Statement of Applicability

of the information security management system
on the basis of the ISO/IEC 27001:2013 of the
Hetzner Online GmbH & Hetzner Finland Oy

version:	3.0
Date of the version:	24.07.2019
Created by	Sebastian Lippold

classification	- OPEN -

1. Document Control

1.1. Handling Note

Document Manager:	CISO	
business area / department	all	
document classification:	- OPEN -	Date
Document created by:	Sebastian Lippold	08.07.2019
Document released by:	Management Board Hetzner Online GmbH	24.07.2019
	Management Board Hetzner Finland Oy	23.07.2019
Recipients:	All employees	

1.2. Modification History

Date	Vers.	created by	Description of the modification
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 & Hetzner Finland Oy

A.5 Information security policies

A.5.1 Management direction for information security

A.5.1.1	Policies for information security	YES
A.5.1.2	Review of the policies for information security	YES

A.6 Organization of information security

A.6.1 Internal organization

A.6.1.1	Information security roles and responsibilities	YES
A.6.1.2	Segregation of duties	YES
A.6.1.3	Contact with authorities	YES
A.6.1.4	Contact with special interest groups	YES
A.6.1.5	Information security in project management	YES

A.6.2 Mobile devices and teleworking

A.6.2.1	Mobile device policy	YES
A.6.2.2	Teleworking	YES

A.7 Human resource security

A.7.1 Prior to employment

A.7.1.1	Screening	YES
A.7.1.2	Terms and conditions of employment	YES

A.7.2 During employment

A.7.2.1	Management responsibilities	YES
A.7.2.2	Information security awareness, education and training	YES
A.7.2.3	Disciplinary process	YES

A.7.3 Termination and change of employment

A.7.3.1	Termination or change of employment responsibilities	YES

A.8 Asset Management

A8.1 Responsibility for assets

A.8.1.1	Inventory of assets	YES
A.8.1.2	Ownership of assets	YES
A.8.1.3	Acceptable use of assets	YES
A.8.1.4	Return of assets	YES

A.8.2 Information classification

A.8.2.1	Classification of information	YES
A.8.2.2	Labelling of information	YES
A.8.2.3	Handling of assets	YES

A.8.3 Media handling

A.8.3.1	Management of removable media	YES
A.8.3.2	Disposal of media	YES
A.8.3.3	Physical media transfer	YES

A.9 Access control

A.9.1 Access control policy

A.9.1.1	Access control policy	YES
A.9.1.2	Access to networks and network services	YES

A.9.2 User access management

A.9.2.1	User registration and de-registration	YES
A.9.2.2	User access provisioning	YES
A.9.2.3	Management of privileged access rights	YES
A.9.2.4	Management of secret authentication information of users	YES
A.9.2.5	Review of user access rights	YES
A.9.2.6	Removal or adjustment of access rights	YES

A.9.3 User responsibilities

A.9.3.1	Use of secret authentication information	YES

A.9.4 System and application access control

A.9.4.1	Information access restriction	YES
A.9.4.2	Secure log-on procedures	YES
A.9.4.3	Password management system	YES
A.9.4.4	Use of privileged utility programs	YES
A.9.4.5	Access control to program source code	YES

A.10 Cryptography

A.10.1 Cryptographic controls

A.10.1.1	Policy on the use of cryptographic controls	YES
A.10.1.2	Key management	YES

A.11 Physical and environmental security

A.11.1 Secure areas

A.11.1.1	Physical security perimeter	YES
A.11.1.2	Physical entry controls	YES
A.11.1.3	Securing offices, rooms and facilities	YES
A.11.1.4	Protecting against external and environmental threats	YES
A.11.1.5	Working in secure areas	YES
A.11.1.6	Delivery and loading areas	YES

A.11.2 Equipment

A.11.2.1	Equipment siting and protection	YES
A.11.2.2	Supporting utilities	YES
A.11.2.3	Cabling security	YES

