viedoc™

Information Security Statement of Applicability

Date 2024-03-19

Disclaimer

No part of this document may be modified, copied, or distributed without prior written consent from Viedoc Technologies AB. The information contained herein is subject to change without notice. Viedoc Technologies AB shall not be liable for technical or editorial errors or omissions contained herein.

Document History

Version	Author	Date	Change
1	Jens Pettersson	2019-05-09	Initial version.
2	Jens Pettersson	2020-06-04	Added headings, walk-through of current status.
3	Jens Pettersson	2020-11-20	Update after annual risk management workshops.
4	Jens Pettersson	2021-02-27	Inclusion of A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.11.2.5. Update implementation status of A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7, A.18.1.5, A.18.2.1.
4 rev 1	Jens Pettersson	2021-04-23	Updated justification risk references for controls A.8.3.1, A.8.3.2, A.9.4.2, A.9.4.3, A.10.1.2, A.11.1.3, A.11.2.8, A.11.2.9, A.12.6.2, A.13.1.3, A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4, A.15.1.1, A.15.1.2, A.15.1.3, A.18.1.1, A.18.1.3, A.18.1.5. Updated justification risk reference for controls A.9.2.5, A.12.1.3. Updated documentation of A.6.1.5, A.14.3.1. Included 21ViaNet in justification and documentation of controls A.11.1.1-2, A.11.1.4-6, A.11.2.1-5.
4 rev 2	Jens Pettersson	2022-02-18	New template. Updated implementation status of A.13.2.1, A.13.2.3, A.15.2.2. Updated risk references on A.5.1.1, A.6.1.2, A.6.1.3, A.6.1.5, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.10.1.2, A.11.1.2, A.11.1.3, A.11.2.8, A.11.2.9, A.12.1.1, A.12.1.2, A.12.3.1, A.13.2.2, A.14.1.1, A.14.2.9, A.14.3.1, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.18.1.1, A.18.1.3, A.18.2.3. Updated documentation on A.6.1.4, A.7.1.2, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.1, A.8.2.1, A.8.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.15.2.1, A.17.1.3, A.18.1.3.
4 rev 3	Jens Pettersson	2022-04-29	Document name change. Added ISO 27017:2021 and ISMAP controls.
4 rev 4	Jens Pettersson	2022-09-05	Added the subset of NIST SP 800-53 controls that are mapped to NIST SP 800-171 rev 2 (with mapping to ISO 27002 where applicable).
4 rev 5	Jens Pettersson	2023-03-21	Updated documentation on controls A.6.1.2, A.6.1.5, A.7.2.2, A.7.3.1, A.8.1.4, A.8.2.3, A.8.3.2, A.11.1.5, A.11.1.6, A.12.1.2, A.12.5.1, A.18.2.1. Updated documentation on controls ISMAP 8.1.2.7. PB, 10.1.2.20.PB.

			Updated documentation on controls NIST SP 800-53 AC-22. Corrected page numbers.
5	Predrag Gaikj	2024-03-19	Updated document template. Updated the security controls as defined in ISO27002:2022

Contents

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
	A.5 ORGANIZATIONAL CONTROLS							
ISO 27002: 2022	**A.5.1**	**Policies for information security**	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes	Starting point of ISMS. To ensure policies remain applicable, appropriate, and effective and comply with current legislation if required.	Implemented.	COMPOL03 Information Security Policy COMSOP18 ISMS Manual	CISO
ISO 27017: 2021		An information security policy for cloud computing should be defined as a topic-specific policy of the cloud service customer. [...]		Yes				
ISO 27017: 2021		The cloud service provider should augment its information security policy to address the provision and use of its cloud services, [...]		Yes				
ISO 27002: 2022	**A.5.2**	**Information security roles and responsibilities**	Information security roles and responsibilities should be defined and allocated according to the organization needs.	Yes	Required for effective management of the ISMS.	Implemented.	COMPOL03 Information Security Policy QSOff218 Role Description and Training Matrix	CISO CFO
ISO 27017: 2021		The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities and confirm that it can fulfil its allocated roles and responsibilities. [...]		Yes				
ISO 27017: 2021		The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers and its suppliers.		Yes				

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.5.3** *(NIST SP 800-53 AC-5, PL-2)*	**Segregation of duties**	Conflicting duties and conflicting areas of responsibility should be segregated.	Yes	Best practice and required for effective management of the ISMS.	Implemented.	COMPOL03 Information Security Policy QSOff218 Role Description and Training Matrix COMDOC16 Authorization Policy Viedoc Group VIESOP20 Managing Customer Projects	CISO CFO Global Head PS
ISO 27002: 2022	**A.5.4**	**Management responsibilities**	Management should require all personel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes	To ensure all personnel follow policies and procedures and thereby act in the best interest of the company.	Implemented.	COMPOL03 Information Security Policy	CISO
ISO 27002: 2022	**A.5.5** *(NIST SP 800-53 IR-6)*	**Contact with authorities**	The organization should establish and maintain contact with relevant authorities.	Yes	To ensure compliance with all applicable legislation and regulatory requirements.	Implemented.	COMPOL02 Data Protection Policy QSSOP16 Data Protection Officer	DPO
ISO 27017: 2021		The cloud service customer should identify the authorities relevant to the combined operation of the cloud service customer and the cloud service provider.		Yes		Implemented.	QA department have contacts with regulatory authorities through industry forums.	QA
ISO 27017: 2021		The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data.		Yes		Implemented.	MSA Appendix 4 – Data Processing Agreement Viedoc Privacy Policy	DPO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	A.5.6	**Contact with special interest groups**	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	To ensure we're kept up to date with developments in information security, IT vulnerabilities and developments in our industry that can affect information security.	Implemented.	CERT-SE CISSP ISACA ITSOP04 Back-office infrastructure [In ticket system] Recorded Future Cyber Daily CISA US-CERT CISA ICS-CERT [Industry forum memberships] CDISC eClinical Forum EUCROF ACDM RQA	CISO MIT MQA
ISO 27002: 2022	A.5.7	**Threat inteligence**	Information related to information security threats should be collected and analysed to produce threat inteligence.	Yes	To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.	Implemented.	COMSOP35 Office Infrastructure ITSOP13 Continuity Qualification	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.5.8**	**Information security in project management**	Information security should be integrated in project management.	Yes	To ensure project managers consider information security at the planning stage of all projects to ensure security weakness are not introduced and compliance with ISMS objectives are maintained.	Implemented.	DEVSOP01 Product Development Process VIESOP20 Managing Customer Projects SMPOL02 Information Security within Sales COMSOP19 Information Classification DEVPOL01 Secure Development Policy	CPO MPS CCO CISO CTO
ISO 27002: 2022	**A.5.9** *(NIST SP 800-53 CM-8)*	**Inventory of information and other associated assets**	An inventory of information and other associated assets, including owners, should be developed and maintained.	Yes	We need to know what information we are in possession of to protect it. Ownership of an asset is the first step in taking responsibility for protecting it.	Implemented.	COMDOC24 Asset Inventory COMSOP17 Risk Assessment and Risk Treatment Methodology ITOff183 Overview - IT infrastructure & system dependencies ITOff165 Asset overview - Internet domains ITOff182 Asset overview - Software subscriptions & licenses ITPCG48 Asset Inventory (working document not in ISMS document repository)	CISO MIT
ISO 27017: 2021		The cloud service customer's inventory of assets should account for information and associated assets stored in the cloud computing environment. The records of the inventory should indicate where the assets are maintained, e.g. identification of the cloud service.		Yes				
ISO 27017: 2021		The inventory of assets of the cloud service provider should explicitly identify: ▪ cloud service customer data; ▪ cloud service derived data.		Yes				

