Statement of Applicability

Document Classification Level : Normal
Document Reference : MAD-4
Document Name : Statement of Applicability
Document Creator : Alice Pearce

Date	Version	Purpose of the revision
10 Dec 2022	0.1	Creation of the document
19 Jan 2023	1.00	Document approval by CTOO
7 Dec 2023	1.1	Updated to align with ISO27001:2022

The purpose of the Statement of Applicability is to detail which controls are relevant to managing Gandi’s information security risk.

				Reasons for selection					
		Applicable?	**Implemented?**	**Risk Assessment Output**	**Legal and Regulatory Compliance**	**Contractual Obligation**	**Business Requirement**	**Best practice**	**Justification for Exemption**
5	**Organisational controls**								
5.1	Policies for information security	X	X	X			X	X	N/A
5.2	Information Security roles & responsibilities	X	X	X			X	X	N/A
5.3	Segregation of duties	X	X	X	X		X	X	N/A
5.4	Management responsibilities	X	X	X			X	X	N/A
5.5	Contact with authorities	X	X	X	X		X	X	N/A
5.6	Contact with special interest groups	X	X	X			X	X	N/A
5.7	Threat intelligence	X	X	X				X	N/A
5.8	Information security in project management	X	X	X				X	N/A
5.9	Inventory of information and other associated assets	X	X	X				X	N/A
5.10	Acceptable use of information and other associated assets	X	X	X				X	N/A
5.11	Return of assets	X	X	X			X	X	N/A
5.12	Classification of information	X	X	X			X	X	N/A
5.13	Labelling of information	X	X	X			X	X	N/A

5.14	Information transfer	X	X	X				X	N/A
5.15	Access control	X	X	X				X	N/A
5.16	Identity management	X	X	X				X	N/A
5.17	Authentication information	X	X	X				X	N/A
5.18	Access rights	X	X	X				X	N/A
5.19	Information security in supplier relationships	X	X	X				X	N/A
5.20	Addressing information security within supplier agreements	X	X	X				X	N/A
5.21	Managing information security in the information and communication technology (ICT) supply chain	X	X	X				X	N/A
5.22	Monitoring, review and change management of supplier services	X	X	X				X	N/A
5.23	Information security for use of cloud services	X	X	X				X	N/A
5.24	Information security incident management planning and preparation	X	X	X			X	X	N/A
5.25	Assessment and decision on information security events	X	X	X				X	N/A
5.26	Response to information security incidents	X	X	X			X	X	N/A
5.27	Learning from information security incidents	X	X	X				X	N/A
5.28	Collection of evidence	X	X	X				X	N/A
5.29	Information security during disruption	X	X	X				X	N/A
5.30	ICT readiness for business continuity	X	X	X				X	N/A
5.31	Legal, statutory, regulatory and contractual requirements	X	X	X				X	N/A
5.32	Intellectual property rights	X	X	X	X			X	N/A
5.33	Protection of records	X	X	X	X			X	N/A
5.34	Privacy and protection of personal identifiable information (PII)	X	X	X	X			X	N/A
5.35	Independent review of information security	X	X	X	X			X	N/A
5.36	Compliance with policies, rules and standards for information security	X	X	X				X	N/A
5.37	Documented operating procedures	X	X	X				X	N/A
6	**People controls**								
6.1	Screening	X	X	X			X	X	N/A
6.2	Terms and conditions of employment	X	X	X	X		X	X	N/A
6.3	Information security awareness, education and training	X	X	X			X	X	N/A
6.4	Disciplinary process	X	X	X			X	X	N/A
6.5	Responsibilities after termination or change of employment	X	X	X			X	X	N/A
6.6	Confidentiality or non-disclosure agreements	X	X	X		X		X	N/A
6.7	Remote working	X	X	X			X	X	N/A
6.8	Information security reporting	X	X	X				X	N/A
7	**Physical controls**								
7.1	Physical security perimeters	X	X	X				X	N/A
7.2	Physical entry	X	X	X				X	N/A
7.3	Securing offices, rooms and facilities	X	X	X				X	N/A

7.4	Physical security monitoring	X	X	X				X	N/A
7.5	Protecting against physical and environmental threats	X	X	X				X	N/A
7.6	Working in secure areas	X	X	X				X	N/A
7.7	Clear desk and clear screen	X	X	X				X	N/A
7.8	Equipment siting and protection	X	X	X	X			X	N/A
7.9	Security of assets off-premises	X	X	X	X			X	N/A
7.10	Storage media	X	X	X				X	N/A
7.11	Supporting utilities	X	X	X				X	N/A
7.12	Cabling security	X	X	X				X	N/A
7.13	Equipment maintenance	X	X	X	X			X	N/A
7.14	Secure disposal of re-use of equipment	X	X	X	X			X	N/A
8	**Technological controls**								
8.1	User end point devices	X	X	X				X	N/A
8.2	Privileged access rights	X	X	X	X			X	N/A
8.3	Information access restriction	X	X	X	X			X	N/A
8.4	Access to source code	X	X	X				X	N/A
8.5	Secure authentication	X	X	X	X			X	N/A
8.6	Capacity management	X	X	X				X	N/A
8.7	Protection against malware	X	X	X				X	N/A
8.8	Management of technical vulnerabilities	X	X	X				X	N/A
8.9	Configuration management	X	X	X				X	N/A
8.10	Information deletion	X	X	X				X	N/A
8.11	Data masking	X	X	X				X	N/A
8.12	Data leakage prevention	X	X	X				X	N/A
8.13	Information backup	X	X	X		X	X	X	N/A
8.14	Redundancy of information processing facilities	X	X	X		X	X	X	N/A
8.15	Logging	X	X	X		X		X	N/A
8.16	Monitoring activities	X	X	X				X	N/A
8.17	Clock synchronisation	X	X	X	X			X	N/A
8.18	Use of privileged utility programs	X	X	X				X	N/A
8.19	Installation of software on operational systems	X	X	X				X	N/A
8.20	Networks security	X	X	X			X	X	N/A
8.21	Security of network services	X	X	X			X	X	N/A
8.22	Segregation of networks	X	X	X			X	X	N/A
8.23	Web filtering	X	X	X				X	N/A
8.24	Use of cryptography	X	X	X				X	N/A
8.25	Secure development life cycle	X	X	X				X	N/A

8.26	Application security requirements	X	X	X				X	N/A
8.27	Secure system architecture and engineering principles	X	X	X				X	N/A
8.28	Secure coding	X	X	X				X	N/A
8.29	Security testing in development and acceptance	X	X	X				X	N/A
8.30	Outsourced development	N/A	N/A						Gandi does not outsource Any development.
8.31	Separation of development, test and production environments	X	X	X				X	N/A
8.32	Change management	X	X	X				X	N/A
8.33	Test information	X	X	X				X	N/A
8.34	Protection of information systems during audit testing	X	X	X				X	N/A