Erklärung der Anwendbarkeit / Statement of Applicability (SOA)

Freigegeben am 02.05.2025 durch Gerhard Pölz (CEO)

ASTRUM IT

Nr.	Control	Anwend-barkeit	Grund: Gesetz	Grund: Vertrag	Grund: Risiko	Grund:Eigen
5.1	Policies for information security	umgesetzt				x
5.2	Information security roles and responsibilities	umgesetzt		x	x	x
5.3	Segregation of duties	umgesetzt			x	x
5.4	Management responsibilities	umgesetzt		x	x	x
5.5	Contact with authorities	umgesetzt				x
5.6	Contact with special interest groups	umgesetzt				x
5.7	Threat intelligence	umgesetzt				x
5.8	Information security in project management	umgesetzt			x	x
5.9	Inventory of information and other associated assets	umgesetzt				x
5.10	Acceptable use of information and other associated assets	umgesetzt				x
5.11	Return of assets	umgesetzt		x	x	x
5.12	Classification of information	umgesetzt		x	x	x
5.13	Labelling of information	umgesetzt		x	x	x
5.14	Information transfer	umgesetzt				x
5.15	Access control	umgesetzt		x	x	x
5.16	Identity management	umgesetzt		x	x	x
5.17	Authentication information	umgesetzt		x	x	x
5.18	Access rights	umgesetzt			x	x
5.19	Information security in supplier relationships	umgesetzt			x	x
5.20	Addressing information security within supplier agreements	umgesetzt			x	x
5.21	Managing information security in the information and communication technology (ICT) supply chain	umgesetzt			x	x
5.22	Monitoring, review and change management of supplier services	umgesetzt			x	x
5.23	Information security for use of cloud services	umgesetzt			x	x
5.24	Information security incident management planning and preparation	umgesetzt		x	x	x
5.25	Assessment and decision on information security events	umgesetzt		x	x	x
5.26	Response to information security incidents	umgesetzt		x	x	x
5.27	Learning from information security incidents	umgesetzt			x	x
5.28	Collection of evidence	umgesetzt		x	x	x
5.29	Information security during disruption	umgesetzt			x	x
5.30	ICT readiness for business continuity	umgesetzt			x	x
5.31	Legal, statutory, regulatory and contractual requirements	umgesetzt			x	
5.32	Intellectual property rights	umgesetzt	x	x	x	x
5.33	Protection of records	umgesetzt	x	x	x	x
5.34	Privacy and protection of personal identifiable information (PII)	umgesetzt	x	x	x	x
5.35	Independent review of information security	umgesetzt				x
5.36	Compliance with policies, rules and standards for information security	umgesetzt				x
5.37	Documented operating procedures	umgesetzt			x	x
6.1	Screening	umgesetzt			x	x
6.2	Terms and conditions of employment	umgesetzt			x	x
6.3	Information security awareness, education and training	umgesetzt			x	x
6.4	Disciplinary process	umgesetzt				x

Nr.	Control	Anwend-barkeit	Grund: Gesetz	Grund: Vertrag	Grund: Risiko	Grund:Eigen
6.5	Responsibilities after termination or change of employment	umgesetzt		x	x	x
6.6	Confidentiality or non-disclosure agreements	umgesetzt		x	x	x
6.7	Remote working	umgesetzt			x	x
6.8	Information security event reporting	umgesetzt			x	x
7.1	Physical security perimeters	umgesetzt		x	x	x
7.2	Physical entry	umgesetzt		x	x	x
7.3	Securing offices, rooms and facilities	umgesetzt		x	x	x
7.4	Physical security monitoring	umgesetzt		x	x	x
7.5	Protecting against physical and environmental threats	umgesetzt		x	x	x
7.6	Working in secure areas	umgesetzt		x	x	x
7.7	Clear desk and clear screen	umgesetzt			x	x
7.8	Equipment siting and protection	umgesetzt		x	x	x
7.9	Security of assets off-premises	umgesetzt			x	x
7.10	Storage media	umgesetzt	x	x	x	x
7.11	Supporting utilities	umgesetzt		x	x	x
7.12	Cabling security	umgesetzt	x	x	x	x
7.13	Equipment maintenance	umgesetzt	x	x	x	x
7.14	Secure disposal or re-use of equipment	umgesetzt		x	x	x
8.1	User end point devices	umgesetzt		x	x	x
8.2	Privileged access rights	umgesetzt		x	x	x
8.3	Information access restriction	umgesetzt		x	x	x
8.4	Access to source code	umgesetzt		x	x	x
8.5	Secure authentication	umgesetzt		x	x	x
8.6	Capacity management	umgesetzt		x	x	x
8.7	Protection against malware	umgesetzt		x	x	x
8.8	Management of technical vulnerabilities	umgesetzt		x	x	x
8.9	Configuration management	umgesetzt			x	x
8.10	Information deletion	umgesetzt	x	x	x	x
8.11	Data masking	umgesetzt	x	x	x	x
8.12	Data leakage prevention	umgesetzt			x	x
8.13	Information backup	umgesetzt	x	x	x	x
8.14	Redundancy of information processing facilities	umgesetzt		x	x	x
8.15	Logging	umgesetzt		x	x	x
8.16	Monitoring activities	umgesetzt		x	x	x
8.17	Clock synchronization	umgesetzt			x	x
8.18	Use of privileged utility programs	umgesetzt			x	x
8.19	Installation of software on operational systems	umgesetzt			x	x
8.20	Networks security	umgesetzt			x	x
8.21	Security of network services	umgesetzt			x	x
8.22	Segregation of networks	umgesetzt			x	x
8.23	Web filtering	umgesetzt			x	x
8.24	Use of cryptography	umgesetzt			x	x

Nr.	Control	Anwend-barkeit	Grund: Gesetz	Grund: Vertrag	Grund: Risiko	Grund:Eigen
8.25	Secure development life cycle	umgesetzt			x	x
8.26	Application security requirements	umgesetzt			x	x
8.27	Secure system architecture and engineering principles	umgesetzt			x	x
8.28	Secure coding	umgesetzt			x	x
8.29	Security testing in development and acceptance	umgesetzt			x	x
8.30	Outsourced development	umgesetzt				x
8.31	Separation of development, test and production environments	umgesetzt		x	x	x
8.32	Change management	umgesetzt		x	x	x
8.33	Test information	umgesetzt	x	x	x	x
8.34	Protection of information systems during audit testing	umgesetzt		x	x	x