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	A.5.10 *(NIST SP 800-53 MP-2, MP-4, MP-6, MP-5, MP-7, SC-8, SC-28)*	**Acceptable use of information and othet associated assets**	Rules for the acceptable and procedures for handling information and other associated assets should be identified, documented and implemented.	Yes	The risk of a security incident is significantly reduced if acceptable use is clear. To ensure that all staff and third parties are aware of the classification of information to prevent unauthorized disclosure.	Implemented.	COMPOL03 Information Security Policy COMSOP19 Information Classification COMSOP35 Office Infrastructure QSSOP03 Document Control VIESOP20 Managing Customer Projects	CISO MIT MQA MPS
ISO 27002: 2022	A.5.11 *(NIST SP 800-53 PS-4, PS-5)*	**Return of assets**	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Yes	To reduce risk of disclosure or loss of information assets.	Implemented.	COMSOP35 Office Infrastructure COMSOP32 Employee Offboarding [ISMS document repository interactive termination checklist]	MIT CFO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021		Removal of cloud service customer assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement. [...] Customer: Request a documented description of the termination Provider: Provide information about the arrangements for the return	Yes	To reduce risk of disclosure of information assets.	Implemented.	ITSOP08 Electronic Data Continuity ITSOP12 Electronic Data Destruction https://help.viedoc.net/c/331b7a/a18275/en https://help.viedoc.net/c/331b7a/704ef7/en/	MIT CPO
ISO 27002: 2022	**A.5.12**	**Classification of information**	Information shoul be classified according to the information security needs of the organization based on confidentiality, integrity and availability and relevant interested party requirements.	Yes	To ensure that all staff and third parties are aware of the classification of information to prevent unauthorized disclosure.	Implemented.	COMSOP19 Information Classification COMDOC24 Asset Inventory QSSOP03 Document Control	CISO MQA
ISO 27002: 2022	**A.5.13**	**Labeling of information**	An appropriate set of procedures for information labeling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	To ensure that all staff and third parties are aware of the classification of information to prevent unauthorized disclosure.	Implemented.	QSSOP03 Document Control	MQA
ISO 27017: 2021		The cloud service customer should label information and associated assets maintained in the cloud computing environment in accordance with the cloud service customer's adopted procedures for labelling. [...]		Yes			Structured labelling of assets is applied.	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021		The cloud service provider should document and disclose any service functionality it provides allowing cloud service customers to classify and label their information and associated assets.		Yes			This is by design. The Viedoc platform is built for structured and labelled data management.	CPO
ISMAP	8.2.2.7.PB	The cloud service provider documents and discloses the service functions that allow cloud service customers to classify and label the information and related assets handled by the cloud service providers.		Yes				
ISO 27002: 2022	**A.5.14** *(NIST SP 800-53 AC-4, AC-17, AC-18, AC-19, AC-20, PE-17, SC-7, SC-8, SC-15)*	**Informaton transfer**	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes	To protect from privacy/confidentiality breach, which can have substantial impact on both finances and reputation, and to reassure customers of our ability to maintain data integrity.	Implemented.	COMSOP35 Office Infrastructure ITSOP20 Electronic Messaging COMSOP19 Information Classification MSA Appendix 4 – Data Processing Agreement COMTemp47 Data Processing Agreement	MIT CISO DPO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
NIST SP 800-53	SC-19	Voice Over Internet Protocol	The organization: a) Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b) Authorizes, monitors, and controls the use of VoIP within the information system.	Yes				
ISO 27002: 2022	**A.5.15** *(NIST SP 800-53 AC-3, AC-6)*	**Access control**	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and infromation security requirements.	Yes	A fundamental part of an effective ISMS. An extension of the principle of least privilege and aligned with the proper segregation of duties.	Implemented.	COMPOL03 Information Security Policy COMSOP20 Access Management	CISO MIT
ISO 27017: 2021		The cloud service customer's access control policy for the use of network services should specify requirements for user access to each separate cloud service that is used.		Yes				
NIST SP 800-53	AC-17(1)	Remote Access: Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.	Yes				
NIST SP 800-53	AC-18(1)	Wireless Access: Authentication and Encryption	Protect wireless access to the system using authentication of users, devices and encryption.	Yes				

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.5.16** *(NIST SP 800-53 AC-2, IA-2, IA-4, IA-5)*	**Identity management**	The full life cycle of identities should be managed.	Yes	To ensure unique identification of users and o enable proper access rights.	Implemented.	QSOff218 Role Description and Training Matrix COMSOP20 Access Management [ISMS document repository interactive introduction checklist] [ISMS document repository interactive termination checklist]	MQA MIT CFO
ISO 27017: 2021		To manage access to cloud services by a cloud service users, the cloud service provider should provide user registration and deregistration functions, and specifications for the use of these functions to the cloud service customer.		Yes		Implemented.	https://help.viedoc.net/c/331b7a/d36177/en/	CPO
ISO 27002: 2022	**A.5.17** *(NIST SP 800-53 IA-5)*	**Authentication information**	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication processes.	Yes	To ensure non authorized users do not gain access to initial authentication information.	Implemented.	COMPOL01 Code of Conduct COMTemp48 Employment agreement SE COMTemp49 Employment agreement JP COMTemp52 Employment agreement CN COMTemp53 Employment agreement US COMPOL08 Password Policy ITSOP23 Password Management	MIT
ISO 27017: 2021		The cloud service customer should verify that the cloud service provider's management procedure for allocating secret authentication information, such as passwords, meets the cloud service customer's requirements.		Yes		Implemented.	ITOff122 Colo, IaaS, SaaS provider qualification - Azure China ITOff155 Colo, IaaS, SaaS provider qualification - Azure Global	CISO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021		The cloud service provider should provide information on procedures for the management of the secret authentication information of the cloud service customer, including the procedures for allocating such information and for user authentication.		Yes		Implemented.	https://help.viedoc.net/c/331b7a/d36177/en/	CPO
ISO 27002: 2022	**A.5.18** *(NIST SP 800-53 AC-2)*	**Access rights**	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy and rules for access controls.	Yes	To be able to manage the whole user life-cycle and mitigate risk and incidents from acess rights misuse.	Implemented.	QSOff218 Role Description and Training Matrix COMSOP20 Access Management [ISMS document repository interactive introduction checklist] [ISMS document repository interactive termination checklist] COMPOL03 Information Security Policy [Access review tickets in LiveAgent]	MQA MIT CFO CISO
ISO 27017: 2021		The cloud service provider should provide functions for managing the access rights of the cloud service customer's cloud service users, and specifications for the use of these functions.		Yes		Implemented.	https://help.viedoc.net/c/331b7a/d36177/en/	CPO
ISO 27002: 2022	**A.5.19**	**Information security in supplier relationships**	Processes and procedures should be defined and implemented ti manage the information security risks associated with the use of supplier's products or services.	Yes	To ensure suppliers are aware of their responsibilities regarding our information assets.	Implemented.	COMSOP19 Information Classification COMSOP23 Supplier management ITOff183 Overview - IT infrastructure & system dependencies COMDOC37 Supplier Inventory [System classifications] [Vendor qualifications] [Vendor agreements]	CISO
ISO 27017: 2021		The cloud service customer should include the cloud service provider as a type of supplier in its information security policy for supplier relationships. This will help to mitigate risks associated with the cloud service provider's access to and management of the cloud service customer data.		Yes		Implemented.		

