June 13, 2023

EGI Foundation: Statement of applicability (SOA) of information security controls according to ISO/IEC 27001

Version: 2.0
Date (last update / approval): 2023-05-16
Dissemination level: TLP:CLEAR - Public

Legend:
Justification for inclusion:
L = Legal requirement
C = Customer (or other stakeholder) requirement
M = Management requirement / State of the art
R = Related risk

+31 (0)20 89 32 007
contact@egi.eu
www.egi.eu

Control (ISO/IEC 27001:2022)	Control (ISO/IEC 27001:2013)	Applicable?	Justification for inclusion / exclusion	Status of implementation
A.5.1 Policies for information security	A.5.1.1, A.5.1.2	Yes	C, M	Defined, fully implemented
A.5.2 Information security roles and responsibilities	A.6.1.1	Yes	M	Defined, fully implemented
A.5.3 Segregation of duties	A.6.1.2	Yes	M	Defined, fully implemented
A.5.4 Management responsibilities	A.7.2.1	Yes	M	Defined, fully implemented
A.5.5 Contact with authorities	A.6.1.3	Yes	L, M	Defined, fully implemented
A.5.6 Contact with special interest groups	A.6.1.4	Yes	M	Defined, fully implemented
A.5.7 Threat intelligence	New	Yes	M	Defined, fully implemented
A.5.8 Information security in project management	A.6.1.5, A.14.1.1	Yes	M	Defined, fully implemented

A.5.9 Inventory of information and other associated assets	A.8.1.1, A.8.1.2	Yes	M	Defined, fully implemented
A.5.10 Acceptable use of information and other associated assets	A.8.1.3, A.8.2.3	Yes	M	Defined, fully implemented
A.5.11 Return of assets	A.8.1.4	Yes	M	Defined, fully implemented
A.5.12 Classification of information	A.8.2.1	Yes	M	Defined, fully implemented
A.5.13 Labelling of information	A.8.2.2	Yes	M	Defined, fully implemented
A.5.14 Information transfer	A.13.2.1, A.13.2.2, A.13.2.3	Yes	M	Defined, fully implemented
A.5.15 Access control	A.9.1.1, A.9.1.2	Yes	M	Defined, fully implemented
A.5.16 Identity management	A.9.2.1	Yes	M	Defined, fully implemented

A.5.17 Authentication information	A.9.2.4, A.9.3.1, A.9.4.3	Yes	M	Defined, fully implemented
A.5.18 Access rights	A.9.2.2, A.9.2.5, A.9.2.6	Yes	M	Defined, fully implemented
A.5.19 Information security in supplier relationships	A.15.1.1	Yes	M	Defined, fully implemented
A.5.20 Addressing information security within supplier agreements	A.15.1.2	Yes	M	Defined, implementation ongoing
A.5.21 Managing information security in the ICT supply chain	A.15.1.4	Yes	M	Defined, implementation ongoing
A.5.22 Monitoring, review and change management of supplier services	A.15.2.1, A.15.2.2	Yes	M	Defined, fully implemented
A.5.23 Information security for use of cloud services	New	Yes	M	Defined, fully implemented

A.5.24 Information security incident management planning and preparation	A.16.1.1	Yes	M	Defined, fully implemented
A.5.25 Assessment and decision on information security events	A.16.1.4	Yes	M	Defined, fully implemented
A.5.26 Response to information security incidents	A.16.1.5	Yes	M	Defined, fully implemented
A.5.27 Learning from information security incidents	A.16.1.6	Yes	M	Defined, fully implemented
A.5.28 Collection of evidence	A.16.1.7	Yes	M	Defined, fully implemented
A.5.29 Information security during disruption	A.17.1.1, A.17.1.2, A.17.1.3	Yes	M	Defined, fully implemented
A.5.30 ICT readiness for business continuity	New	Yes	M	Defined, fully implemented

A.5.31 Legal, statutory, regulatory and contractual requirements	A.18.1.1, A.18.1.5	Yes	L, M	Defined, fully implemented
A.5.32 Intellectual property rights	A.18.1.2	Yes	M	Defined, fully implemented
A.5.33 Protection of records	A.18.1.3	Yes	M	Defined, fully implemented
A.5.34 Privacy and protection of PII	A.18.1.4	Yes	M	Defined, fully implemented
A.5.35 Independent review of information security	A.18.2.1	Yes	M	Defined, fully implemented
A.5.36 Conformance with policies, rules and standards for information security	A.18.2.2, A.18.2.3	Yes	M	Defined, fully implemented
A.5.37 Documented operating procedures	A.12.1.1	Yes	M	Defined, fully implemented

A.6.1 Screening	A.7.1.1	Yes	C, M	Defined, fully implemented
A.6.2 Terms and conditions of employment	A.7.1.2	Yes	M	Defined, fully implemented
A.6.3 Information security awareness, education and training	A.7.2.2	Yes	M	Defined, implementation ongoing
A.6.4 Disciplinary process	A.7.2.3	Yes	M	Defined, fully implemented
A.6.5 Responsibilities after termination or change of employment	A.7.3.1	Yes	M	Defined, fully implemented
A.6.6 Confidentiality or non-disclosure agreements	A.13.2.4	Yes	M	Defined, fully implemented
A.6.7 Remote working	A.6.2.2	Yes	M	Defined, fully implemented
A.6.8 Information security event reporting	A.16.1.2, A.16.1.3	Yes	M	Defined, fully implemented

