Statement of Applicability (SoA)

of the information security management system

Hetzner Online GmbH

Industriestraße 25 – 91710 Gunzenhausen

Date:

19.07.2023

Created by:

Alena Scholz

Classification:

- open -

Version:
3.0

isms@hetzner.com

Document control

Handling instructions

Document created by	Alena Scholz
Document created on	19.07.2023
Document released by	Management of Hetzner Online GmbH
Document released on	24.07.2019
Classification	- open -
Recipients	All employees and customers of Hetzner Online GmbH

Modification history

Date	Version	Created by	Description of modifications
22.08.2016	2.2	Sebastian Lippold	Publishing SoA
12.07.2017	2.2	Sebastian Lippold	Review SoA – no modifications
18.07.2018	2.2	Sebastian Lippold	Review SoA – no modifications
08.07.2019	3.0	Sebastian Lippold	Hetzner Finland Oy included; annual review of SoA
23. / 24.07.2019	3.0	Sebastian Lippold	Approval by the management of Hetzner Online GmbH and Hetzner Finland Oy
28.04.2020	3.0	Sebastian Lippold	Review SoA – no modifications
25.02.2021	3.0	Sebastian Lippold	Review SoA – no modifications
30.05.2022	3.0	Sebastian Lippold	Review SoA – no modifications
19.07.2023	3.0	Alena Scholz	Review SoA – no modifications

Reference controls - Information security controls

A.5 Information Security Policies		
A.5.1	Management direction for information security	No exclusions contained

A.6 Organization of Information Security		
A.6.1	Internal organization	No exclusions contained
A.6.2	Mobile devices and teleworking	No exclusions contained

A.7 Human Resource Security		
A.7.1	Prior to employment	No exclusions contained
A.7.2	During employment	No exclusions contained
A.7.3	Termination and change of employment	No exclusions contained

A.8 Asset Management		
A.8.1	Responsibility for assets	No exclusions contained
A.8.2	Information classification	No exclusions contained
A.8.3	Media handling	No exclusions contained

A.9 Access Control		
A.9.1	Access control policy	No exclusions contained
A.9.2	User access management	No exclusions contained
A.9.3	User responsibilities	No exclusions contained
A.9.4	System and application access control	No exclusions contained

A.10 Cryptography		
A.10.1	Cryptographic controls	No exclusions contained

A.11 Physical and Environmental Security		
A.11.1	Secure areas	No exclusions contained
A.11.2	Equipment	No exclusions contained

A.12 Operational Security		
A.12.1	Operational procedures and responsibilities	No exclusions contained
A.12.2	Protection from malware	No exclusions contained
A.12.3	Backup	No exclusions contained
A.12.4	Logging and monitoring	No exclusions contained
A.12.5	Control of operational software	No exclusions contained
A.12.6	Technical vulnerability management	No exclusions contained
A.12.7	Information systems audit considerations	No exclusions contained

A.13 Communications Security		
A.13.1	Network security management	No exclusions contained
A.13.2	Information transfer	No exclusions contained

A.14 System Acquisition, Development, and Maintenance		
A.14.1	Security requirements of information systems	No exclusions contained
A.14.2	Security in development and support processes	No exclusions contained
A.14.3	Test data	No exclusions contained

A.15 Supplier Relationships		
A.15.1	Information security in supplier relationships	No exclusions contained
A.15.2	Supplier service delivery management	No exclusions contained

A.16 Information Security Incident Management		
A.16.1	Management of information security incidents and improvements	No exclusions contained

A.17 Information Security Aspects of Business Continuity Management		
A.17.1	Information security continuity	No exclusions contained
A.17.2	Redundancies	No exclusions contained

A.18 Compliance		
A.18.1	Compliance with legal and contractual requirements	No exclusions contained
A.18.2	Information security reviews	No exclusions contained