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISMAP	15.1.1.16.B		The cloud service provider evaluates the risk of information handled in the service provided by the cloud service provider being accessed or processed without the cloud service customer's intention as a result of the application of laws other than domestic laws to the information handled. Based on this evaluations, the cloud service provider selects an external contractor and, if necessary, specify the location where the contracted work will be performed and the governing law and jurisdiction as stipulated in the contract.	Yes		Implemented.		
ISO 27002: 2022	**A.5.20**	**Addressing information security within supplier agreements**	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Yes	To ensure suppliers are aware of their responsibilities regarding our information assets.	Implemented.	COMSOP19 Information Classification ITOff183 Overview - IT infrastructure & system dependencies COMDOC37 Supplier Inventory [System classifications] [Vendor qualifications] [Vendor agreements]	CISO
ISO 27017: 2021			The cloud service customer should confirm the information security roles and responsibilities relating to the cloud service, as described in the service agreement. [...]	Yes		Implemented.	Microsoft Online Services DPA - Processor and Controller Roles and Responsibilities	CISO
ISO 27017: 2021			The cloud service customer should confirm the information security roles and responsibilities relating to the cloud service, as described in the service agreement. [...] The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider will implement to ensure no misunderstanding between the cloud service provider and cloud service customer. [...]	Yes		Implemented.	MSA Appendix 2 – General Terms and Conditions MSA Appendix 3 – Service Level Agreement MSA Appendix 4 – Data Processing Agreement	DPO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISMAP	15.1.2.18. PB	The cloud service provider defines, as part of the agreement, appropriate information security measures to be implemented by the cloud service provider to avoid misunderstandings between the cloud service provider and cloud service customers.		Yes				
ISO 27002: 2022	**A.5.21**	**Managing information security in the ICT supply chain**	Processes and procedures should be defined and implemented to manage the infromation security risks associated with the ICT products and services supply chain.	Yes	To ensure all elements of the supply chain maintain the required level of security over our information assets.	Implemented.	COMSOP19 Information Classification ITOff183 Overview - IT infrastructure & system dependencies COMDOC37 Supplier Inventory [System classifications] [Vendor qualifications] [Vendor agreements]	CISO
ISO 27017: 2021		If a cloud service provider uses cloud services of peer cloud service providers, the cloud service provider should ensure information security levels to its own cloud service customers are maintained or exceeded. [...]		Yes		Implemented.		
ISO 27002: 2022	**A.5.22**	**Monitoring, review and change management of supplier services**	The organization sloudl regularly monitor, review , evaluate and manage change in supplier information security practices and service delivery.	Yes	To ensure supplier performance supports and enhances the provision of services to our customers in accordance and compliance with SLA:s. To ensure continuity of service to our customers with maintenance or enhancement of information security. We also want to stay informed of any improvements that can benefit us.	Implemented.	QSSOP13 QA Assessment of sub-contractors ITSOP13 Continuity Qualification ITPCG46 IT Report (working document not in ISMS document repository) COMSOP18 ISMS Manual COMSOP23 Supplier Management	MIT CISO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.5.23**	**Information security for use of Cloud services**	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	Yes	We are offer cloud base solution so this is esential for us and our ISMS.	Implemented.	COMPOL03 Information Security Policy COMSOP37 Cloud Services Security	CISO MIT
ISO 27002: 2022	**A.5.24**	**Information security incident management planning and preparation**	The organization should plan and prepare for managing information securty incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes	To ensure a quick, effective and orderly response to information security incidents.	Implemented.	COMPOL03 Information Security Policy COMSOP21 Information Security Incident Management	CISO
ISO 27017: 2021		The cloud service customer should verify the allocation of responsibilities for information security incident management and should ensure that it meets the requirements of the cloud service customer.		Yes		Implemented.	Microsoft Online Services DPA	
ISO 27017: 2021		As a part of the service specifications, the cloud service provider should define the allocation of information security incident management responsibilities and procedures between the cloud service customer and the cloud service provider. [...]		Yes		Implemented.	MSA Appendix 4 – Data Processing Agreement	DPO
ISO 27002: 2022	**A.5.25** *(NIST SP 800-53 AU-6, IR-4, SI-5)*	**Assessment and decision on information security events**	The organization should assess information security events and decide if they are to be categorized as information security incidents.	Yes	To ensure incidents are reported to and acted on by the correct personnel.	Implemented.	COMPOL03 Information Security Policy COMSOP21 Information Security Incident Management	CISO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.5.26** *(NIST SP 800-53 IR-4)*	**Response to information security incidents**	Information security incidents should be responded to in accordance with the documented procedures.	Yes	To ensure an appropriate response and follow through.	Implemented.	COMPOL03 Information Security Policy COMSOP21 Information Security Incident Management	CISO
ISO 27002: 2022	**A.5.27** *(NIST SP 800-53 IR-4)*	**Learning from information security incidents**	Knowledge gained from information security incidents should be used for strenghten and improve the information security controls.	Yes	Lessons learned are input to our ISMS and risk assessement and mitigation.	Implemented.	COMPOL03 Information Security Policy COMSOP21 Information Security Incident Management	CISO
NIST SP 800-53	IR-5	The organization tracks and documents information system security incidents.		Yes				
ISO 27002: 2022	**A.5.28** *(NIST SP 800-53 AU-12)*	**Collection of evidence**	The organization should establish and implement procedures for identification, collection, accquisition and preservation of evidence related to information security events.	Yes	Required for the proper investigation of incidents, events and weaknesses and the identification of root cause.	Implemented.	COMPOL03 Information Security Policy COMSOP21 Information Security Incident Management	CISO
ISO 27017: 2021		Cloud service customer: The cloud service customer and the cloud service provider should agree upon the procedures to respond to requests for potential digital evidence or other information from within the cloud computing environment.		Yes		Implemented.	Microsoft Online Services DPA	
ISO 27017: 2021		Cloud service provider: The cloud service customer and the cloud service provider should agree upon the procedures to respond to requests for potential digital evidence or other information from within the cloud computing environment.		Yes		Implemented.	MSA Appendix 4 – Data Processing Agreement	DPO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	A.5.29 *(NIST SP 800-53 CP-9)*	**Information security during disruption**	The organization should plan how to maintain information security at an appropriate level during disruption.	Yes	All part of good DR and BCP planning, testing, review and improvement, and expected of us as part of contractual agreements.	Implemented.	COMDOC02 Business Continuity Plan ITPCG40 Viedoc Disaster Precaution and Recovery Plan ITSOP08 Electronic Data Continuity [Test protocols]	CISO MIT
ISO 27002: 2022	A.5.30	**ICT readiness for business continuity**	ICT readiness should be planned, implemented, maintaned and tested based on business continuity objectives and ICT continuity requirements.	Yes	To ensure the availability of information and other associated assets during disruption.	Implemented	COMDOC02 Business Continuity Plan ITPCG40 Viedoc Disaster Precaution and Recovery Plan ITSOP08 Electronic Data Continuity [Test protocols]	CISO MIT
ISO 27002: 2022	A.5.31 *(NIST SP 800-53 SC-13)*	**Legal, statutory, regulatory and contractual requirements**	Legal, statutory, regulatory and contractual requirements relevant to information security and theo rganizationäs approach to meet these requirements should be identified, documented and kept up to date.	Yes	To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.	Implemented	COMSOP16 Identification of Legal, Contractual and Regulatory Requirements COMDOC19 List of Legal, Contractual and Regulatory Requirements	CISO
ISO 27017: 2021		The cloud service customer should consider the issue that relevant laws and regulations can be those of jurisdictions governing the cloud service provider, in addition to those governing the cloud service customer. [...]		Yes		Implemented	Microsoft Online Services DPA Data protection impact assessment	CISO
ISO 27017: 2021		The cloud service provider should inform the cloud service customer of the legal jurisdictions governing the cloud service.		Yes		Implemented	MSA Appendix 4 – Data Processing Agreement Data protection impact assessment	DPO
ISO 27017: 2021		The cloud service customer should verify that the set of cryptographic controls that apply to the use of a cloud service comply with relevant agreements, legislation and regulations.		Yes		Implemented.	ITPCG62 Infrastructure concept Azure	CISO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021			The cloud service provider should provide descriptions of the cryptographic controls implemented by the cloud service provider to the cloud service customer for reviewing compliance with applicable agreements, legislation and regulations.	Yes		Implemented.	https://help.viedoc.net/l/ccad2a/en/#toc-Informationsecurity12	CISO
ISO 27002: 2022	A.5.32	**Intellectual property rights**	The organization should implement appropriate procedures to protect intellectual property rights.	Yes	To ensure third party IP rights are not breached as that could have a negative impact on the business financially and reputationally.	Implemented	ITOff204 Approved Software DEVDoc05 Overview - Third party components & libraries ITOff182 Asset overview - Software subscriptions & licenses	MIT
ISO 27017: 2021			Installing commercially licensed software in a cloud service can cause a breach of the license terms for the software. [...]	Yes		Implemented.		
ISO 27017: 2021			The cloud service provider should establish a process for responding to intellectual property rights complaints.	Yes		Implemented.	Case-by-case	GC
ISO 27002: 2022	A.5.33 *(NIST SP 800-53 AC-3,AU-9, CP-9)*	**Protection of records**	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	To maintain the confidentiality, integrity and availability of business records.	Implemented	COMDOC24 Asset Inventory ITSOP08 Electronic Data Continuity QSSOP03 Document Control QSSOP10 Archiving	MQA
ISO 27017: 2021			The cloud service customer should request information from the cloud service provider about the protection of records gathered and stored by the cloud service provider that are relevant to the use of cloud services by the cloud service customer.	Yes		Implemented.	Microsoft Online Services DPA	DPO
ISO 27017: 2021			The cloud service provider should provide information to the cloud service customer about the protection of records that are gathered and stored by the cloud service provider relating to the use of cloud services by the cloud service customer.	Yes		Implemented.	MSA Appendix 4 – Data Processing Agreement	DPO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.5.34**	**Privacy and protection of PII**	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	Legal requirement, potential financial impact of breach and essential to maintaining our reputation in our marketplace.	Implemented	COMPOL02 Data Protection Policy QSSOP16 Data Protection Officer	DPO
ISO 27002: 2022	**A.5.35**	**Independent review of information security**	The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Yes	To demonstrate compliance with ISO 27001 via independent annual audit and certification which can be made available to interested parties.	Implemented	QSSOP01 Internal Audits Quality plan Audit plan ISO27001 cert Audit SOC2 report Audit	MQA CISO
ISO 27017: 2021		The cloud service customer should request documented evidence that the implementation of information security controls and guidelines for the cloud service is in line with any claims made by the cloud service provider.		Yes		Implemented.	https://www.microsoft.com/en-ww/trust-center	MQA
ISO 27017: 2021		The cloud service provider should provide documented evidence to the cloud service customer to substantiate its claim of implementing information security controls. [...]		Yes		Implemented.	https://help.viedoc.net/l/fe805c/en/ Additional evidence is provided in audits	MQA
ISO 27002: 2022	**A.5.36** *(NIST SP 800-53 CA-2)*	**Compliance with policies, rules and standards for information security**	Compliance with the organization's information security ploicy, topic-specific policies, rules and standards should be regularly reviewed.	Yes	An essential part of the ongoing management of an ISMS.	Implemented	QSSOP17 Viedoc Technologies eSOP System ITSOP13 Continuity Qualification DEVPOL01 Secure Development Policy [Latest penetration test executive summary available in ISMS document repository (PT)]	MIT CPO CISO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	A.5.37	**Documented operation procedures**	Operating procedures for information processing facilities should be documented and made available to personnel wgo need them.	Yes	To ensure consistent policies and procedures are followed and reduce risk of error in use.	Implemented	QSSOP03 Document Control ITSOP04 Back-office infrastructure COMSOP35 Office Infrastructure ITSOP08 Electronic Data Continuity ITSOP13 Continuity Qualification ITSOP18 Viedoc Deployment and Change Management	MQA
	A6 PEOPLE CONTROLS							
ISO 27002: 2022	A.6.1 *(NIST SP 800-53 PS-3)*	**Screening**	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	To ensure personnel are suitable for the roles for which they are being considered.	Implemented	COMTemp43 Checklist for Recruitment COMSOP13 Staff Recruitment, Introduction and Termination COMDOC08 Employee Handbook	CFO
ISO 27002: 2022	A.6.2	**Terms and conditions of employment**	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	Yes	To ensure all personnel are contractually obliged to follow policies and procedures and thereby act in the best interest of the company.	Implemented	COMPOL01 Code of Conduct COMTemp48 Employment agreement SE COMTemp49 Employment agreement JP COMTemp52 Employment agreement CN COMTemp53 Employment agreement US	CFO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.6.3** *(NIST SP 800-53 AT-2, AT-3, IR-2)*	**Information security awareness, education and training**	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job functions.	Yes	To ensure all personnel have the necessary knowledge to follow policies and procedures thereby act in the best interest of the company.	Implemented	COMPOL03 Information Security Policy COMSOP13 Staff Recruitment, Introduction and Termination COMSOP18 ISMS Manual COMSOP31 Pre- and Onboarding QSSOP15 Staff training [ISMS document repository interactive introduction checklist] [NanoLearning]	CISO
ISO 27017: 2021		The cloud service customer should add the following items to awareness, education and training programmes for cloud service business managers, cloud service administrators, cloud service integrators and cloud service users, including relevant employees and contractors: [...]		Yes				
ISO 27017: 2021		The cloud service provider should provide awareness, education and training for employees, and request contractors to do the same, concerning the appropriate handling of cloud service customer data and cloud service derived data. [...]		Yes				
ISMAP	7.2.2.19.PB	Cloud service providers provide education and training to raise awareness among employees regarding the proper handling of cloud service customer data and cloud service derived data, and require contract parties to do the same.		Yes				
NIST SP 800-53	AT-2(2)	Security Awareness Training: Insider Threat	Provide literacy training on recognizing and reporting potential indicators of insider threat.	Yes				

