Document classification : EcoVadis public

Statement of Applicability, Version 6

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, CO: contractual obligations, BR/BP: business requirements/adopted best practices, RRA: results of risk assessment, TSE: to some extent

ISO 27001:2013 Controls			Remarks (Justification for exclusion)	Applicable	Implementation
Clause	**Sec**	**Control Objective/Control**			
5 Security Policies	5.1	Management direction for information security			
	5.1.1	Policies for information security	BR/BP	Y	Y
	5.1.2	Review of the policies for information security	BR/BP	Y	Y
6 Organisation of information security	6.1	Internal organisation			
	6.1.1	Information security roles and responsibilities	BR/BP	Y	Y
	6.1.2	Segregation of duties	BR/BP	Y	Y
	6.1.3	Contact with authorities	BR/BP	Y	Y
	6.1.4	Contact with special interest groups	BR/BP	Y	Y
	6.1.5	Information security in project management	BR/BP	Y	in progress
	6.2	Mobile devices and teleworking	BR/BP		
	6.2.1	Mobile device policy	BR/BP	Y	Y
	6.2.2	Teleworking	BR/BP	Y	Y
7 Human resource security	7.1	Prior to employment			
	7.1.1	Screening	BR/BP	Y	Y
	7.1.2	Terms and conditions of employment	BR/BP	Y	Y
	7.2	During employment			
	7.2.1	Management responsibilities	BR/BP	Y	Y
	7.2.2	Information security awareness, education and training	BR/BP	Y	Y
	7.2.3	Disciplinary process	BR/BP	Y	Y
	7.3	Termination and change of employment			
	7.3.1	Termination or change of employment responsibilities	BR/BP	Y	Y
	8.1	Responsibility for assets			
	8.1.1	Inventory of assets	BR/BP	Y	Y
	8.1.2	Ownership of assets	BR/BP	Y	Y
	8.1.3	Acceptable use of assets	BR/BP	Y	Y

8 Asset management	8.1.4	Return of assets	BR/BP	Y	Y
	8.2	Information classification			
	8.2.1	Classification of information	BR/BP	Y	Y
	8.2.2	Labeling of information	BR/BP	Y	Y
	8.2.3	Handling of assets	BR/BP	Y	Y
	8.3	Media handling			
	8.3.1	Management of removable media	BR/BP	Y	Y
	8.3.2	Disposal of media	BR/BP	Y	Y
	8.3.3	Physical media transfer	BR/BP	Y	Y
9 Access control	9.1	Business requirements of access control			
	9.1.1	Access control policy	BR/BP	Y	Y
	9.1.2	Access to networks and network services	BR/BP	Y	Y
	9.2	User access management			
	9.2.1	User registration and de-registration	BR/BP	Y	Y
	9.2.2	User acces provisioning	BR/BP	Y	Y
	9.2.3	Management of privileged access rights	BR/BP	Y	Y
	9.2.4	Management of secret authentication information of users	BR/BP	Y	Y
	9.2.5	Review of user access rights	BR/BP	Y	Y
	9.2.6	Removal or adjustment of access rights	BR/BP	Y	Y
	9.3	User responsibilities			
	9.3.1	Use of secret authentication information	BR/BP	Y	Y
	9.4	System and application access control			
	9.4.1	Information access restriction	BR/BP	Y	Y
	9.4.2	Secure log-on procedures	BR/BP	Y	Y
	9.4.3	Password management system	BR/BP	Y	Y
	9.4.4	Use of privileged utility programs	BR/BP	Y	Y
	9.4.5	Access control to program source code	BR/BP	Y	Y
10 Cryptography	10.1	Cryptographic controls			
	10.1.1	Policy on the use of cryptographic controls	BR/BP	Y	in progress
	10.1.2	Key management	BR/BP	Y	in progress
	11.1	Secure areas			
	11.1.1	Physical security perimeter	BR/BP	Y	Y
	11.1.2	Physical entry controls	BR/BP	Y	Y
	11.1.3	Securing office, room and facilities	BR/BP	Y	Y

