

Statement of Applicability

ISO/IEC 27001:2022 | Public extract | SoA version 2.0

Certification reference

Certified organisation	Humly Solutions AB
Certified locations	Sveavägen 124, Stockholm, Sweden Industrigatan 50, Kristianstad, Sweden
Standard on certificate	ISO 27001:2022
Certified scope	Development and sales of workplace solutions.
Certificate number	CI-23524/2026
Certification body	C1 Certification AB
Certification body address	Olof Palmes Gata 29, 111 22 Stockholm, Sweden
Initial certification	30 May 2024
Certificate issue date	21 April 2026
Certificate expiry date	29 May 2027
Signatory named on certificate	Thomas Andersson, CEO
SoA cited by certificate	Version 2.0

About this public extract

This extract presents the control families, control references, control names and applicability decisions from Humly's Statement of Applicability version 2.0.

Certificate CI-23524/2026, issued on 21 April 2026, identifies Statement of Applicability version 2.0. This public extract presents the applicability register for that version.

Applicability decisions are reproduced from the External Version register. Inclusion and exclusion justifications, implementation details and internal references remain in the full SoA.

Public extract prepared: 11 October 2026

Applicability register

Statement of Applicability version 2.0 | 93 controls

Control family	Control	Control name	Applicability
Organisational	A.5.1	Policies for information security	Applicable
Organisational	A.5.2	Information Security Roles and Responsibilities	Applicable
Organisational	A.5.3	Segregation of duties	Applicable
Organisational	A.5.4	Management responsibilities	Applicable
Organisational	A.5.5	Contact with authorities	Applicable
Organisational	A.5.6	Contact with special interest groups	Applicable
Organisational	A.5.7	Threat intelligence	Applicable
Organisational	A.5.8	Information security in project management	Applicable
Organisational	A.5.9	Inventory of information and other associated assets	Applicable
Organisational	A.5.10	Acceptable use of information and other associated assets	Applicable
Organisational	A.5.11	Return of assets	Applicable
Organisational	A.5.12	Classification of information	Applicable
Organisational	A.5.13	Labelling of information	Not Applicable
Organisational	A.5.14	Information transfer	Applicable
Organisational	A.5.15	Access control	Applicable
Organisational	A.5.16	Identity management	Applicable
Organisational	A.5.17	Authentication information	Applicable
Organisational	A.5.18	Access rights	Applicable
Organisational	A.5.19	Information security in supplier relationships	Applicable
Organisational	A.5.20	Addressing information security within supplier agreements	Applicable
Organisational	A.5.21	Managing information security in the ICT supply chain	Applicable
Organisational	A.5.22	Monitoring, review and change management of supplier services	Applicable
Organisational	A.5.23	Information security for use of cloud services	Applicable
Organisational	A.5.24	Information security incident management planning and preparation	Applicable
Organisational	A.5.25	Assessment and decision on information security events	Applicable

Control family	Control	Control name	Applicability
Organisational	A.5.26	Response to information security incidents	Applicable
Organisational	A.5.27	Learning from information security incidents	Applicable
Organisational	A.5.28	Collection of evidence	Applicable
Organisational	A.5.29	Information security during disruption	Applicable
Organisational	A.5.30	ICT readiness for business continuity	Applicable
Organisational	A.5.31	Identification of legal, statutory, regulatory and contractual requirements	Applicable
Organisational	A.5.32	Intellectual property rights	Applicable
Organisational	A.5.33	Protection of records	Applicable
Organisational	A.5.34	Privacy and protection of PII	Applicable
Organisational	A.5.35	Independent review of information security	Applicable
Organisational	A.5.36	Compliance with policies and standards for information security	Applicable
Organisational	A.5.37	Documented operating procedures	Applicable
People	A.6.1	Screening	Applicable
People	A.6.2	Terms and conditions of employment	Applicable
People	A.6.3	Information security awareness, education and training	Applicable
People	A.6.4	Disciplinary process	Applicable
People	A.6.5	Responsibilities after termination or change of employment	Applicable
People	A.6.6	Confidentiality or non-disclosure agreements	Applicable
People	A.6.7	Remote working	Applicable
People	A.6.8	Information security event reporting	Applicable
Physical	A.7.1	Physical security perimeter	Applicable
Physical	A.7.2	Physical entry controls	Applicable
Physical	A.7.3	Securing offices, rooms and facilities	Applicable
Physical	A.7.4	Physical security monitoring	Applicable
Physical	A.7.5	Protecting against physical and environmental threats	Applicable
Physical	A.7.6	Working in secure areas	Not Applicable
Physical	A.7.7	Clear desk and clear screen	Applicable
Physical	A.7.8	Equipment siting and protection	Applicable

Control family	Control	Control name	Applicability
Physical	A.7.9	Security of assets off-premises	Applicable
Physical	A.7.10	Storage media	Applicable
Physical	A.7.11	Supporting Utilities	Applicable
Physical	A.7.12	Cabling Security	Applicable
Physical	A.7.13	Equipment Maintenance	Applicable
Physical	A.7.14	Secure Disposal or Re-Use of Equipment	Applicable
Technology	A.8.1	User Endpoint Devices	Applicable
Technology	A.8.2	Privileged Access Rights	Applicable
Technology	A.8.3	Information Access Restriction	Applicable
Technology	A.8.4	Access To Source Code	Applicable
Technology	A.8.5	Secure Authentication	Applicable
Technology	A.8.6	Capacity Management	Applicable
Technology	A.8.7	Protection Against Malware	Applicable
Technology	A.8.8	Management of Technical Vulnerabilities	Applicable
Technology	A.8.9	Configuration Management	Applicable
Technology	A.8.10	Information Deletion	Applicable
Technology	A.8.11	Data Masking	Applicable
Technology	A.8.12	Data Leakage Prevention	Applicable
Technology	A.8.13	Information Backup	Applicable
Technology	A.8.14	Redundancy of Information Processing Facilities	Applicable
Technology	A.8.15	Logging	Applicable
Technology	A.8.16	Monitoring Activities	Applicable
Technology	A.8.17	Clock Synchronisation	Applicable
Technology	A.8.18	Use of Privileged Utility Programs	Applicable
Technology	A.8.19	Installation of Software on Operational Systems	Applicable
Technology	A.8.20	Network Security	Applicable
Technology	A.8.21	Security of Network Services	Applicable
Technology	A.8.22	Segregation of Networks	Applicable
Technology	A.8.23	Web Filtering	Applicable

Control family	Control	Control name	Applicability
Technology	A.8.24	Use of Cryptography	Applicable
Technology	A.8.25	Secure Development Life Cycle	Applicable
Technology	A.8.26	Application Security Requirements	Applicable
Technology	A.8.27	Secure Systems Architecture and Engineering Principles	Applicable
Technology	A.8.28	Secure Coding	Applicable
Technology	A.8.29	Security Testing in Development and Acceptance	Applicable
Technology	A.8.30	Outsourced Development	Applicable
Technology	A.8.31	Separation of Development, Test and Production Environments	Applicable
Technology	A.8.32	Change Management	Applicable
Technology	A.8.33	Test Information	Applicable
Technology	A.8.34	Protection of information systems during audit testing	Applicable