.3	**Termination and change of employment**	**Protect the organisation's interests as part of the process of changing or terminating employment.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	YES	X	X			X	Employees are informed of their responsibilities in the event of a change, termination, or end of contract by their HR correspondent	Employment contract
8	**Asset management**									**SEPO5-Asset management**
8.1	**Responsibility for assets**	**Identify organisational assets and define appropriate protection responsibilities**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	YES				X	X	The inventory of assets is reviewed and updated in the risk analysis tool	List of assets
8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	YES				X	X	The assets are the property of the Cloud Services Department	Define the owner of physical assets and the role of the owner
8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	YES		X		X	X	An Acceptable Use Policy has been drafted and communicated to employees	Acceptable Use Policy
8.1.4	Return of assets	All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract, or agreement.	YES		X		X		Return of assets according to the inventory of the employee termination form under the responsibility of the manager	Cegid Group Human Resources department sheet
8.2	**Information classification**	**Ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		**SEPS2-Documentation Management**
8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorised disclosure or modification.	YES				X		The information is classified according to 5 criteria	
8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation	YES				X		All assets (documents, client assets) are subject to the asset management policy. This policy takes into account the level of classification of assets associated with its level of dissemination and encryption necessary for its dissemination	RCNT7- Client disk lifecycle
8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.	YES				X			
8.3	**Media handling**	**Prevent unauthorised disclosure, modification, removal, or destruction of information stored on media.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	YES			X			Restriction of use of removable media (USB) for employees DC supplier Procedure for removable media for client data storage	Charter for the use of IS tools
8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	YES	X	X	X		X	Low-level formatting of the storage media of the employees' workstations Physical destruction of customer data storage media by the DC suppliers	Evidence of data destruction by SaaS production/access to shredder
8.3.3	Physical media transfer	Media containing information shall be protected against unauthorised access, misuse, or corruption during transportation.	YES		X	X		X	Encryption of removable storage media in case of customer data transfer Tracking of receipts and shipments by Chronopost	RCNT7- Client disk lifecycle
9	**Access control**									**SEPO1-Access control**
9.1	**Business requirements of access control**	**Limit access to information and information processing facilities**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
9.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and information security requirements.	YES	X		X	X	X	Access control policy reviewed annually	
9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorised to use.	YES			X	X		A rights matrix ensures the management of user rights and access to resources. This matrix is revised at least annually	Rights matrix
9.2	**User access management**	**Ensure authorised user access and prevent unauthorised access to systems and services**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	YES	X	X	X	X	X	Management of user registrations/deregistrations in our Cloud Factory platform orchestration tool	Service Request and Workflow stratus
9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	YES	X	X	X	X	X		
9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	YES			X	X	X	Allocation rights by user group on the applications to be used	Cegid Cloud Factory rights matrix
9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	YES			X	X	X	Authentication information is communicated according to a formalised HR process It is communicated only when the employee's personnel number is assigned	
9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals	YES			X	X	X	A revalidation of team rights by managers is conducted every quarter	Quarterly rights revalidation list validated by managers

9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change.	YES			X	X	X	On receipt of confirmation of our HR tools that the employment period has ended, the request is processed in our orchestration tool.	Service Request and Stratus Workflow
9.3	**User responsibilities**	**Make users accountable for safeguarding their authentication information.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
9.3.1	Use of secret authentication information	Users shall be required to follow the organisation's practices in the use of secret authentication information	YES			X	X	X	Rules for the use of secret information are clearly defined in the IT tool use charter	SENT14- Password management policy Acceptable Use Policy
9.4	**System and application access control**	**prevent unauthorised access to systems and applications**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	YES			X	X		The rights and access matrix defines access by business group and by application	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.	YES				X	X	The connection of Cegid Cloud Factory employees to the production environments is done via a P.A.M. (Bastion) and via a secure remote access system (RDM)	PAM user manual
9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	YES				X	X	A password management policy is defined for Cegid Cloud Factory employees as well as for clients using Cegid SaaS applications	SENT14- Password management policy
9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	YES						A shadow IT management and mitigation tool is used to control the use of unauthorised programs and applications	Rights matrix
9.4.5	Access control to program source code	Access to program source code shall be restricted	YES				X	X	Scripts are stored in secure areas that are accessible only to the production teams	List of authorised users
10	**Cryptography**									**SEPO12-Information transfer and encryption**
10.1	**Cryptographic controls**	**Ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	YES	X	X	X	X		Policy on encryption of flows and data This policy is reviewed regularly to provide the best level of security in keeping with standard good practices	Annual review of this policy
10.1.2	Key management	A policy on the use, protection, and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle	YES			X	X		Administration of certificates for HTTPS access in keeping with good practices Recognised certification authority, storage of keys in a key vault Management of encryption keys for data stored in the Datacenters	Certificates administered by Cegid and issued by a recognised CA Key management by Cegid (Private Cloud) or by the provider (Public Cloud)
11	**Physical and environmental security**									**SEPO1 Access control / SEPO6 Physical and environmental Security**
11.1	**Secure areas**	**Prevent unauthorised physical access, damage, and interference to the organisation information and information processing facilities.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities	YES				X		Operations and production teams are in physically isolated premises	Service agreement with supporting utilities
11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access	YES				X	X	Secure access to the production premises by badge for authorised employees only	Monthly access control list
11.1.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities shall be designed and applied	YES				X	X	Locked doors with alarms in case of prolonged opening	
11.1.4	Protecting against external and environmental threats	Physical protection measures against natural disasters, malicious attacks or accidents should be designed and implemented	YES		X	X	X	X	Protection of the building housing the production teams Power supply, air conditioning, network cabling, etc.	Internal supplier service agreement with General Services
11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	YES					X	Protection of the building housing the production teams Power supply, air conditioning, network cabling, etc. For Talentsoft's long-time premises, there is no work in secure areas. This requirement is therefore not included.	
