Statement of Applicability

Organization ManpowerGroup, Diemerhof 16, 1112 XN Diemen

Date 26 May 2025

Section	Applicable	Information security control	Status	Validation for applicability OR reason for exclusion from scope: Policy	Risk analysis	Laws & Regulations
A5		**Organizational controls**				
A.5.1	√	Policies for information security	Implemented	√	√	
A.5.2	√	Information security roles and responsibilities	Implemented	√	√	
A.5.3	√	Segregation of duties	Implemented	√	√	
A.5.4	√	Management responsibilities	Implemented	√	√	
A.5.5	√	Contact with authorities	Implemented	√	√	
A.5.6	√	Contact with special interest groups	Implemented	√	√	
A.5.7	√	Threat intelligence	Implemented	√	√	
A.5.8	√	Information security in projectmanagement	Implemented	√	√	
A.5.9	√	Inventory of information and other associated assets	Implemented	√	√	
A.5.10	√	Acceptable use of information and other associated assets	Implemented	√	√	
A.5.11	√	Return of assets	Implemented	√	√	
A.5.12	√	Classification of information	Implemented	√	√	
A.5.13	√	Labelling of information	Implemented	√	√	
A.5.14	√	Information transfer	Implemented	√	√	
A.5.15	√	Access control	Implemented	√	√	
A.5.16	√	Identity management	Implemented	√	√	
A.5.17	√	Authentication information	Implemented	√	√	
A.5.18	√	Access rights	Implemented	√	√	
A.5.19	√	Information security in supplier relationships	Implemented	√	√	
A.5.20	√	Addressing information security within supplier agreements	Implemented	√	√	
A.5.21	√	Managing information security in the information and communication technology (ICT) supply-chain	Implemented	√	√	
A.5.22	√	Monitoring, review and change management of supplier services	Implemented	√	√	
A.5.23	√	Information security for use of cloud services	Implemented	√	√	
A.5.24	√	Information security incident management planning and preparation	Implemented	√	√	
A.5.25	√	Assessment and decision on information security events	Implemented	√	√	
A.5.26	√	Response to information security incidents	Implemented	√	√	√
A.5.27	√	Learning from information security incidents	Implemented	√	√	
A.5.28	√	Collection of evidence	Implemented	√	√	
A.5.29	√	Information security during disruption	Implemented	√	√	
A.5.30	√	ICT readiness for business continuity	Implemented	√	√	
A.5.31	√	Legal, statutory, regulatory and contractual requirements	Implemented	√	√	√
A.5.32	√	Intellectual property rights	Implemented	√	√	√
A.5.33	√	Protection of records	Implemented	√	√	√
A.5.34	√	Privacy and protection of personal identifiable information (PII)	Implemented	√	√	√
A.5.35	√	Independent review of information security	Implemented	√	√	
A.5.36	√	Compliance with policies, rules and standards for information security	Implemented	√	√	
A.5.37	√	Documented operating procedures	Implemented	√	√	
A6		**People controls**				
A.6.1	√	Screening	Implemented	√	√	
A.6.2	√	Terms and conditions of employment	Implemented	√	√	√
A.6.3	√	Information security awareness, education and training	Implemented	√	√	
A.6.4	√	Disciplinary process	Implemented	√	√	√
A.6.5	√	Responsibilities after termination or change of employment	Implemented	√	√	
A.6.6	√	Confidentiality or non-disclosure agreements	Implemented	√	√	
A.6.7	√	Remote working	Implemented	√	√	
A.6.8	√	Information security event reporting	Implemented	√	√	
A7		**Physical controls**				
A.7.1	√	Physical security perimeters	Implemented	√	√	
A.7.2	√	Physical entry	Implemented	√	√	

Statement of Applicability

Organization ManpowerGroup, Diemerhof 16, 1112 XN Diemen

Date 26 May 2025

Section	Applicable	Information security control	Status	Validation for applicability OR reason for exclusion from scope		
				Policy	Risk analysis	Laws & Regulations
A.7.3	√	Securing offices, rooms and facilities	Implemented	√	√	
A.7.4	√	Physical security monitoring	Implemented	√	√#1	
A.7.5	√	Protecting against physical and environmental threats	Implemented	√	√	
A.7.6	√	Working in secure areas	Implemented	√	√	
A.7.7	√	Clear desk and clear screen	Implemented	√	√	
A.7.8	√	Equipment siting and protection	Implemented	√	√	
A.7.9	√	Security of assets off-premises	Implemented	√	√	
A.7.10	√	Storage media	Implemented	√	√	
A.7.11	√	Supporting utilities	Implemented	√	√	
A.7.12	√	Cabling security	Implemented	√	√	
A.7.13	√	Equipment maintenance	Implemented	√	√	
A.7.14	√	Secure disposal or re-use of equipment	Implemented	√	√	
A8		**Technological controls**				
A.8.1	√	User end point devices	Implemented	√	√	
A.8.2	√	Privileged access rights	Implemented	√	√	
A.8.3	√	Information access restriction	Implemented	√	√	
A.8.4	X	Access to source code	Not Applicable	We don't develop software within the scope		
A.8.5	√	Secure authentication	Implemented	√	√	
A.8.6	√	Capacity management	Implemented	√	√	
A.8.7	√	Protection against malware	Implemented	√	√	
A.8.8	√	Management of technical vulnerabilities	Implemented	√	√	
A.8.9	√	Configuration management	Implemented	√	√	
A.8.10	√	Information deletion	Implemented	√	√	
A.8.11	√	Data masking	Implemented	√	√	
A.8.12	√	Data leakage prevention	Implemented	√	√	
A.8.13	√	Information backup	Implemented	√	√	
A.8.14	√	Redundancy of information processing facilities	Implemented	√	√	
A.8.15	√	Logging	Implemented	√	√	
A.8.16	√	Monitoring activities	Implemented	√	√	
A.8.17	√	Clock synchronization	Implemented	√	√	
A.8.18	√	Use of privileged utility programs	Implemented	√	√	
A.8.19	√	Installation of software on operational systems	Implemented	√	√	
A.8.20	√	Networks security	Implemented	√	√	
A.8.21	√	Security of network services	Implemented	√	√	
A.8.22	√	Segregation of networks	Implemented	√	√	
A.8.23	√	Web filtering	Implemented	√	√	
A.8.24	√	Use of cryptography	Implemented	√	√	
A.8.25	X	Secure development life cycle	Not Applicable	We don't develop software within the scope		
A.8.26	√	Application security requirements	Implemented	√	√	
A.8.27	X	Secure system architecture and engineering principles	Not Applicable	We don't develop software within the scope		
A.8.28	X	Secure coding	Not Applicable	We don't develop software within the scope		
A.8.29	√	Security testing in development and acceptance	Implemented	√	√	
A.8.30	X	Outsourced development	Not Applicable	We don't develop software within the scope		
A.8.31	√	Separation of development, test and production environments	Implemented	√	√	
A.8.32	√	Change management	Implemented	√	√	
A.8.33	√	Test information	Implemented	√	√	
A.8.34	√	Protection of information systems during audit testing	Implemented	√	√	

Statement of Applicability

Organization ManpowerGroup, Diemerhof 16, 1112 XN Diemen

Date 26 May 2025

Validation for applicability OR reason for exclusion from scope

Section	Applicable	Information security control	Status	Policy	Risk analysis	Laws & Regulations
#1	Physical security monitoring is fully implemented only at our headquarters in Diemen, as this is the sole location housing critical systems. The security measures in place are designed to prevent and detect unauthorized access, as well as to protect against break-ins and theft.					