11 Physical and environmental security	11.1.4	Protecting against external end environmental threats	BR/BP	Y	Y
	11.1.5	Working in secure areas	BR/BP	Y	Y
	11.1.6	Delivery and loading areas	BR/BP	Y	Y
	11.2	Equipment			
	11.2.1	Equipment siting and protection	BR/BP	Y	Y
	11.2.2	Supporting utilities	BR/BP	Y	Y
	11.2.3	Cabling security	BR/BP	Y	Y
	11.2.4	Equipment maintenance	BR/BP	Y	Y
	11.2.5	Removal of assets	BR/BP	Y	Y
	11.2.6	Security of equipment and assets off-premises	BR/BP	Y	Y
	11.2.7	Security disposal or re-use of equipment	BR/BP	Y	Y
	11.2.8	Unattended user equipment	BR/BP	Y	Y
	11.2.9	Clear desk and clear screen policy	BR/BP	Y	Y
12 Operations security	12.1	Operational procedures and responsibilities			
	12.1.1	Documented operating procedures	BR/BP	Y	Y
	12.1.2	Change management	BR/BP	Y	Y
	12.1.3	Capacity management	BR/BP	Y	Y
	12.1.4	Separation of development, testing and operational environments	BR/BP	Y	Y
	12.2	Protection from malware			
	12.2.1	Controls against malware	BR/BP	Y	Y
	12.3	Backup			
	12.3.1	Information backup	BR/BP	Y	Y
	12.4	Logging and monitoring			
	12.4.1	Event logging	BR/BP	Y	Y
	12.4.2	Protection of log information	BR/BP	Y	Y
	12.4.3	Administrator and operator logs	BR/BP	Y	Y
	12.4.4	Clock synchronisation	BR/BP	Y	Y
	12.5	Control of operational software			
	12.5.1	Installation of software on operational systems	BR/BP	Y	Y
	12.6	Technical vulnerability management			
	12.6.1	Management of technical vulnerabilities	BR/BP	Y	Y
	12.6.2	Restrictions on software installation	BR/BP	Y	Y
	12.7	Information systems audit considerations			
	12.7.1	Information systems audit controls	BR/BP	Y	Y

13 Communications security	13.1	Network security management			
	13.1.1	Network controls	BR/BP	Y	Y
	13.1.2	Security of network services	BR/BP	Y	Y
	13.1.3	Segregation in networks	BR/BP	Y	Y
	13.2	Information transfer			
	13.2.1	Information transfer policies and procedures	BR/BP	Y	Y
	13.2.2	Agreements on information transfer	BR/BP	Y	Y
	13.2.3	Electronic messaging	BR/BP	Y	Y
	13.2.4	Confidentiality or non-disclosure agreements	BR/BP	Y	Y
14 System acquisition, development and maintenance	14.1	Security requirements of information systems			
	14.1.1	Security requirements analysis and specification	BR/BP	Y	Y
	14.1.2	Securing applications services on public networks	BR/BP	Y	Y
	14.1.3	Protecting application services transactions	BR/BP	Y	Y
	14.2	Security in development and support processes			
	14.2.1	Secure development policy	BR/BP	Y	Y
	14.2.2	System change control procedures	BR/BP	Y	Y
	14.2.3	Technical review of applications after operating platform changes	BR/BP	Y	Y
	14.2.4	Restrictions on changes to software packages	BR/BP	Y	Y
	14.2.5	Secure system engineering principles	BR/BP	Y	Y
	14.2.6	Secure development environment	BR/BP	Y	Y
	14.2.7	Outsourced development		NA	
	14.2.8	System security testing	BR/BP	Y	Y
	14.2.9	System acceptance testing	BR/BP	Y	Y
	14.3	Test data			
	14.3.1	Protection of test data	BR/BP	Y	Y
15 Supplier relationships	15.1	Security in supplier relationships			
	15.1.1	Information security policy for supplier relationships	BR/BP	Y	Y
	15.1.2	Addressing security within supplier agreements	BR/BP	Y	Y
	15.1.3	Information and Communication technology supply chain	BR/BP	Y	Y
	15.2	Supplier service delivery management			
	15.2.1	Monitoring and review of supplier services	BR/BP	Y	Y
	15.2.2	Managing changes to supplier services	BR/BP	Y	Y
	16.1	Management of information security incidents and improvements			

16 Information security incident management	16.1.1	Responsibilities and procedures	BR/BP	Y	Y	
	16.1.2	Reporting information security events	BR/BP	Y	Y	
	16.1.3	Reporting information security weaknesses	BR/BP	Y	Y	
	16.1.4	Assessment and decision on information security events	BR/BP	Y	Y	
	16.1.5	Response to information security incidents	BR/BP	Y	Y	
	16.1.6	Learning from information security incidents	BR/BP	Y	Y	
	16.1.7	Collection of evidences	BR/BP	Y	Y	
17 Information security aspects of business continuity management	17.1	Information security continuity				
	17.1.1	Planning information security continuity	BR/BP	Y	Y	
	17.1.2	Implementing information security continuity	BR/BP	Y	Y	
	17.1.3	Verify, review and evaluate information security continuity	BR/BP	Y	Y	
	17.2	Redundancies				
	17.2.1	Availability of information processing facilities	BR/BP	Y	in progress	
18 Compliance	18.1	Compliance with legal and contractual requirements				
	18.1.1	Identification of applicable legislation and contractual requirements	BR/BP	Y	Y	
	18.1.2	Intellectual property rights	BR/BP	Y	Y	
	18.1.3	Protection of records	BR/BP	Y	Y	
	18.1.4	Privacy and protection of personally identifiable information	BR/BP	Y	Y	
	18.1.5	Regulation of cryptographic controls	BR/BP	Y	Y	
	18.2	Information security reviews				
	18.2.1	Independent review of information security	BR/BP	Y	Y	
	18.2.2	Compliance with security policies and standards	BR/BP	Y	Y	
	18.2.3	Technical compliance review	BR/BP	Y	Y	