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.6.4**	**Disciplinary process**	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have commited an information security policy violation.	Yes	To ensure all personnel are aware of the consequences of not following policies and procedures.	Implemented	COMPOL01 Code of Conduct COMTemp48 Employment agreement SE COMTemp49 Employment agreement JP COMTemp52 Employment agreement CN COMTemp53 Employment agreement US COMPOL15 Disciplinary Process	CFO
ISO 27002: 2022	**A.6.5** *(NIST SP 800-53 PS-4, PS-5)*	**Responsibilities after termination or change of employment**	Information security responsibilites and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and othet interested parties.	Yes	To ensure all personnel are aware of their ongoing contractual responsibilities post termination and to ensure equipment is collected and access removed or updated properly.	Implemented	COMSOP32 Employee Offboarding COMPOL01 Code of Conduct COMTemp48 Employment agreement SE COMTemp49 Employment agreement JP COMTemp52 Employment agreement CN COMTemp53 Employment agreement US [ISMS document repository interactive termination checklist]	CFO
ISO 27002: 2022	**A.6.6**	**Confidentiality or non-disclosure agreements**	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other interested parties.	Yes	To protect from privacy/confidentiality breach, which can have substantial impact on both finances and reputation, and to reassure customers of our ability to maintain data integrity.	Implemented	QSSOP03 Document Control COMTemp05 Secrecy Agreement English SMTemp14 NDA template [Typically also covered by A.13.2.2] (SMSOP01 Customer Contracts)	GC

