Statement of Applicability ISO27001:2013

February 2021

Version
3.0

Classification
Public

Document index

Author Unit QIS
Document name Statement of Applicability ISO27001:2013
Date February 2021
Distribution Public

Document history

Version	Explanation	Author	Date
0.1	First new draft	TransIP	2018-05-22
0.2	Reviewed and updated	TransIP	2018-05-28
0.3	Updated	TransIP	2018-07-13
0.4	Updated	TransIP	2018-09-20
1.0	Finalized for audit	TransIP	2018-09-24
1.1	Review for 2019 audit	TransIP	2019-10-21
1.2	Updated to include NEN 7510	TransIP	2019-11-01
2.0	Review for 2020 audit	Team.blue NL	2020-10-08
2.1	Updated to include NEN 7510 better	Team.blue NL	2020-11-23
3.0	NEN7510 removed and placed in separate SoA	Team.blue NL	2021-02-05

Contents

Introduction

This document contains the Statement of Applicability (hereinafter SoA) for the certification of the ISO27001:2013 standards. The purpose of this document is to identify the applicable control measures that must be implemented to monitor and manage the threats against the team.blue NL organization and business processes.

The control measures have been identified on the basis of the management measures included in the ISO27001:2013 standard as listed in Annex 1. The applicability is declared per control measure. For each applicable control measure, a reference is made to the relevant defined security control. If a control measure does not apply, an explanation is given for this.

Management Statement

The management of team.blue NL hereby declares that the measures mentioned in this SoA are validated in relation to the performed risk analyses and accepts any residual risk of measures not taken.

The management hereby confirms that all measures selected in this document have actually been implemented.

Mark van Teunenbroek, Managing Director team.blue NL
Leiden, February 2021

. Scope

ISO/IEC 27001:2013: Information security related to related to internet and IT Services, the registration of domain names, sales of webhosting, VPS and colocations and the development of tools needed in accordance with the Statement of Applicability version 3.0 2021.

. Statement of Applicability

Table Clarification

Columns 1-3 show the description and reference to the ISO27001:2013 Annex A controls.

Column "Reasons for selection" shows the reason why the control applies to team.blue NL and can have the following values:
- LR: Legal Requirements
- CO: Contractual Obligations
- BR/BP: Business Requirements/adopted Best Practices
- RRA: Results of Risk Assessment
- TSE: To Some Extent
- N/A: Not Applicable

The final columns show the associated policy and any additional remarks and if a control is excluded the reason why.

Statement of Applicability

ISO27001:2013 Controls				
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
5 Security Policies	**A5.1 Management direction for information security**			
	A5.1.1 Policies for information security	BR/BP	TBNL-POL-030	Management Systems Policy
	A5.1.2 Review of the policies for information security			
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
6 Organization of information security	**A6.1 Internal organization**			
	A6.1.1 Information security roles and responsibilities	BR/BP	TBNL-POL-030	Management Systems Policy
	A6.1.2 Segregation of duties	BR/RP	TBNL-POL-007	Access Control Policy
	A6.1.3 Contact with authorities	BR/BP/LR	TBNL-POL-030	Management Systems Policy
	A6.1.4 Contact with special interest groups	BR/BP		
	A6.1.5 Information security in Project management	BR/BP	TBNL-POL-031	Secure Development Policy
	A6.2 Mobile devices and teleworking			
	A6.2.1 Mobile device policy	BR/BP	TBNL-POL-029	Security Cookbook
	A6.2.2 Teleworking	BR/BP	TBNL-POL-012	Remote Working Policy
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
7 Human resource security	**A7.1 Prior to employment**			
	A7.1.1 Screening	BR/BP/LR	TBNL-POL-030	Management Systems Policy
	A7.1.2 Terms and conditions of employment			
	A7.2 During employment			
	A7.2.1 Management responsibilities	BR/BP	TBNL-POL-030	Management Systems Policy
	A7.2.2 Information security awareness, education and training			
	A7.2.3 Disciplinary process			
	A7.3 Termination and change of employment			
	A7.3.1 Termination or change of employment responsibilities	BR/BP	TBNL-POL-007	Access Control Policy
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
8 Asset management	**A8.1 Responsibilities for assets**			
	A8.1.1 Inventory of assets	BR/BP	TBNL-POL-030	Management Systems Policy
	A8.1.2 Ownership of assets			

