eschbach

Statement of applicability

Exported on November 06, 2024

Status: APPROVED

Confidentiality: PROTECTED

eschbach GmbH • Steinbrückstr. 10 • 79713 Bad Säckingen • Germany
Phone +49 (0)7761 55959-0 • Fax +49 (0)7761 55 959-29 • info@eschbach.com • www.eschbach.com
Trade Register Freiburg, HRB 621631 • VAT ID: DE814509205 • Managing Director: Andreas Eschbach

eschbach

eschbach

Table of Contents

eschbach

Document Owner	Version	Document ID	Status	Confidentiality	Site
QM	14	272990335	APPROVED	PROTECTED	

Author

Lisa Köpfer

DocuSigned by:
Lisa Köpfer
60A0E03BE84A4C2...

Head of Quality Management

Approver

CEO

DocuSigned by:
6F80EBA8D699481...

Andreas Eschbach

eschbach

1 5 Organizational Controls

Legend: Sec = Section of ISO/ IEC 27001:2022 Annex A; LR= legal requirement; CO= contractual obligation; BR = business requirement; BP = best practice; RA = result of risk assessment

Sec	Control Description	Applicable	Implemented	Justification for inclusion					Justification for exclusion
				LR	CO	BR	BP	RA	
5.1	Policies for information security	Yes	Yes				✓	✓	n/a
5.2	Information security roles and responsibilities	Yes	Yes				✓	✓	n/a
5.3	Segregation of duties	Yes	Yes				✓	✓	n/a
5.4	Management responsibilities	Yes	Yes				✓	✓	n/a
5.5	Contact with authorities	Yes	Yes	✓					n/a
5.6	Contact with special interest groups	Yes	Yes			✓	✓		n/a
5.7	Threat intelligence	Yes	Yes			✓	✓	✓	n/a
5.8	Information security in project management	Yes	Yes		✓	✓	✓	✓	n/a

5.9	Inventory of information and other associated assets	Yes	Yes			✓	✓	✓	n/a
5.10	Acceptable use of information and other associated assets	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.11	Return of assets	Yes	Yes		✓	✓	✓	✓	n/a
5.12	Classification of information	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.13	Labelling of information	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.14	Information transfer	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.15	Access control	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.16	Identity management	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.17	Authentication information	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.18	Access rights	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.19	Information security in supplier relationships	Yes	Yes	✓	✓	✓	✓	✓	n/a

5.20	Addressing information security within supplier agreements	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.21	Managing information security in the ICT supply chain	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.22	Monitoring, review and change management of supplier services	Yes	Yes		✓		✓	✓	n/a
5.23	Information security for use of cloud services	Yes	Yes		✓	✓	✓	✓	n/a
5.24	Information security incident management planning and preparation	Yes	Yes		✓	✓	✓	✓	n/a
5.25	Assessment and decision on information security events	Yes	Yes		✓	✓	✓	✓	n/a
5.26	Response to information security incidents	Yes	Yes		✓	✓	✓	✓	n/a
5.27	Learning from information security incidents	Yes	Yes			✓	✓	✓	n/a
5.28	Collection of evidence	Yes	Yes			✓	✓	✓	n/a

5.29	Information security during disruption	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.30	ICT readiness for business continuity	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.31	Identification of legal, statutory, regulatory and contractual requirements	Yes	Yes	✓		✓	✓	✓	n/a
5.32	Intellectual property rights	Yes	Yes		✓	✓	✓	✓	n/a
5.33	Protection of records	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.34	Privacy and protection of PII	Yes	Yes	✓	✓	✓	✓	✓	n/a
5.35	Independent review of information security	Yes	Yes				✓	✓	n/a
5.36	Compliance with policies and standards for information security	Yes	Yes			✓	✓	✓	n/a
5.37	Documented operating procedures	Yes	Yes			✓	✓	✓	n/a

eschbach

2 6 People Controls

Legend: Sec = Section of ISO/ IEC 27001:2022 Annex A; LR= legal requirement; C= contractual requirement; BR = business requirement; BP = best practice; RA = result of risk assessment