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.6.7** *(NIST SP 800-53 AC-3, AC-17, PE-17)*	**Remote working**	Security measures should be implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organizations premises.	Yes	We consider all work to be telework as we have no in-office-perimeter production equipment, which makes it of utter importance to only use the protected equipment supplied by the company for work.	Implemented	COMPOL03 Information Security Policy COMSOP35 Office Infrastructure	MIT
ISO 27017: 2021	CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider. [...] Customer: Define procedure/policy and inform Provider: Document/communicate capabilities/roles/responsibilities	Yes	To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management.	Implemented	COMPOL03 Information Security Policy QSOff218 Role Description and Training Matrix COMSOP20 Access Management	CISO
				Yes		Implemented	▪ https://help.viedoc.net/c/331b7a/d36177/en/#toc-AboutrolesinViedoc ▪ https://help.viedoc.net/l/ccad2a/en/#toc-Informationsecurity12 ▪ https://help.viedoc.net/l/b236e3/en/#toc-Privileges4	CPO
ISO 27002: 2022	**A.6.8** *(NIST SP 800-53 AU-6,*	**Information security event reporting**	The organization should provide a mechanism for personnel to report observed or suspected infromation security events through appropriate channels in a timely manner.	Yes	To ensure incidents are reported at the correct level in a timely fashion. To help prevent weaknesses becoming incidents.	Implemented	COMPOL03 Information Security Policy	CISO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021	*IR-6,* *SI-2)*	The cloud service customer should request information from the cloud service provider about the mechanisms for: […]		Yes		Implemented	Microsoft Online Services DPA	
ISO 27017: 2021		The cloud service provider should provide mechanisms for: […]		Yes		Implemented	MSA Appendix 4 – Data Processing Agreement	DPO
	A7 PHYSICAL CONTROLS							
ISO 27002: 2022	**A.7.1** *(NIST SP 800-53 PE-3)*	**Physical security perimeters**	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA).	Implemented	COMSOP35 Office Infrastructure ITSOP04 Back-office infrastructure ITPCG40 Viedoc Disaster Precaution and Recovery Plan Microsoft Azure ISO 27001 SOA See Appendix A – Security Measures for Microsoft Online Services DPA. More details: https://servicetrust.microsoft.com/ViewPage/datacentercontrols https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.7.2** *(NIST SP 800-53 PE-2, PE-4, PE-5, PE-3)*	**Physical entry**	Secure areas should be protected by appropriate entry controls and access points.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA).	Implemented.	COMSOP35 Office Infrastructure ITSOP04 Back-office infrastructure ITPCG40 Viedoc Disaster Precaution and Recovery Plan Microsoft Azure ISO 27001 SOA See Appendix A – Security Measures for Microsoft Online Services DPA. More details: https://servicetrust.microsoft.com/ViewPage/datacentercontrols https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security	MIT
ISO 27002: 2022	**A.7.3** *(NIST SP 800-53 PE-5, PE-3)*	**Securing offices, rooms and facilities**	Physical security for offices, rooms and facilities should be designed and implemented.	Yes	Work from employee client devices are always considered teleworking, however our offices can be used to store such equipment without supervision.	Implemented.	COMSOP35 Office Infrastructure	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	A.7.4	**Physical security monitoring**	Premises should be continuosly monitored for unauthorized physical access.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA). Viedoc is responsible for monitoring physical security n our offices.	Implemented.	COMSOP35 Office Infrastructure ITSOP04 Back-office infrastructure ITPCG40 Viedoc Disaster Precaution and Recovery Plan Microsoft Azure ISO 27001 SOA See Appendix A – Security Measures for Microsoft Online Services DPA. More details: https://servicetrust.microsoft.com/ViewPage/datacentercontrols https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security	MIT
ISO 27002: 2022	A.7.5	**Protecting against physical and environmental threats**	Protection against physical and enviromental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA).	Implemented.	COMSOP35 Office Infrastructure ITSOP04 Back-office infrastructure ITPCG40 Viedoc Disaster Precaution and Recovery Plan Microsoft Azure ISO 27001 SOA See Appendix A – Security Measures for Microsoft Online Services DPA. More details: https://servicetrust.microsoft.com/ViewPage/datacentercontrols https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	A.7.6	**Working in secure areas**	Security measures for working in secure areas should be designed and implemented.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA).	Implemented.	COMSOP35 Office Infrastructure ITSOP04 Back-office infrastructure ITPCG40 Viedoc Disaster Precaution and Recovery Plan Microsoft Azure ISO 27001 SOA See Appendix A – Security Measures for Microsoft Online Services DPA. More details: https://servicetrust.microsoft.com/ViewPage/datacentercontrols https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security	MIT
ISO 27002: 2022	A.7.7	**Clear desk and clear screeen**	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Yes	To reduce the risk of unauthorized access.	Implemented.	COMPOL03 Information Security Policy	CISO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	A.7.8	**Equipment siting and protection**	Equipment should be sited securely and protected.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA).	Implemented.	COMSOP35 Office Infrastructure ITSOP04 Back-office infrastructure ITPCG40 Viedoc Disaster Precaution and Recovery Plan Microsoft Azure ISO 27001 SOA See Appendix A – Security Measures for Microsoft Online Services DPA. More details: https://servicetrust.microsoft.com/ViewPage/datacentercontrols https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security	MIT
ISO 27002: 2022	A.7.9 *(NIST SP 800-53 AC-19, AC-20, MP-5, PE-17)*	**Security of assets off-premises**	Off-site assets should be protected.	Yes	To ensure confidentiality is maintained.	Implemented.	COMPOL03 Information Security Policy COMSOP35 Office Infrastructure ITSOP21 Client Installation and Validation ITPCG48 Asset Inventory (working document not in ISMS document repository)	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.7.10** *(NIST SP 800-53 MP-2, MP-4, MP-6, MP-7)*	**Storage media**	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	To ensure that accidental disclosure or malicious misappropriation of information on removable media is prevented.	Implemented.	COMSOP35 Office Infrastructure ITSOP12 Electronic Data Destruction COMSOP25 Document Control ITSOP12 Electronic Data Destruction	MIT
NIST SP 800-53	AC-20(2)	Use Of External Information Systems: Portable Storage Devices – Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using organization-defined restrictions.	Yes				
NIST SP 800-53	MP-7(1)	Media Use: Prohibit Use Without Owner	The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	Yes				
ISO 27002: 2022	**A.7.11**	**Supporting utilities**	Information processing utilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA).	Implemented.	Microsoft Azure ISO 27001 SOA See Appendix A – Security Measures for Microsoft Online Services DPA. More details: https://servicetrust.microsoft.com/ViewPage/datacentercontrols https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.7.12** *(NIST SP 800-53 PE-4)*	**Cabling security**	Cables carrying power , data or supporting information services should be protected from interception, interference or damage.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA).	Implemented.	Microsoft Azure ISO 27001 SOA	MIT
ISO 27002: 2022	**A.7.13** *(NIST SP 800-53 MA-2)*	**Equipment maintenance**	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	The physical infrastructure used to process sensitive and/or critical information is outsourced to Microsoft and 21ViaNet (in scope and applicable according to ISO 27001 SOA).	Implemented.	COMSOP35 Office Infrastructure Microsoft Azure ISO 27001 SOA	MIT
ISO 27002: 2022	**A.7.14** *(NIST SP 800-53 MP-6)*	**Secure disposal or re-use of equipment**	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	To ensure that accidental disclosure of information on asset disposals is prevented.	Implemented.	ITSOP12 Electronic Data Destruction	MIT
ISO 27017: 2021		The cloud service customer should request confirmation that the cloud service provider has the policies and procedures for secure disposal or reuse of resources.		Yes				
ISO 27017: 2021		The cloud service provider should ensure that arrangements are made for the secure disposal or reuse of resources (e.g.,equipment, data storage, files, memory) in a timely manner.		Yes				
	A8 TECHNOLOGICAL CONTROLS							

