fiskaly
Information Security
Digest

1. Introduction

Information Security is a priority for fiskaly. Strict data protection, integrity, confidentiality, and availability requirements are met by our services. These requirements and controls are frequently audited internally and by independent organizations.

2. Certifications

As a consequence of the commitment to information security, fiskaly and its subsidiaries have been audited and certified by several standards. More information on our certifications can be found on the following webpage: https://www.fiskaly.com/certificates-associations .

3. ISO 27001

One of the most relevant certifications in the field of information security is the ISO/IEC 27001 standard. fiskaly and its subsidiaries have been successfully audited and certified against this standard. The current certificate can be found on the previously mentioned website.

The latest certification audit was successfully conducted in March 2024 with a positive result, which extends the validity of our certificate and covers fiskaly and all its subsidiaries. fiskaly's certificate can be verified in the following website: Search for system and product certificates - certified by CIS

Certificate Nr. **I-00548/0**

fiskaly's ISO 27001:2022 Statement of Applicability can be found in *Section 6*.

4. Further Information

Because of confidentiality reasons, sharing of internal documents related to our ISMS (Information Security Management System) and the processes documented therein with third parties is not possible.
Nevertheless, interested third parties can request an audit on fiskaly by a competent authority. The total cost of the audit and resources used for it are to be covered by the requesting third party.

More information and further requests can be made through the following email address: infosec@fiskaly.com.

5. Information Security Policy

Following, fiskaly's Information Security Policy:

fiskaly.

Public

Information Security Policy

fiskaly stands for the secure and standard-compliant provision of fiscalization services. fiskaly GmbH, fiskaly Germany GmbH, fiskaly Iberia S.L., and fiskaly Italy S.r.l. are strongly committed to information security and its continuous improvement for all their process, services, and relevant assets, in all locations, whether on premise or remote.

fiskaly's Information Security Management System is designed to achieve *ISO 27001* compliance and the objectives of confidentiality, integrity, and availability in third party services and fiskaly's processes, hardware, software, products, and services.

Therefore, information security is a priority for fiskaly. The entire management and all employees are hereby bound to adhere to this Information Security Policy and to comply and cooperate with fiskaly's Information Security Management System for the continuous improvement of information security.

Vienna, 12/12/2023

6. Statement of Applicability

fiskaly's statement of applicability from the ISO 27001:2022 controls is as follows:

#	CONTROL	APPLICABLE
5	**Organizational Controls**	
5.1	Policies for information security	✔
5.2	Information security roles and responsibilities	✔
5.3	Segregation of duties	✔
5.4	Management responsibilities	✔
5.5	Contact with authorities	✔
5.6	Contact with special interest groups	✔
5.7	Threat intelligence	✔
5.8	Information security in project management	✔
5.9	Inventory of information and other associated assets	✔
5.10	Acceptable use of information and other associated assets	✔
5.11	Return of assets	✔
5.12	Classification of information	✔
5.13	Labelling of information	✔
5.14	Information transfer	✔
5.15	Access control	✔
5.16	Identity management	✔
5.17	Authentication information	✔
5.18	Access rights	✔
5.19	Information security in supplier relationships	✔
5.20	Addressing information security within supplier agreements	✔
5.21	Managing information security in the information and communication technology (ICT) supply chain	✔
5.22	Monitoring, review and change management of supplier services	✔
5.23	Information security for use of cloud services	✔
5.24	Information security incident management planning and preparation	✔
5.25	Assessment and decision on information security events	✔
5.26	Response to information security incidents	✔
5.27	Learning from information security incidents	✔
5.28	Collection of evidence	✔
5.29	Information security during disruption	✔
5.30	ICT readiness for business continuity	✔
5.31	Legal, statutory, regulatory and contractual requirements	✔
5.32	Intellectual property rights	✔

5.33	Protection of records	✔
5.34	Privacy and protection of personal identifiable information (PII)	✔
5.35	Independent review of information security	✔
5.36	Compliance with policies, rules and standards for information security	✔
5.37	Documented operating procedures	✔
6	**People Controls**	
6.1	Screening	✔
6.2	Terms and conditions of employment	✔
6.3	Information security awareness, education and training	✔
6.4	Disciplinary process	✔
6.5	Responsibilities after termination or change of employment	✔
6.6	Confidentiality or non-disclosure agreements	✔
6.7	Remote working	✔
6.8	Information security event reporting	✔
7	**Physical Controls**	
7.1	Physical security perimeters	✔
7.2	Physical entry	✔
7.3	Securing offices, rooms and facilities	✔
7.4	Physical security monitoring	✔
7.5	Protecting against physical and environmental threats	✔
7.6	Working in secure areas	✔
7.7	Clear desk and clear screen	✔
7.8	Equipment siting and protection	✔
7.9	Security of assets off-premises	✔
7.10	Storage media	✔
7.11	Supporting utilities	✔
7.12	Cabling security	✔
7.13	Equipment maintenance	✔
7.14	Secure disposal or reuse of equipment	✔
8	**Technological Controls**	
8.1	User endpoint devices	✔
8.2	Privileged access rights	✔
8.3	Information access restriction	✔
8.4	Access to source code	✔
8.5	Secure authentication	✔
8.6	Capacity management	✔
8.7	Protection against malware	✔

8.8	Management of technical vulnerabilities	✔
8.9	Configuration management	✔
8.10	Information deletion	✔
8.11	Data masking	✔
8.12	Data leakage prevention	✔
8.13	Information backup	✔
8.14	Redundancy of information processing facilities	✔
8.15	Logging	✔
8.16	Monitoring activities	✔
8.17	Clock synchronization	✔
8.18	Use of privileged utility programs	✔
8.19	Installation of software on operational systems	✔
8.20	Networks security	✔
8.21	Security of network services	✔
8.22	Segregation of networks	✔
8.23	Web filtering	✔
8.24	Use of cryptography	✔
8.25	Secure development life cycle	✔
8.26	Application security requirements	✔
8.27	Secure system architecture and engineering principles	✔
8.28	Secure coding	✔
8.29	Security testing in development and acceptance	✔
8.30	Outsourced development	✔
8.31	Separation of development, test and production environments	✔
8.32	Change management	✔
8.33	Test information	✔
8.34	Protection of information systems during audit testing	✔

Controls above marked with "*No*" are not applicable for fiskaly.

Measures to ensure information security for the applicable controls (marked with "✔") are therefore implemented by fiskaly. These measures have been audited successfully by CIS (Certification & Information Security Services GmbH), as mentioned in *Section 3* of this document.