A.11.2.4	Equipment maintenance	YES
A.11.2.5	Removal of assets	YES
A.11.2.6	Security of equipment and assets off-premises	YES
A.11.2.7	Secure disposal or re-use of equipment	YES
A.11.2.8	Unattended user equipment	YES
A.11.2.9	Clear desk and clear screen policy	YES

A.12 Operational Security

A.12.1 Operational procedures and responsibilities

A.12.1.1	Documented operating procedures	YES
A.12.1.2	Change management	YES
A.12.1.3	Capacity management	YES
A.12.1.4	Separation of development, testing and operational environments	YES

A.12.2 Protection from malware

A.12.2.1	Controls against malware	YES

A.12.3 Backup

A.12.3.1	Information backup	YES

A.12.4 Logging and monitoring

A.12.4.1	Event logging	YES
A.12.4.2	Protection of log information	YES
A.12.4.3	Administrator and operator logs	YES
A.12.4.4	Clock synchronisation	YES

A.12.5 Control of operational software

A.12.5.1	Installation of software on operational systems	YES

A.12.6 Technical vulnerability management

A.12.6.1	Management of technical vulnerabilities	YES
A.12.6.2	Restrictions on software installation	YES

A.12.7 Information systems audit considerations

A.12.7.1	Information systems audit controls	YES

A.13 Communications security

A.13.1 Network security management

A.13.1.1	Network controls	YES
A.13.1.2	Security of network services	YES
A.13.1.3	Segregation in networks	YES

A.13.2 Information transfers

A.13.2.1	Information transfer policies and procedures	YES
A.13.2.2	Agreements on information transfer	YES
A.13.2.3	Electronic messaging	YES
A.13.2.4	Confidentiality or non-disclosure agreements	YES

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems

A.14.1.1	Information security requirements analysis and specification	YES
A.14.1.2	Securing application services on public networks	YES
A.14.1.3	Protecting application services transactions	YES

A.14.2 Security in development and support processes

A.14.2.1	Secure development policy	YES
A.14.2.2	System change control procedures	YES
A.14.2.3	Technical review of applications after operating platform changes	YES
A.14.2.4	Restrictions on changes to software packages	YES
A.14.2.5	Secure system engineering principles	YES
A.14.2.6	Secure development environment	YES
A.14.2.7	Outsourced development	YES
A.14.2.8	System security testing	YES
A.14.2.9	System acceptance testing	YES

A.14.3 Test data

A.14.3.1	Protection of test data	YES

A.15 Supplier Relationship

A.15.1 Information security in supplier relationships

A.15.1.1	Information security policy for supplier relationships	YES
A.15.1.2	Addressing security within supplier agreements	YES
A.15.1.3	Information and communication technology supply chain	YES

A.15.2 Supplier service delivery management

A.15.2.1	Monitoring and review of supplier services	YES
A.15.2.2	Managing changes to supplier services	YES

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

A.16.1.1	Responsibilities and procedures	YES
A.16.1.2	Reporting information security events	YES
A.16.1.3	Reporting information security weaknesses	YES
A.16.1.4	Assessment of and decision on information security events	YES
A.16.1.5	Response to information security incidents	YES
A.16.1.6	Learning from information security incidents	YES
A.16.1.7	Collection of evidence	YES

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity

A.17.1.1	Planning information security continuity	YES
A.17.1.2	Implementing information security continuity	YES

A.17.1.3	Verify, review and evaluate information security continuity	YES

A.17.2 Redundancies

A.17.2.1	Availability of information processing facilities	YES

A.18 Compliance

A18.1 Compliance with legal and contractual requirements

A.18.1.1	Identification of applicable legislation and contractual requirements	YES
A.18.1.2	Intellectual property rights	YES
A.18.1.3	Protection of records	YES
A.18.1.4	Privacy and protection of personally identifiable information	YES
A.18.1.5	Regulation of cryptographic controls	YES

A.18.2 Information security reviews

A.18.2.1	Independent review of information security	YES
A.18.2.2	Compliance with security policies and standards	YES
A.18.2.3	Technical compliance review	YES