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.8.1** *(NIST SP 800-53 AC-11, AC-17, AC-18, AC-19)*	**User endpoint devices**	Information stored on, processed by or accessible via user endpoint devices should be protected.	Yes	We supply employees with endpoint devices, and this is what must be used to avoid risks related to BYOD.	Implemented.	COMPOL03 Information Security Policy COMSOP35 Office Infrastructure	MIT
ISO 27002: 2022	**A.8.2** *(NIST SP 800-53 AC-2,AC-6, CM-5)*	**Privileged access rights**	The allocation and use of privileged access rights should be restricted and managed.	Yes	To ensure privileged access rights are assigned according to the principle of least privilege and with restrictions of how they are used.	Implemented.	COMSOP20 Access Management	MIT
ISO 27017: 2021			The cloud service customer should use sufficient authentication techniques (e.g.,multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks.	Yes		Implemented.	COMPOL03 Information Security Policy	CISO
ISO 27017: 2021			The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risks.	Yes		Implemented.	https://help.viedoc.net/c/331b7a/6870ff/en/#toc-Twofactorauthentication6 https://help.viedoc.net/c/331b7a/6bea8e/en/#toc-Securitysettings15 https://help.viedoc.net/c/331b7a/3d30ad/en/	CPO
ISMAP	9.2.3.11.PB		Depending on the identified risks, cloud service providers provide sufficiently strong authentication technologies for administrator authentication of cloud service customers that are tailored to the management capabilities of the cloud service	Yes		Implemented.		

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.8.3** *(NIST SP 800-53 AC-3)*	**Information access restriction**	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Yes	To prevent accidental or malicious unauthorized access to systems and applications.	Implemented.	COMPOL03 Information Security Policy COMSOP20 Access Management	MIT
ISO 27017: 2021			The cloud service customer should ensure that access to information in the cloud service can be restricted in accordance with its access control policy and that such restrictions are realized. This includes restricting access to cloud services, cloud service functions, and cloud service customer data maintained in the service.	Yes		Implemented.		
ISO 27017: 2021			The cloud service provider should provide access controls that allow the cloud service customer to restrict access to its cloud services, its cloud service functions and the cloud service customer data maintained in the service.	Yes		Implemented.	https://help.viedoc.net/c/331b7a/d36177/en/https://help.viedoc.net/c/e311e6/bac6fa/en/	CPO
ISO 27002: 2022	**A.8.4** *(NIST SP 800-53 AC-3,AC-6, CM-5)*	**Access to source code**	Read and write access to source code, development tools and software libraries should be appropriately managed.	Yes	Source code is one of our most valuable assets, and if in the wrong hands can be used to harm us in several ways.	Implemented.	COMPOL03 Information Security Policy COMSOP20 Access Management	CTO
ISO 27002: 2022	**A.8.5** *(NIST SP 800-53 AC-7, AC-8, IA-6)*	**Secure authentication**	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	To prevent accidental or malicious unauthorized access to systems and applications.	Implemented.	COMPOL03 Information Security Policy COMPOL08 Password Policy COMSOP19 Information Classification	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
NIST SP 800-53	IA-2(1)	Identification And Authentication (Organizational Users): Network Access To Privileged Accounts	The information system implements multifactor authentication for network access to privileged accounts.	Yes				
NIST SP 800-53	IA-2(2)	Identification And Authentication (Organizational Users): Network Access To Non-Privileged Accounts	The information system implements multifactor authentication for network access to non-privileged accounts.	Yes				
NIST SP 800-53	IA-2(3)	Identification And Authentication (Organizational Users): Local Access To Privileged Accounts	The information system implements multifactor authentication for local access to privileged accounts.	Yes				
NIST SP 800-53	IA-2(8)	Identification And Authentication (Organizational Users): Network Access To Privileged Accounts –	The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	Yes				

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
		Replay Resistant						
NIST SP 800-53	IA-2(9)	Identification And Authentication (Organizational Users): Network Access To Non-Privileged Accounts – Replay Resistant	The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	Yes				
NIST SP 800-53	IA-5(1)	Authenticator Management: Password-Based Authentication	The information system, for password-based authentication: [...] a)	Yes				
ISO 27002: 2022	**A.8.6**	**Capacity management**	The use of resources shoud be monitored and adjusted in line with current and expected capacity requirements.	Yes	To ensure availability of systems is not compromised due to lack of resources.	Implemented.	ITSOP04 Back-office infrastructure ITSOP13 Continuity Qualification	MIT
ISO 27017: 2021		The cloud service customer should ensure that the agreed capacity provided by the cloud service meets the cloud service customer's requirements. [...]		Yes				