	A8.1.3 Acceptable use of assets		TBNL-POL-006	Acceptable Use Policy
	A8.1.4 Return of assets			
	A8.2 Information classification			
	A8.2.1 Classification of information	BR/BP	TBNL-POL-013	Information Classification Policy
	A8.2.3 Handling of assets	BR/BP/LR	TBNL-POL-006	Acceptable Use Policy
	A8.3 Media handling			
	A8.3.1 Management of removable media	BR/BP/LR	TBNL-POL-006	Acceptable Use Policy
	A8.3.2 Disposal of media	RRA/LR		
	A8.3.3 Physical media transfer	BR/BP/LR	TBNL-POL-028	Equipment Siting and Protection
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
9 Access control	**A9.1 Business requirements of access control**			
	A9.1.1 Access control policy	BR/BP	TBNL-POL-007	Access Control Policy
	A9.1.2 Access to networks and network services	BR/BP/RRA		
	A9.2 User access management			
	A9.2.1 User registration and de-registration	BR/RP	TBNL-POL-030	Management Systems Policy
	A9.2.2 User access provisioning	RRA/BR/BP	TBNL-POL-007	Access Control Policy
			TBNL-POL-030	Management Systems Policy
	A9.2.3 Management of privileged access rights	BR/BP/LR	TBNL-POL-007	Access Control Policy
	A9.2.4 Management of secret authentication information of users	BR/BP		
	A9.2.5 Review of user access rights	BR/BP	TBNL-POL-030	Management Systems Policy
	A9.2.6 Removal or adjustment of access rights	BR/BP	TBNL-POL-007	Access Control Policy
			TBNL-POL-030	Management Systems Policy
	A9.3 User responsibilities			
	A9.3.1 Use of secret authentication information	BR/BP	TBNL-POL-016	Password Policy
			TBNL-POL-029	Security Cookbook
	A9.4 System and application access control			

	A9.4.1 Information access restriction	BR/BP/LR	TBNL-POL-007	Access Control Policy
	A9.4.2 Secure log-on procedures			
	A9.4.3 Password management system	BR/BP	TBNL-POL-016	Password Policy
	A9.4.4 Use of privileged utility programs	BR/BP	TBNL-POL-029	Security Cookbook
	A9.4.5 Access control to program source code	BR/BP	TBNL-POL-013	Information Classification Policy
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
10 Cryptography	**A10.1 Cryptographic controls**			
	A10.1.1 Policy on the use of cryptographic controls	BR/BP/LR	TBNL-POL-005	Acceptable Cryptography Policy
	A10.1.2 Key management	BR/BP/LR	TBNL-POL-016	Password Policy
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
11 Physical and environmental security	**A11.1 Secure areas**			
	A11.1.1 Physical security perimeter	RRA	TBNL-POL-024	Physical Access Policy
	A11.1.2 Physical entry controls	BR/BP		
	A11.1.3 Securing offices, rooms and facilities			
	A11.1.4 Protecting against external and environmental threats	BR/BP	TBNL-POL-029	Security Cookbook
	A11.1.5 Working in secure areas			
	A11.1.6 Delivery and loading areas	BR/BP	TBNL-POL-024	Physical Access Policy
	A11.2 Equipment			
	A11.2.1 Equipment siting and protection	BR/BP/LR	TBNL-POL-028	Equipment Siting and Protection
	A11.2.2 Supporting utilities	BR/BP	TBNL-POL-029	Security Cookbook
	A11.2.3 Cabling security	RRA/BR/BP		
	A11.2.4 Equipment maintenance	BR/BP/LR	TBNL-POL-028	Equipment Siting and Protection
	A11.2.5 Removal of assets			
	A11.2.6 Security of equipment and assets off premises			
	A11.2.7 Secure disposal or reuse of equipment			
	A11.2.8 Unattended user equipment	BR/BP/LR	TBNL-POL-029	Security Cookbook
	A11.2.9 Clear desk and clear screen policy			
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
	A12.1 Operational procedures and responsibilities			

12 Operations security	A12.1.1 Documented operating procedures	BR/BP	TBNL-POL-030	Management Systems Policy
	A12.1.2 Change management	BR/BP	TBNL-POL-032	Change Management Policy
	A12.1.3 Capacity management	BR/BP	TBNL-POL-028	Equipment Siting and Protection
	A12.1.4 Separation of development, Testing and operational environments	BR/BP	TBNL-POL-031	Secure Development Policy
	A12.2 Protection from malware			
	A12.2.1 Control against malware	BR/BP	TBNL-POL-029	Workplace Requirements
	A12.3 Backup			
	A12.3.1 Information backup	BR/BP	TBNL-POL-009	Backup Policy
	A12.4 Logging and monitoring			
	A12.4.1 Event logging	BR/BP/RRA	TBNL-POL-015	Logging and Monitoring Policy
	A12.4.2 Protection of log information	BR/BP/LR		
	A12.4.3 Administrator and operator logs	BR/BP/LR		
	A12.4.4 Clock synchronization	BR/BP/LR		
	A12.5 Control of operational software			
	A12.5.1 Installation of software on operational systems	BR/RP	TBNL-POL-023	System Hardening Policy
	A12.6 Technical vulnerability management			
	A12.6.1 Management of technical vulnerabilities	BR/BP/CO/LR	TBNL-POL-018	Patch and Vulnerability Management Policy
	A12.6.2 Restriction on software installation	BR/BP/CO	TBNL-POL-023	System Hardening Policy
	A12.7 Information systems audit considerations			
	A12.7.1 Information systems audit controls	BR/BP/CO	TBNL-POL-003	Internal AuditPolicy
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
13 Communications security	**A13.1 Network security management**			
	A13.1.1 Network controls	BR/BP/RRA	TBNL-POL-023	System Hardening Policy
	A13.1.2 Security of network services			
	A13.1.3 Segregation in networks			
	A13.2 Information transfer			
	A13.2.1 Information transfer policies and procedures	BR/BP/LR/CO	TBNL-POL-010	Data Transfer Policy
	A13.2.2 Agreements on information transfer			
	A13.2.3 Electronic messaging	BR/BP	TBNL-POL-019	Internal & External Communication Policy