11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access	YES				X	X	Deliveries are made to the building's security PC Control is carried out by a private security company under the responsibility of Cegid's SG	
11.2	**Equipment**	**Prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	YES				X	X	Sensitive equipment is stored in secure premises	Internal supplier service agreement with General Services
11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	YES					X	Independent power supply system is operational in case of failure of the general system	Inverter supplier maintenance contract
11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.	YES				X	X	The SaaS production LAN is a switched network physically independent from the rest of the company	SaaS network architecture configuration and scheme
11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity	YES				X	X	The maintenance of internal equipment and collaborators is subcontracted and formalised by contract by the IT Department	Internal supplier service agreement with the IT Department
11.2.5	Removal of assets	Equipment, information, or software shall not be taken off-site without prior authorization	YES					X	Formalised in the charter for use of IT tools and resources	
11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organisation's premises.	YES				X	X	Disk encryption, antivirus, secure remote connection via access gateway and/or VPN	Internal supplier service agreement with the IT Department
11.2.7	Secure disposal or 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	YES	X	X	X	X	X	Destruction of media containing customer data or related to such data (employees' workstations)	Evidence of data destruction through Cloud Contract SaaS production
11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection	YES				X	X	Anti-theft cable on employee workstations	Screens lock after 15 minutes (AD strategy)
11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted	YES				X		Storage of documents in a special collaborative space Individual storage locker - Shredder for documents to be disposed Automatic locking of sessions in case of an extended period of inactivity	
12	**Operational security**									**SEPO4 Operational security**
12.1	**Operational procedures and responsibilities**	**Ensure correct and secure operations of information processing facilities**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them	YES				X	X	All operating procedures are documented and accessible to all SaaS employees in EDM	Electronic document management process
12.1.2	Change management	Changes to the organisation, business processes, information processing facilities, and systems that affect information security shall be controlled	YES				X	X	A weekly meeting on change management is planned	Minutes and management of changes in Inside

12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance	YES			X	X	X	Ongoing monitoring of resource allocation Monthly committee on infrastructure and resource sizing	Centreon monitoring console Capacity planning meeting minutes Adaptation of HR to the activity
12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment	YES			X	X	X	Segregation through automated workflow in Azure DevOps	Network Architecture
12.2	**Protection from malware**	**Ensure that information and information processing facilities are protected against malware**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
12.2.1	Controls against malware	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness	YES				X	X	Centralised and managed antivirus/antimalware for all resources	Antiviral console (update of the document to be seen)
12.3	**Backup**	**Protect against loss of data**	**Included**	**LO**	**BO**	**BC**	**BP**	**RA**		
12.3.1	Information backup	Backup copies of information, software, and system images shall be taken and tested regularly in accordance with an agreed backup policy	YES					X	The backup policy takes into account the specific of each client offer. It takes into account availability, integrity, and retention.	Backup reports
12.4	**Logging and monitoring**	**Record events and generate evidence.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
12.4.1	Event logging	Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed	YES	X	X	X	X	X	Information security events are centralised in a log aggregation tool. This tool is governed by a well-defined policy	Log centralization consoles (Splunk)
12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorised access	YES	X			X	X	The log management tool is hosted in a secure architecture (redundancy, encryption of flows and disks, access management, backup)	Log centralization consoles (Splunk)
12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	YES		X		X	X	An automatic report of the administrator and operator logs is produced monthly	Administrator accounts report (Splunk)
12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source	YES		X		X	X	An NTP synchronisation is configured on all assets	Group strategies and NTP doc