A.7.1 Physical security perimeters	A.11.1.1	Yes	M	Defined, fully implemented
A.7.2 Physical entry	A.11.1.2, A.11.1.6	Yes	M	Defined, fully implemented
A.7.3 Securing offices, rooms and facilities	A.11.1.3	Yes	M	Defined, fully implemented
A.7.4 Physical security monitoring	New	Yes	M	Defined, fully implemented
A.7.5 Protecting against physical and environmental threats	A.11.1.4	Yes	M	Defined, fully implemented
A.7.6 Working in secure areas	A.11.1.5	Yes	M	Defined, fully implemented
A.7.7 Clear desk and clear screen	A.11.2.9	Yes	M	Defined, fully implemented
A.7.8 Equipment siting and protection	A.11.2.1	Yes	M	Defined, fully implemented

A.7.9 Security of assets off-premises	A.11.2.6	Yes	M	Defined, fully implemented
A.7.10 Storage media	A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5	Yes	M	Defined, fully implemented
A.7.11 Supporting utilities	A.11.2.2	Yes	M	Defined, fully implemented
A.7.12 Cabling security	A.11.2.3	Yes	M	Defined, fully implemented
A.7.13 Equipment maintenance	A.11.2.4	Yes	M	Defined, fully implemented
A.7.14 Secure disposal or re-use of equipment	A.11.2.7	Yes	M	Defined, fully implemented
A.8.1 User endpoint devices	A.6.2.1, A.11.2.8	Yes	M	Defined, fully implemented
A.8.2 Privileged access rights	A.9.2.3	Yes	M	Defined, fully implemented
A.8.3 Information access restriction	A.9.4.1	Yes	M	Defined, fully implemented

A.8.4 Access to source code	A.9.4.5	Yes	M	Defined, fully implemented
A.8.5 Secure authentication	A.9.4.2	Yes	M	Defined, fully implemented
A.8.6 Capacity management	A.12.1.3	Yes	M	Defined, fully implemented
A.8.7 Protection against malware	A.12.2.1	Yes	M	Defined, fully implemented
A.8.8 Management of technical vulnerabilities	A.12.6.1, A.18.2.3	Yes	M	Defined, fully implemented
A.8.9 Configuration management	New	Yes	M	Defined, fully implemented
A.8.10 Information deletion	New	Yes	M	Defined, fully implemented
A.8.11 Data masking	New	Yes	M	Defined, implementation ongoing
A.8.12 Data leakage prevention	New	Yes	M	Defined, implementation ongoing

A.8.13 Information backup	A.12.3.1	Yes	M, R	Defined, fully implemented
A.8.14 Redundancy of information processing facilities	A.17.2.1	Yes	M	Defined, fully implemented
A.8.15 Logging	A.12.4.1, A.12.4.2, A.12.4.3	Yes	M	Defined, fully implemented
A.8.16 Monitoring activities	New	Yes	M	Defined, fully implemented
A.8.17 Clock synchronization	A.12.4.4	Yes	M	Defined, fully implemented
A.8.18 Use of privileged utility programs	A.9.4.4	Yes	M	Defined, fully implemented
A.8.19 Installation of software on operational systems	A.12.5.1, A.12.6.2	Yes	M	Defined, fully implemented
A.8.20 Networks security	A.13.1.1	Yes	M	Defined, fully implemented
A.8.21 Security of network services	A.13.1.2	Yes	M	Defined, fully implemented

A.8.22 Segregation of networks	A.13.1.3	Yes	M	Defined, fully implemented
A.8.23 Web filtering	New	Yes	M	Defined, fully implemented
A.8.24 Use of cryptography	A.10.1.1, A.10.1.2	Yes	M	Defined, implementation ongoing
A.8.25 Secure development life cycle	A.14.2.1	Yes	M	Defined, fully implemented
A.8.26 Application security requirements	A.14.1.2, A.14.1.3	Yes	M	Defined, fully implemented
A.8.27 Secure system architecture and engineering principles	A.14.2.5	Yes	M	Defined, fully implemented
A.8.28 Secure coding	New	Yes	M	Defined, fully implemented
A.8.29 Security testing in development and acceptance	A.14.2.8, A.14.2.9	Yes	M	Defined, fully implemented

A.8.30 Outsourced development	A.14.2.7	Yes	M	Defined, fully implemented
A.8.31 Separation of development, test and production environments	A.14.1.4, A.14.2.6	Yes	M	Defined, fully implemented
A.8.32 Change management	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4	Yes	M	Defined, fully implemented
A.8.33 Test information	A.14.3.1	Yes	M	Defined, fully implemented
A.8.34 Protection of information systems during audit testing	A.12.7.1	Yes	M	Defined, fully implemented