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021		The cloud service provider should monitor the total resource capacity to prevent information security incidents caused by resource shortages.		Yes				
ISO 27002: 2022	**A.8.7** *(NIST SP 800-53 AT-2,SI-3)*	**Protection against malware**	Protection against malware should be implemented and supported by appropriate awareness.	Yes	Malware is an increasing threat and protection against it an essential part of running a business heavily dependent on IT systems.	Implemented.	ITSOP04 Back-office infrastructure COMSOP35 Office Infrastructure ITSOP13 Continuity Qualification	MIT
ISO 27002: 2022	**A.8.8** *(NIST SP 800-53 RA-3, RA-5, SI-2, CA-2)*	**Management of technical vulnerabilties**	Information about technical vulnerabilties of information systems in use should be obtained, the organization's exposure to such vulnerabilties should be evaluated and appropriate measures should be taken.	Yes	To ensure we do what we can to protect against zero-day vulnerabilities.	Implemented.	ITSOP04 Back-office infrastructure ITSOP13 Continuity Qualification ITSOP18 Viedoc Deployment and Change Management COMSOP23 Supplier Management [Latest penetration test executive summary available in ISMS document repository (PT)]	MIT
ISO 27017: 2021		The cloud service customer should request information from the cloud service provider about the management of technical vulnerabilities that can affect the cloud services provided.		Yes				
ISO 27017: 2021		The cloud service provider should make available to the cloud service customer information about the management of technical vulnerabilities that can affect the cloud services provided.		Yes		Implemented.	https://status.viedoc.com/ Release notes - Known limitations	CPO
NIST SP 800-53	RA-5(1)	Vulnerability Scanning: Update Tool Capability	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	Yes		Implemented.	ITSOP13 Continuity Qualification	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.8.9**	**Configuration management**	Configurations, including security configurations, of hardware, software, and networks should be established documented, implemented, monitored, and reviewed.	Yes	To ensure we maintain secure and consistent configuration in all parts of our infrastructure. We are moving towards IaC with predifened configurations.	Implemented.	ITSOP04 Back-office infrastructure ITSOP21 Client installation and validation SOP	MIT
ISO 27002: 2022	**A.8.10**	**Information deletion**	Information stored in information systems, devices, or in any other storage media should be deleted when no longer required.	Yes	To prevent unecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for informationd deletion. We are responsible only for data that Viedoc is stated as contoller, all customer data is customer responsibility.	Implemented.	COMPOL02 Data Protection Policy COMDOC58 Data Protection Impact Assessment SMTemp06 Appendix 4 - DPA COMDOC117-01 Register Of Processing Activities ITOff60 Viedoc Security - Technical and organisational measures ITSOP12 Electronic Data Destruction	DPO CISO MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.8.11**	**Data masking**	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes	To limit the exposure of sensitive data including PII. We are responsible only for data that Viedoc is stated as contoller, all customer data is customer responsibility and data related to clinical trial sibjects is pseudonymized and encrypted in the system.	Implemented.	COMPOL02 Data Protection Policy COMDOC58 Data Protection Impact Assessment SMTemp06 Appendix 4 - DPA Data masking: https://help.viedoc.net/c/47e0ad/a80c3c/en/#toc-Maskingofsensitivedata28 Encryption details: https://help.viedoc.net/l/ccad2a/en/ TOff60 Viedoc Security - Technical and organisational measures	DPO CPO CISO
ISO 27002: 2022	**A.8.12**	**Data leakage prevention**	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes	To detect and prevent unauthorized disclosure and extraction of information by individuals or systems.	Implemented.	COMSOP35 Office Infrastructure COMSOP19 Information classification ITSOP08 Electronic Data Continuity COMSOP20 Access Management COMSOP25 Document Control	MIT
ISO 27002: 2022	**A.8.13** *(NIST SP*	**Information backup**	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	Even if all systems are redundant and never fail, we might need to be able to “step back in time” to recover from information integrity issues.	Implemented.	ITSOP08 Electronic Data Continuity	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021	*800-53 CP-9)*	Where the cloud service provider provides backup capability as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider. [...]		Yes		Implemented.	Microsoft Service Level Agreements (SLA) for Online Services ITOff122 Colo, IaaS, SaaS provider qualification - Azure China ITOff155 Colo, IaaS, SaaS provider qualification - Azure Global ITSOP08 Electronic Data Continuity	
ISO 27017: 2021		The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. [...]		Yes		Implemented.	MSA Appendix 3 – Service Level Agreement https://help.viedoc.net/l/ccad2a/en/#toc-Backup33	
ISO 27002: 2022	**A.8.14**	**Redundancy of information processing facilities**	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Yes	We have successfully employed this approach to availability and continuity since we started the business in 2003. We believe it has strongly contributed to our great track-record of high availability.	Implemented.	ITSOP04 Back-office infrastructure ITSOP13 Continuity Qualification ITSOP08 Electronic Data Continuity	MIT
ISO 27002: 2022	**A.8.15** *(NIST SP 800-53 AU-3, AU-6,*	**Logging**	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Yes	To ensure evidence of activity and events is available to assist in investigations and monitoring.	Implemented.	ITSOP04 Back-office infrastructure ITSOP13 Continuity Qualification ITOff252 Monitoring Of Security Events	MIT
ISO 27017: 2021		If a privileged operation is delegated to the cloud service customer, the operation and performance of those operations should be logged. [...]		Yes				

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021	*AU-9, AU-11, AU-12)*	The cloud service provider should provide logging capabilities to the cloud service customer.		Yes		Implemented.	https://status.viedoc.com/ https://help.viedoc.net/c/94d6f0/a80c3c/en/ https://help.viedoc.net/c/47e0ad/e28906/en/#toc-Userlogs8 https://help.viedoc.net/c/47e0ad/b67c56/en/#toc-Includehistory11 https://help.viedoc.net/c/331b7a/d36177/en/#toc-Usersettings13	CPO
ISO 27002: 2022	**A.8.16**	**Monitoring activities**	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	To ensure all relevant security events are captured and corelated so appropriate alarm and notification is raised.	Implemented.	ITOff252 Monitoring Of Security Events	MIT
ISO 27002: 2022	**A.8.17** *(NIST SP 800-53 AU-8)*	**Clock synchronization**	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Yes	To ensure evidence of activity and events is available to assist in investigations and monitoring.	Implemented.	ITSOP04 Back-office infrastructure	MIT
ISO 27017: 2021		The cloud service customer should request information about the clock synchronization used for the cloud service provider's systems.		Yes				
ISO 27017: 2021		The cloud service provider should provide information to the cloud service customer regarding the clock used by the cloud service provider's systems, and information about how the cloud service customer can synchronize local clocks with the cloud service clock.		Yes			https://help.viedoc.net/c/47e0ad/a559c4/en/#C (the definition of UTC)	CPO
ISO 27002: 2022	**A.8.18** *(NIST SP 800-53*	**Use of privileged utility programs**	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Yes	To prevent accidental or malicious unauthorized access to systems and applications.	Implemented.	COMPOL03 Information Security Policy COMSOP20 Access Management	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021	*AC-3, AC-6)*		Where the use of utility programs is permitted, the cloud service customer should identify the utility programs to be used in its cloud computing environment and ensure that they do not interfere with the controls of the cloud service.	Yes				
ISO 27017: 2021			The cloud service provider should identify the requirements for any utility programs used within the cloud service. The cloud service provider should ensure that any use of utility programs capable of bypassing normal operating or security procedures is strictly limited to authorized personnel, and that the use of such programs is reviewed and audited regularly.	Yes			The Viedoc platform permits the client to run custom JavaScript server-side, but this is sandboxed and have no privileged access by design. Uploaded files are never executed on server-side.	CPO
ISO 27002: 2022	**A.8.19** *(NIST SP 800-53 CM-5, CM-7, CM-11)*	**Installation of software on operational systems**	Procedures and measures should be implemented to securely manage software installation on operational systems.	Yes	To ensure that the confidentiality, integrity and availability of information held on operational systems is not compromised.	Implemented.	ITSOP04 Back-office infrastructure COMSOP35 Office Infrastructure ITSOP18 Viedoc Deployment and Change Management ITSOP21 Client Installation and Validation ITSOP27 Qualification and approval of software ITOff204 Approved Software	MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.8.20** *(NIST SP 800-53 AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10)*	**Networks security**	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Yes	To prevent unauthorized accidental or malicious internal or remote connections to our networks.	Implemented.	ITSOP04 Back-office infrastructure ITPCG62 Infrastructure concept Azure	MIT
ISO 27002: 2022	**A.8.21**	**Security of network services**	Security mechanisms, service levels and service requirements od network services should be identified, implemented and monitored.	Yes	To ensure appropriate controls are in place over network traffic.	Implemented.	ITSOP04 Back-office infrastructure ITPCG51 Viedoc Network Overview ITPCG62 Infrastructure concept Azure ITOff122 Colo, IaaS, SaaS provider qualification - Azure China ITOff155 Colo, IaaS, SaaS provider qualification - Azure Global	MIT
ISO 27002: 2022	**A.8.22** *(NIST SP 800-53 AC-4,SC-7)*	**Segregation of networks**	Groups of information services, user and information systems shouldbe separated in the organization's networks.	Yes	Groups of information services, users and information systems shall be segregated on networks.	Implemented.	ITSOP04 Back-office infrastructure ITPCG62 Infrastructure concept Azure	MIT
ISO 27017: 2021		The cloud service customer should define its requirements for segregating networks to achieve tenant isolation in the shared environment of a cloud service and verify that the cloud service provider meets those requirements.		Yes				
ISO 27017: 2021		The cloud service provider should enforce segregation of network access for the following cases: […]		Yes		Implemented.	COMPOL03 Information Security Policy By application design	CTO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.8.23**	**Web filtering**	Access to external websites should be managed to reduce exposure to malicious content.	Yes	To ensure that we protect systems from being infected by malware and to prevent access to unauthorized web resources.	Implemented.	COMSOP35 Office Infrastructure	MIT
ISO 27002: 2022	**A.8.24** *(NIST SP 800-53 SC-12, SC-13)*	**Use of cryptography**	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Yes	We require encryption at some level for all information, both in rest and in transit, to ensure confidentiality is maintained for confidential information.	Implemented.	COMPOL03 Information Security Policy ITSOP20 Electronic Messaging COMSOP19 Information Classification COMSOP35 Office Infrastructure ITPCG62 Infrastructure concept Azure ITSOP23 Password Management	CISO MIT
ISO 27017: 2021		The cloud service customer should implement cryptographic controls for its use of cloud services if justified by the risk analysis. [...]		Yes			https://help.viedoc.net/l/ccad2a/en/#toc-Informationsecurity12	CPO
ISO 27017: 2021		The cloud service provider should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the information it processes. [...]		Yes				
ISO 27017: 2021		The cloud service customer should identify the cryptographic keys for each cloud service, and implement procedures for key management.		Yes			COMPOL03 Information Security Policy ITSOP23 Password Management	CISO MIT