12.5	**Control of operational software**	**Ensure the integrity of operational systems**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	YES				X	X	A tool and a centralised console make inventory management of software in operation possible. Installation templates are used for the configuration of virtual servers	Software inventory consoles
12.6	**Technical vulnerability management**	**Prevent exploitation of technical vulnerabilities**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		**Operational Security (OPSEU4)**
12.6.1	Management of Technical vulnerability	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk	YES				X	X	Vulnerability management is done through a scanning tool and through alerts from the CERTs Policy for handling these vulnerabilities by scope in escalation mode	Minutes of IS security monitoring meetings
12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented	YES				X	X	Shadow IT detection policy Tools on employee workstations	Charter for the use of tools
12.7	**Information systems audit considerations**	**Minimise the impact of audit activities on operational systems**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		**Operational Security (OPSEU4)**
12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes	YES				X	X	The various policies (Scan) and agreements (Pentest) take into account the periods of activity of the business lines in order to minimise the impact	Audit/Pentest agreement templates
13	**Communications security**									**SEPO14-Network security management**
13.1	**Network security management**	**Ensure the protection of information in networks and its supporting information processing facilities**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications	YES				X	X	Networks and links are overseen by monitoring tools. Access is tracked and controlled	Procedure for segregation of rights and teams. Access control and logs on equipment. Redundancy of teams, equipment, and resources. Internal supplier - IT Department service agreement A service agreement covering the service guarantee is applied with the IT department for the LAN and WAN part Network partitioning by setting up DMZs and VLANs. Networks and links are overseen live by monitoring tools.
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 whether these services are provided in-house or outsourced	YES				X	X	An internal service agreement is formalised annually with the IT Department It takes network security into account	Networks and links are overseen live by monitoring tools.
13.1.3	Segregation in networks	Groups of information services, users, and information systems shall be segregated on networks	YES				X	X	Network partitioning by setting up DMZs and VLANs.	Network architecture documents
13.2	**Information transfer**	**Maintain the security of information transferred within an organisation and with any external entity.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		**SEPO2- Information transfer and encryption**
13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures, and controls shall be in place to protect the transfer of information through the use of all types of communication facilities	YES				X	X	A policy setting out the rules for encryption and security of communications is established. It is reviewed periodically.	
13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organisation and external parties	YES			X	X	X	The secure exchange protocols used with third parties make it possible to guarantee the integrity, confidentiality, and non-repudiation of information	
13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected	YES				X	X	Email uses only secure processes (flow, authentication)	Email server configuration
13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or nondisclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented	YES		X		X	X	All Cegid personnel working with confidential data sign a confidentiality agreement, with no time limit, involving disciplinary measures or prosecution in the event of non-compliance.	HR processes
14	**Acquisition, development, and maintenance**									**SEPO8-Information security policy in project management**
14.1	**Security requirements of information systems**	**Ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		**SEPO2- Information transfer and encryption**
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	YES				X	X	Formalised security procedures are integrated into all projects and throughout the project lifecycle	Project security requirement questionnaires
14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.	YES	X			X	X	Perimeter protection of public network access (Firewall, IDS/IPS probe) Encryption of flows by certificates issued by a recognised certification body; the keys are stored in a digital safe	Information transfer and encryption policy
14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.	YES				X	X	Use of secure protocols that ensure complete transmission without possible modification of the information and prohibiting unauthorised modification, unauthorised disclosure, and unauthorised duplication.	

