Statement of Applicability
Eurofiber Nederland B.V. and Eurofiber N.V.
ISO27001:2022
Version 1.0
Date 4-4-2025

	#	Title	Applicable Y/N	Implemented Y/N	Reason inclusion: Risk	Reason inclusion: Legal	Reason inclusion: Contractual	Reason for exclusion
	5.1	Policies for information security	Y	Y	☐	☐	☑	
	5.2	Information security roles and responsibilities	Y	Y	☐	☐	☑	
	5.3	Segregation of duties	Y	Y	☐	☐	☑	
	5.4	Management responsibilities	Y	Y	☑	☐	☑	
	5.5	Contact with authorities	Y	Y	☐	☑	☑	
	5.6	Contact with special interest groups	Y	Y	☑	☑	☐	
	5.7	Threat intelligence	Y	Y	☑	☑	☐	
	5.8	Information security in project management	Y	Y	☑	☐	☐	
	5.9	Inventory of information and other associated assets	Y	Y	☑	☐	☑	
	5.10	Acceptable use of information and other associated assets	Y	Y	☑	☐	☑	
	5.11	Return of assets	Y	Y	☑	☐	☑	
	5.12	Classification of information	Y	Y	☑	☐	☑	
	5.13	Labelling of information	Y	Y	☑	☐	☐	
	5.14	Information transfer	Y	Y	☑	☐	☑	
	5.15	Access control	Y	Y	☑	☐	☑	
	5.16	Identity management	Y	Y	☑	☐	☑	
	5.17	Authentication information	Y	Y	☑	☐	☑	

5. Organizational controls	5.18	Access rights	Y	Y	☑	☐	☑	
	5.19	Information security in supplier relationships	Y	Y	☑	☐	☑	
	5.20	Addressing information security within supplier agreements	Y	Y	☑	☐	☑	
	5.21	Managing information security in the information and communication technology (ICT) supply chain	Y	Y	☑	☐	☐	
	5.22	Monitoring, review and change management of supplier services	Y	Y	☑	☐	☐	
	5.23	Information security for use of cloud services	Y	Y	☑	☑	☑	
	5.24	Information security incident management planning and preparation	Y	Y	☑	☑	☐	
	5.25	Assessment and decision on information security events	Y	Y	☑	☐	☑	
	5.26	Response to information security incidents	Y	Y	☑	☐	☐	
	5.27	Learning from information security incidents	Y	Y	☑	☐	☐	
	5.28	Collection of evidence	Y	Y	☑	☑	☐	
	5.29	Information security during disruption	Y	Y	☑	☐	☑	
	5.30	ICT readiness for business continuity	Y	Y	☑	☑	☑	
	5.31	Legal, statutory, regulatory and contractual requirements	Y	Y	☑	☑	☑	
	5.32	Intellectual property rights	Y	Y	☐	☑	☑	
	5.33	Protection of records	Y	Y	☐	☑	☑	
	5.34	Privacy and protection of personal identifiable information (PII)	Y	Y	☑	☑	☑	
	5.35	Independent review of information security	Y	Y	☐	☑	☑	
	5.36	Compliance with policies, rules and standards for information security	Y	Y	☐	☑	☐	
	5.37	Documented operating procedures	Y	Y	☑	☐	☐	
	6.1	Screening	Y	Y	☑	☐	☑	
	6.2	Terms and conditions of employment	Y	Y	☑	☐	☐	

6. People controls	6.3	Information security awareness, education and training	Y	Y	☑	☐	☑	
	6.4	Disciplinary process	Y	Y	☑	☐	☐	
	6.5	Responsibilities after termination or change of employment	Y	Y	☑	☐	☑	
	6.6	Confidentiality or non-disclosure agreements	Y	Y	☑	☑	☑	
	6.7	Remote working	Y	Y	☑	☐	☐	
	6.8	Information security event reporting	Y	Y	☑	☐	☐	
7. Physical controls	7.1	Physical security perimeters	Y	Y	☑	☐	☑	
	7.2	Physical entry	Y	Y	☑	☐	☑	
	7.3	Securing offices, rooms and facilities	Y	Y	☑	☐	☑	
	7.4	Physical security monitoring	Y	Y	☑	☑	☑	
	7.5	Protecting against physical and environmental threats	Y	Y	☑	☐	☑	
	7.6	Working in secure areas	Y	Y	☑	☐	☑	
	7.7	Clear desk and clear screen	Y	Y	☑	☐	☑	
	7.8	Equipment siting and protection	Y	Y	☑	☐	☑	
	7.9	Security of assets off-premises	Y	Y	☑	☐	☑	
	7.10	Storage media	Y	Y	☑	☐	☑	
	7.11	Supporting utilities	Y	Y	☑	☐	☑	
	7.12	Cabling security	Y	Y	☑	☐	☑	
	7.13	Equipment maintenance	Y	Y	☑	☐	☑	
	7.14	Secure disposal or re-use of equipment	Y	Y	☑	☐	☑	
	8.1	User end point devices	Y	Y	☑	☐	☐	
	8.2	Privileged access rights	Y	Y	☑	☐	☑	

	8.3	Information access restriction	Y	Y	☑	☐	☑	
	8.4	Access to source code	Y	Y	☑	☐	☑	
	8.5	Secure authentication	Y	Y	☑	☐	☑	
	8.6	Capacity management	Y	Y	☑	☐	☑	
	8.7	Protection against malware	Y	Y	☑	☐	☑	
	8.8	Management of technical vulnerabilities	Y	Y	☑	☐	☑	
	8.9	Configuration management	Y	Y	☑	☐	☑	
	8.10	Information deletion	Y	Y	☑	☑	☑	
	8.11	Data masking	Y	Y	☑	☑	☑	
	8.12	Data leakage prevention	Y	Y	☑	☑	☑	
	8.13	Information backup	Y	Y	☑	☐	☑	
	8.14	Redundancy of information processing facilities	Y	Y	☑	☐	☐	
8. Technological controls	8.15	Logging	Y	Y	☑	☐	☑	
	8.16	Monitoring activities	Y	Y	☑	☐	☑	
	8.17	Clock synchronization	Y	Y	☑	☐	☑	
	8.18	Use of privileged utility programs	Y	Y	☑	☐	☑	
	8.19	Installation of software on operational systems	Y	Y	☑	☐	☐	
	8.20	Networks security	Y	Y	☑	☐	☑	
	8.21	Security of network services	Y	Y	☑	☐	☑	
	8.22	Segregation of networks	Y	Y	☑	☐	☑	
	8.23	Web filtering	Y	Y	☑	☐	☐	
	8.24	Use of cryptography	Y	Y	☐	☐	☑	
	8.25	Secure development life cycle	Y	Y	☑	☐	☐	
	8.26	Application security requirements	Y	Y	☑	☐	☐	

	8.27	Secure system architecture and engineering principles	Y	Y	☑	☐	☐	
	8.28	Secure coding	Y	Y	☑	☐	☑	
	8.29	Security testing in development and acceptance	Y	Y	☑	☐	☐	
	8.30	Outsourced development	Y	Y	☑	☐	☑	
	8.31	Separation of development, test and production environments	Y	Y	☑	☐	☐	
	8.32	Change management	Y	Y	☑	☐	☐	
	8.33	Test information	Y	Y	☑	☐	☐	
	8.34	Protection of information systems during audit testing	Y	Y	☑	☐	☑	