Sec	Control Description	Applicable	Implemented	Justification for inclusion					Justification for exclusion
				LR	CO	BR	BP	RA	
6.2	Terms and conditions of employment	Yes	Yes		✓	✓	✓	✓	n/a
6.3	Information security awareness, education and training	Yes	Yes	✓	✓	✓	✓	✓	n/a
6.4	Disciplinary Process	Yes	Yes		✓	✓	✓		n/a
6.5	Responsibilities after termination or change of employment	Yes	Yes	✓	✓	✓	✓	✓	n/a
6.6	Confidentiality or non-disclosure agreements	Yes	Yes		✓	✓	✓	✓	n/a
6.7	Remote working	Yes	Yes		✓	✓	✓	✓	n/a
6.8	Information security event reporting	Yes	Yes		✓	✓	✓	✓	n/a

eschbach

3 7 Physical Controls

Legend: Sec = Section of ISO/ IEC 27001:2022 Annex A; LR= legal requirement; C= contractual requirement; BR = business requirement; BP = best practice; RA = result of risk assessment

Sec	Control Description	Applicable	Implemented	Justification for inclusion					Justification for exclusion
				LR	CO	BR	BP	RA	
7.2	Physical entry controls	Yes	Yes		✓	✓	✓	✓	n/a
7.3	Securing offices, rooms and facilities	Yes	Yes		✓	✓	✓	✓	n/a
7.4	Physical security monitoring	Yes	Yes			✓	✓	✓	n/a
7.5	Protecting against physical and environmental threats	Yes	Yes		✓	✓	✓	✓	n/a
7.6	Working in secure areas	Yes	Yes		✓	✓	✓	✓	n/a
7.7	Clear desk and clear screen	Yes	Yes			✓	✓	✓	n/a
7.8	Equipment siting and protection	Yes	Yes			✓	✓	✓	n/a
7.9	Security of assets off-premises	Yes	Yes		✓	✓	✓	✓	n/a

7.10	Storage media	Yes	Yes		✓	✓	✓	✓	n/a
7.11	Supporting utilities	Yes	Yes		✓	✓	✓	✓	n/a
7.12	Cabling security	Yes	Yes		✓	✓	✓	✓	n/a
7.13	Equipment maintenance	Yes	Yes		✓	✓	✓	✓	n/a
7.14	Secure disposal or re-use of equipment	Yes	Yes	✓	✓	✓	✓	✓	n/a

eschbach

4 8 Technological Controls

Legend: App = control applicable; Impl = control implemented; LR= legal requirement; C= contractual requirement; BR = business requirement; BP = best practice; RA = result of risk assessment

Sec	Control Description	Applicable	Implemented	Justification for inclusion					Justification for exclusion
				LR	CO	BR	BP	RA	
8.1	User endpoint devices	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.2	Privileged access rights	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.3	Information access restriction	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.4	Access to source code	Yes	Yes		✓	✓	✓	✓	n/a
8.5	Secure authentication	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.6	Capacity management	Yes	Yes		✓	✓	✓		n/a
8.7	Protection against malware	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.8	Management of technical vulnerabilities	Yes	Yes	✓	✓	✓	✓	✓	n/a

8.9	Configuration management	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.10	Information Deletion	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.11	Data Masking	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.12	Data Leakage Prevention	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.13	Information Backup	Yes	Yes		✓	✓	✓	✓	n/a
8.14	Redundancy of Information Processing Facilities	Yes	Yes		✓	✓	✓	✓	n/a
8.15	Logging	Yes	Yes		✓	✓	✓	✓	n/a
8.16	Monitoring Activities	Yes	Yes		✓	✓	✓	✓	n/a
8.17	Clock Synchronization	Yes	Yes			✓	✓		n/a
8.18	Use of Privileged Utility Programs	Yes	Yes		✓	✓	✓	✓	n/a
8.19	Installation of Software on Operational Systems	Yes	Yes			✓	✓	✓	n/a
8.20	Network controls	Yes	Yes	✓	✓	✓	✓	✓	n/a

8.21	Security of Network Services	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.22	Segregation of Networks	Yes	Yes		✓	✓	✓	✓	n/a
8.23	Web filtering	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.24	Use of Cryptography	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.25	Secure Development Life Cycle	Yes	Yes		✓	✓	✓	✓	n/a
8.26	Application Security Requirements	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.27	Secure System Architecture and Engineering Principles	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.28	Secure Coding	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.29	Security Testing in Development and Acceptance	Yes	Yes	✓	✓	✓	✓	✓	n/a
8.30	Outsourced development	Yes	Yes			✓	✓	✓	n/a
8.31	Separation of development, test and production environments	Yes	Yes	✓	✓	✓	✓	✓	n/a

8.32	Change Management	Yes	Yes		✓	✓	✓	✓	n/a
8.33	Test Information	Yes	Yes		✓	✓	✓	✓	n/a
8.34	Protection of information systems during audit and testing	Yes	Yes		✓	✓	✓		n/a