14.2	**Security in development and support processes**	**Ensure that information security is designed and implemented within the development lifecycle of information systems**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		**SEPO15 - Secure development policy**
14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organisation	YES				X	X	A policy describes and establishes a framework for the security of development processes	STRATUS
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	YES				X		Standard changes are made via the workflow of the platform orchestrator. Non-standard changes are handled by the change process	
14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business-critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security	YES				X	X	Hardware and/or system upgrades are tested on pilot groups before application to production environments	System update process
14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	YES				X		All changes relating to scripts and automatic control systems are logged in a GIT	No changes to the code of software packages used
14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	YES				X	X	Scripts and automatic control systems are standardised and tested before going into production	Training/Awareness
14.2.6	Secure development environment	Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle	YES				X	X	Manage through AzureDevOps workflow and development servers	Network Architecture
14.2.7	Outsourced development	The organisation shall supervise and monitor the activity of outsourced system development	YES		X		X		An internal service agreement with the development BUs oversees and controls activities and applications external to ISMS	
14.2.8	System security testing	Testing of security functionality shall be carried out during development	YES				X	X	The test phases and compliance tests are handled in the Azure DevOps workflow	
14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades, and new versions	YES				X	X		Vulnerability scan results
14.3	**Test data**	**Ensure the protection of data used for testing**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled	YES				X	X	Manage through AzureDevOps workflow and development servers	Copy logging
15	**Supplier relationships**									**SEP013-Supplier relationships**
15.1	**Information security in supplier relationships**	**Ensure protection of the organisation's assets that is accessible by suppliers**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with the supplier's access to the organisation's assets shall be agreed with the supplier and documented.	YES	X	X	X	X	X	The security policy in supplier relationships takes into account and describes the security requirements and measures necessary to comply with Cegid's legal, regulatory, and contractual obligations	
15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information	YES	X	X		X	X	Cegid ensures that its suppliers are involved in the security of the delivered service through certification and contractual commitments	
15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain	YES	X	X		X	X	Cegid ensures that its suppliers are involved in the security of the service delivered through certification and contractual commitments For Talentsoft's historical activities, there is no supply in the context of production, which is the responsibility of Quadria. This requirement is therefore not included.	
15.2	**Supplier service delivery management**	**Maintain an agreed level of information security and service delivery in line with supplier agreements**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
15.2.1	Monitoring and review of supplier services	Organisations shall regularly monitor, review, and audit supplier service delivery	YES	X	X		X	X		
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 controls, shall be managed, taking account of the criticality of business information, systems, and processes involved and re-assessment of risks	YES	X	X		X		Security steering committee meetings are planned and organised with suppliers on a recurring basis. Audits make it possible to assess developments and changes in the contractual framework	Kyndryl/Microsoft security committee meeting minutes
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**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents	YES	X		X	X	X	Security incident management process in accordance with ISO 27035 including Reporting of the security event Pre-qualification of the event Qualification phase Investigation Communication / Reporting Processing Feedback Closure of the incident A RACI matrix determines the roles and responsibilities for each phase A weekly review of incidents is conducted	Stratus
16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible	YES	X		X	X	X		
16.1.3	Reporting information security weaknesses	Employees and contractors using the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services	YES	X		X	X	X		
16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents	YES	X		X	X	X		
16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	YES	X		X	X	X		
16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	YES	X		X	X	X		
16.1.7	Collection of evidence	The organisation shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence	YES	X		X	X	X		
17	**Information security aspects of business continuity management**									**SEIT25-SaaS crisis management**
17.1	**Information security continuity**	**Information security continuity shall be embedded in the organisation's business continuity management systems**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
17.1.1	Planning information security continuity	The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster	YES			X	X	X	A business continuity policy provides a framework for the organisation and processes of information security continuity A "code red" process regulates crisis management	

17.1.2	Implementing information security continuity	The organisation shall establish, document, implement, and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation	YES			X	X	X	Various processes allow for the continuity of information security (data backup, resilience of infrastructure and human resources, administration of secure remote production tools)	Incident management / Code Red
17.1.3	Verify, review and evaluate information security continuity	The organisation 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	YES			X	X	X	Continuity of information security is assessed on a recurring basis	
17.2	**Redundancies**	**Ensure availability of information processing facilities**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements	YES		X	X	X	X	Redundancy and resilience mechanisms for architectures and teams are active from end to end. There is constant supervision of these mechanisms	SaaS architecture documents
18	**Compliance**									**SEPO10-Compliance and audit management**
18.1	**Compliance with legal and contractual requirements**	**Avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation	YES	X	X		X	X	The Cegid Group's legal process defines, documents, and updates all legal, regulatory, and contractual requirements applicable to the ISMS	Legal Process
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	YES	X	X		X	X	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.	Licence register
18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorised access, and unauthorised release, in accordance with legislative, regulatory, contractual, and business requirements	YES	X	X		X		Records are protected from loss, destruction, falsification, unauthorised access, and unauthorised publication.	
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	YES	X	X		X	X	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	
18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations	YES					X	Cegid Cloud Factory complies with the applicable agreements, laws, and regulations relating to cryptography. Cegid does not import or export any cryptographic solutions.	
18.2	**Information security reviews**	**Ensure that information security is implemented and operated in accordance with the organisational policies and procedures**	**Included**	**LO**	**CO**	**BC**	**BP**	**RA**		
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	YES				X	X	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	YES					X		ISMS Indicators and Objectives
18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards	YES			X	X	X	A policy of pentests and technical auditing helps to identify deviations	Scan Report