Statement of Applicability

Company details CoreMedia GmbH, Rödingsmarkt 9 20459 Hamburg (Germany) - 5th floor
CoreMedia S.A, Rua do Visconde de Bóbeda 70,4000-108 Porto (Portugal)

Scope Information security related to the end-to-end process for creating, delivering and supporting the cloud based CoreMedia Digital Experience Platform.

Purpose: This document contains the Statement of Applicability, based on the ISO 27002:2022 control objectives.

Agreed by: Roy Smeets

History: V1.3



L = Legal/regulatory;
R = Risk driven;
BP = Best practice / Company Req;
PCR - Partner Contractual Req;
CCR = Customer Contractual Req

CONFIDENTIAL

ISO Ref.	ISO Control	ISO Control Description	Applicable ?	Justification						Implemented
				Reason to include					Reason to exclude	
				L	R	BP	PCR	CCR		
A.5	**Organizational controls**									
5.1	Policies for information security	Information security policy and topic-specific policies shall 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	No	Yes	Yes	No	No		Yes

5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes	No	Yes	Yes	No	No		Yes
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Yes	No	Yes	No	No	No		Yes
5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes	No	Yes	Yes	No	No		Yes
5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Yes	No	Yes	Yes	No	No		Yes
5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	No	Yes	Yes	No	No		Yes
5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes	No	Yes	Yes	No	No		Partially

CONFIDENTIAL

5.8	Information security in project management	Information security shall be integrated into project management.	Yes	No	Yes	Yes	No	No		Yes
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes	No	Yes	Yes	No	No		Yes
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Yes	No	Yes	No	No	No		Yes
5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization'	Yes	No	Yes	Yes	No	No		Yes
5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Yes	No	Yes	No	No	No		Yes
5.13	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 organization.	Yes	No	Yes	No	No	No		Yes

CONFIDENTIAL

5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes	No	Yes	No	No	No		Yes
5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Yes	No	Yes	No	No	No		Yes
5.16	Identity management	The full life cycle of identities shall be managed.	Yes	No	Yes	Yes	No	No		Yes
5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Yes	No	Yes	No	No	No		Yes

CONFIDENTIAL

5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes	No	Yes	No	No	No		Yes
5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes	No	Yes	Yes	No	No		Yes
5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Yes	No	Yes	Yes	No	No		Yes
5.21	Managing information security in the ICT supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	No	Yes	Yes	No	No		Yes
5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Yes	No	Yes	Yes	No	No		Yes
5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes	No	Yes	No	No	No		Yes
5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Yes	No	Yes	Yes	No	No		Yes
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	No	Yes	Yes	No	No		Yes
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Yes	No	Yes	Yes	No	No		Yes
5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	No	Yes	Yes	No	No		Yes
5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes	No	Yes	Yes	No	No		Yes
5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	No	Yes	No	No	No		Yes

CONFIDENTIAL

5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes	No	Yes	Yes	No	No		Yes
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Yes	Yes	No	Yes	No	No		Yes
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	No	Yes	Yes	No	No		Yes
5.34	Privacy and protection of PII	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	Yes	No	Yes	No	No		Yes
5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Yes	No	Yes	Yes	No	No		Yes
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes	No	Yes	Yes	No	No		Yes
A.6	**People Controls**									
6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an 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	No	Yes	No	No	No		Yes
6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes	Yes	Yes	No	No	No		Yes
6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall 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 function.	Yes	No	Yes	No	No	No		Yes
6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes	No	Yes	No	No	No		Yes
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	Yes	Yes	Yes	No	No		Yes
6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes	No	Yes	Yes	No	No		Yes
6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	No	Yes	Yes	No	No		Yes
A7	**Physical Controls**									
7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Yes	No	Yes	Yes	No	No		Yes
7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Yes	No	Yes	Yes	No	No		Yes
7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access	Yes	No	Yes	Yes	No	No		Yes
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Yes	No	Yes	Yes	No	No		Yes
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Yes	No	Yes	Yes	No	No		Yes
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Yes	No	Yes	Yes	No	No		Yes
7.9	Security of assets off-premises	Off-site assets shall be protected.	Yes	No	Yes	Yes	No	No		Yes
7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation.	Yes	No	Yes	Yes	No	No		yes
7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	No	Yes	Yes	No	No		Yes
7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Yes	No	Yes	Yes	No	No		Yes
7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

7.14	Secure disposal or re-use of equipment	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	No	Yes	Yes	No	No		Yes
8	**Technological controls**									
8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices shall be protected.	Yes	No	Yes	No	No	No		Yes
8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Yes	No	Yes	No	No	No		Yes
8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Yes	No	Yes	Yes	No	No		Yes
8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	No	Yes	No	No	No		Yes

CONFIDENTIAL

8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes	No	Yes	Yes	No	No		Yes
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Yes	No	Yes	No	No	No		Yes
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Yes	No	Yes	Yes	No	No		yes
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes	No	Yes	No	No	No		Yes
8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Yes	Yes	Yes	Yes	No	No		Partially

CONFIDENTIAL

8.11	Data masking	Data masking shall 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	No	Yes	No	No	No		Partially
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes	No	Yes	No	No	No		Yes
8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	No	Yes	Yes	No	No		Yes
8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	No	Yes	Yes	No	No		Yes
8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.	Yes	No	Yes	No	No	No		Yes
8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	No	Yes	Yes	No	No		Yes
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes	No	Yes	Yes	No	No		Yes
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes	No	Yes	No	No	No		Yes
8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Yes	No	Yes	No	No	No		Yes
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Yes	No	Yes	No	No	No		Yes
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Yes	No	Yes	Yes	No	No		Yes
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Yes	No	Yes	Yes	No	No		Yes
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Yes	No	Yes	No	No	No		Partially

CONFIDENTIAL

8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	Yes	No	Yes	Yes	No	No		Yes
8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Yes	No	Yes	Yes	No	No		Yes
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Yes	No	Yes	Yes	No	No		Yes
8.28	Secure coding	Secure coding principles shall be applied to software development.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL

8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Yes	No	Yes	Yes	No	No		Yes
8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Yes	No	Yes	Yes	No	No		No
8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Yes	No	Yes	Yes	No	No		Yes
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes	No	Yes	No	No	No		Yes

CONFIDENTIAL

8.33	Test information	Test information shall be appropriately selected, protected and managed.	Yes	No	Yes	Yes	No	No		Yes
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Yes	No	Yes	Yes	No	No		Yes

CONFIDENTIAL