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.8.25**	**Secure development life cycle**	Rules for secure development of software and systems should be established and applied.	Yes	To ensure the development of software and systems is carried out in a consistent and secure manner according to best practices.	Implemented.	DEVPOL01 Secure Development Policy DEVOTH01 Programming Guidelines	CTO
ISO 27017: 2021		The cloud service customer should request information from the cloud service provider about the cloud service provider's use of secure development procedures and practices		Yes			https://docs.microsoft.com/en-us/windows/security/threat-protection/msft-security-dev-lifecycle	CISO
ISO 27017: 2021		The cloud service provider should provide information about its use of secure development procedures and practices to the extent compatible with its policy for disclosure.		Yes			DEVPOL01 Secure Development Policy DEVOTH01 Programming Guidelines https://help.viedoc.net/l/ccad2a/en/	MQA CPO
ISO 27002: 2022	**A.8.26** (NIST SP 800-53 AC-3, AC-4, AC-17, SC-7, SC-8, SC-13)	**Application security requirements**	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Yes	Viedoc is exposed and delivered over public networks, which means we need to protect it from all kinds of public and anonymous threats. Viedoc data entry, and especially sensitive one-time activities like randomization, must be protected in accordance with this control to ensure data integrity.	Implemented.	COMPOL03 Information Security Policy DEVPOL01 Secure Development Policy ITSOP04 Back-office infrastructure	CTO MIT
ISO 27002: 2022	**A.8.27** *(NIST SP 800-53 SA-8)*	**Secure system architecture and engineering principles**	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Yes	To ensure the development of software and systems is carried out in a consistent and secure manner according to best practices.	Implemented.	DEVPOL01 Secure Development Policy	CTO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27002: 2022	**A.8.28**	**Secure coding**	Secure coding principles should be applied to software development.	Yes	To ensure that the code is written securely thereby reducing the number of potential information security vulnerabilties in the software.	Implemented.	DEVPOL01 Secure Development Policy	CTO
ISO 27002: 2022	**A.8.29** *(NIST SP 800-53 CA-2)*	**Security testing in development and acceptance**	Security testing processes should be defined and implemented in the development life cycle.	Yes	To ensure each release of, or modification to, the software makes it no less secure than the previous version.	Implemented.	DEVSOP06 Testing DEVPOL01 Secure Development Policy PMSOP04 Performance Qualification	CPO
ISO 27002: 2022	**A.8.30**	**Outsourced development**	The organization should direct, monitor and review the activities related to outsourced system development.	Yes	To ensure outsourced development of software and systems is carried out in accordance with our internal procedures and policies, and in a consistent and secure manner.	Implemented.	DEVSOP11 Outsourced Development	CTO
ISO 27002: 2022	**A.8.31** *(NIST SP 800-53 CM-5)*	**Separation fo development, test and production environments**	Development, testing and production environments should be separated and secured.	Yes	To protect the integrity of the operational environment and thereby maintain the confidentiality, integrity and availability of information assets within it.	Implemented.	COMPOL03 Information Security Policy DEVSOP01 Product Development Process ITSOP18 Viedoc Deployment and Change Management DEVSOP07 Azure DevOps Workflow COMSOP35 Office Infrastructure ITSOP21 Client Installation and Validation ITOff204 Approved Software	CTO

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
ISO 27017: 2021	CLD.12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored. [...]	Yes	To ensure correct and secure operations of information processing facilities.	Implemented.	ITSOP18 Viedoc Deployment and Change Management ITSOP13 Continuity Qualification COMSOP23 Supplier Management COMSOP20 Access Management	MIT
			Customer: Document procedures for critical operations Provider: Provide documentation about the critical operations	Yes		Implemented.	https://help.viedoc.net/c/331b7a/dbaf67/en/	CPO
ISO 27002: 2022	**A.8.32** *(NIST SP 800-53 CM-3, CM-4, CM-5, SI-2)*	**Change management**	Changes to information processing facilities and information systems should be subject to change management procedures.	Yes	In order to prevent accidental or malicious changes, and to ensure authorized changes do not introduce risks or vulnerabilities.	Implemented.	COMPOL04 Quality Policy ITSOP04 Back-office infrastructure ITSOP13 Continuity Qualification ITSOP18 Viedoc Deployment and Change Management QSSOP17 Viedoc Technologies eSOP System DEVSOP03 Product Lifecycle Management DEVSOP01 Product Development Process PMSOP02 Change Control Board PMSOP01 Product Release Process PMSOP03 System Retirement Process	MQA MIT CTO
ISO 27017: 2021		The cloud service customer's change management process should take into account the impact of any changes made by the cloud service provider.		Yes		Implemented.	ITSOP13 Continuity Qualification COMSOP23 Supplier Management	MIT
ISO 27017: 2021		The cloud service provider should provide the cloud service customer with information regarding changes to		Yes		Implemented.	COMPOL03 Information Security Policy https://status.viedoc.com/	MIT CPO MPS

Source	Control ID	Control name	Description	Applicable	Justification	Status	Documentation	Responsible
		the cloud service that could adversely affect the cloud service. [...]					https://www.viedoc.com/support/service-status/	
ISMAP	12.1.2.11. PB	The cloud service provider provides cloud service customers with information about changes in cloud services that can adversely affect the information security of cloud service customers		Yes		Implemented.		
ISO 27002: 2022	**A.8.33**	**Test information**	Test information should be appropriately selected, protected and managed.	Yes	We do not use production data for testing purposes. We do not think it's possible to securely anonymize production data for it to be used in testing and we now have contractual obligations that prevent us from developing that approach.	Implemented.	DEVSOP06 Testing VIESOP19 Validation of Study Build	CTO MPS
ISO 27002: 2022	**A.8.34**	**Protection of information systems during audit testing.**	Audit tests and other assurance activities involving operational systems should be planned and agreed between the tester and appropriate management.	Yes	To ensure all necessary audits are carried out, but with minimum disruption to business.	Implemented.	QSSOP05 Inspections and Audits	MQA