	A13.2.4 Confidentiality or non-disclosure agreements	BR/BP	TBNL-POL-013	Information Classification Policy
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
14 System acquisition, development and maintenance	**A14.1 Security requirements of information systems**			
	A14.1.1 Information security requirements analysis and specification	BR/BP	TBNL-POL-031	Secure Development Policy
	A14.1.2 Securing application services on public networks			
	A14.1.3 Protecting application services transactions			
	A14.2 Security in development and support processes			
	A14.2.1 Secure development policy	BR/RP	TBNL-POL-031	Secure Development Policy
	A14.2.2 System change control procedures	BR/RP	TBNL-POL-023	System Hardening Policy
	A14.2.3 Technical review of applications after operating platform changes	BR/RP/LR	TBNL-POL-032	Change Management Policy
	A14.2.4 Restrictions on changes to software packages	BR/RP	TBNL-POL-023	System Hardening Policy
	A14.2.5 Secure system engineering principles	BR/RP		
	A14.2.6 Secure development environment	BR/RP	TBNL-POL-031	Secure Development Policy
	A14.2.7 Outsourced development	BR/RP		
	A14.2.8 System security testing	BR/RP	TBNL-POL-022	Security Testing Policy
	A14.2.9 System acceptance testing	BR/RP	TBNL-POL-031	Secure Development Policy
	A14.3 Test data			
	A14.3.1 Protecting of test data	BR/BP	TBNL-POL-031	Secure Development Policy
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
15 Supplier relationships	**A15.1 Information security in supplier relations**			
	A15.1.1 Information security policy for supplier relationships	BR/RP	TBNL-POL-002	Supplier Policy
	A15.1.2 Addressing security within supplier agreements			
	A15.1.3 Information and communication technology supply chain			
	A15.2 Supplier service delivery management			
	A15.2.1 Monitoring and review of supplier services	BR/RP	TBNL-POL-002	Supplier Policy
	A15.2.2 Managing changes to supplier services			
Clause	**Control Objectives ISO 27001:2013**	**Reasons for selection**	**Policy ID**	**Corresponding Policy**
	A16.1 Management of information security incidents and improvements			
	A16.1.1 Responsibilities and procedures	BR/RP		

16 Information security incident management	A16.1.2 Reporting information security events	BR/BP/LR	TBNL-POL-021	Information Security Incident Management Policy
	A16.1.3 Reporting information security weaknesses	BR/RP	TBNL-POL-018	Patch and Vulnerability Management Policy
	A16.1.4 Assessment of and decision on information security events	BR/RP	TBNL-POL-021	Information Security Incident Management Policy
	A16.1.5 Response to information security incidents	BR/RP	TBNL-POL-021	Information Security Incident Management Policy
			TBNL-POL-018	Patch and Vulnerability Management Policy
	A16.1.6 Learning from information security incidents	BR/RP	TBNL-POL-021	Information Security Incident Management Policy
	A16.1.7 Collection of evidence	BR/RP	TBNL-POL-015	Logging and Monitoring Policy

Clause	Control Objectives ISO 27001:2013	Reasons for selection	Policy ID	Corresponding Policy
17 Information security aspects of business continuity management	**A17.1 Informatiebeveiligingscontinuiteit**			
	A17.1.1 Planning information security continuity	BR/BP/LR	TBNL-POL-030	Management Systems Policy
	A17.1.2 Implementing information security continuity			
	A17.1.3 Verify, review and evaluate information security testing	BR/RP	TBNL-POL-021	Information Security Incident Management Policy
	A17.2 Redundancies			
	A17.2.1 Availability of information processing facilities	BR/BP/CO	TBNL-POL-031	Secure Development Policy

Clause	Control Objectives ISO 27001:2013	Reasons for selection	Policy ID	Corresponding Policy
18 Compliance	**A18.1 Compliance with legal and contractual requirements**			
	A18.1.1 Identification of applicable legislation and contractual requirements	BR/BP/LR	TBNL-POL-030	Management Systems Policy
	A18.1.2 Intellectual property rights	BR/BP/LR	TBNL-POL-014	Intellectual Property Rights Policy
	A18.1.3 Protection of records	BR/BP/LRBR/BP/LR	TBNL-POL-013	Information Classification Policy
	A18.1.4 Privacy and protection of personally identifiable information	BR/BP/LR		

	A18.1.5 Regulations of cryptographic controls	BR/BP/LR	TBNL-POL-005	Acceptable Cryptography Policy
	A18.2 Information security reviews			
	A18.2.1 Independent review of information security	BR/BP/LR	TBNL-POL-003	Internal AuditPolicy
	A18.2.2 Compliance with security policies and standards			
	A18.2.3 Technical compliance review			