Declaration of Applicability

Parantion Groep B.V.

ISO27001:2017

Document index

Author	Parantion Groep B.V.
Document name	Declaration of applicability_ISO_Directie_v4.3_jul2022_Openbaar.docx
Date	July 20th 2022
Distribution	Public

Toc

1. Introduction

This document contains the Declaration of Applicability for the purpose of certification for the ISO27001 standard. The purpose of this document is to identify the applicable control measures to be implemented in order to monitor and manage the threats against Parantion Groep B.V. and business processes.

The applicable control measures are identified on the basis of the control measures mentioned in the ISO 27001 standard Annex 1. For the applicable control measures, please refer to the defined ISO27002 'best practices' guidelines, which have been made specific for application in Parantion Groep B.V. business processes. If a control measure does not apply, an explanation is given for this.

2. Management statement

The Management Board of Parantion Groep B.V. hereby declares that it endorses the measures mentioned in this VVT in relation to the Risk Analysis carried out and accepts the residual risk of any measures not taken.

Deventer, 20-07-2022

Roel Smabers

3. Scope

Information security related to developing, consulting, implementing and providing support on the SaaS platform for portfolio management, personal development, and assessment applications.

4. Declaration of applicability

The Declaration of Applicability is shown in the following table with the following

5. Applicable measures

Measure nr.	Measure description	Reason for application	Implemented
A.5 Security policy			
A.05.01.01	Information security policy document	Baseline	Yes
A.05.01.02	Review of the information security policy	Baseline	Yes
A.6 Organization of information security			
A.06.01.01	Roles and responsibilities	Baseline	Yes
A.06.01.02	Segregation of duties	Baseline	Yes
A.06.01.03	Contact with authorities	Baseline	Yes
A.06.01.04	Contact with special interest groups	Baseline	Yes
A.06.01.05	Information security in project management	Risk analysis	Yes
A.06.02.01	Mobile device policy	Risk analysis	Yes
A.06.02.02	Teleworking	Risk analysis	Yes
A.7 Human resource security			
A.07.01.01	Screening	Risk analysis	Yes
A.07.01.02	Terms and conditions of employment	Baseline	Yes
A.07.02.01	Management responsibilities	Baseline	Yes
A.07.02.02	Information security awareness, education and training	Risk analysis	Yes
A.07.02.03	Disciplinary process	Risk analysis	Yes
A.07.03.01	Termination or change of employment	Risk analysis	Yes
A.8 Asset management			
A.08.01.01	Inventory of assets	Risk analysis	Yes
A.08.01.02	Ownership of assets	Risk analysis	Yes

A.08.01.03	Acceptable use of assets	Risk analysis	Yes
A.08.01.04	Return of assets	Risk analysis	Yes
A.08.02.01	Classification of information	Risk analysis	Yes
A.08.02.02	Labelling of information	Risk analysis	Yes
A.08.02.03	Handling of assets	Risk analysis	Yes
A.08.03.01	Management of removable media	Risk analysis	Yes
A.08.03.02	Disposal of media	Risk analysis	Yes
A.08.03.03	Physical media transfer	Risk analysis	Yes
A.9 Access control			
A.09.01.01	Access control policy	Baseline	Yes
A.09.01.02	Access to networks and network services	Risk analysis	Yes
A.09.02.01	User registration and de-registration	Risk analysis	Yes
A.09.02.02	User access provisioning	Risk analysis	Yes
A.09.02.03	Management of privileged access rights	Risk analysis	Yes
A.09.02.04	Management of secret authentication information of users	Risk analysis	Yes
A.09.02.05	Review of user access rights	Risk analysis	Yes
A.09.02.06	Removal or adjustment of access rights	Risk analysis	Yes
A.09.03.01	Use of secret authentication information	Risk analysis	Yes
A.09.04.01	Information access restriction	Risk analysis	Yes
A.09.04.02	Secure log-on procedures	Risk analysis	Yes
A.09.04.03	Password management system	Risk analysis	Yes
A.09.04.04	Use of privileged utility programs	Risk analysis	Yes
A.09.04.05	Access control to program source code	Risk analysis	Yes
A.10 Cryptography			
A.10.01.01	Policy on the use of cryptographic controls	Baseline	Yes
A.10.01.02	Key management	Risk analysis	Yes

A.11 Physical and environmental security			
A.11.01.01	Physical security perimeter	Risk analysis	Yes
A.11.01.02	Physical entry controls	Risk analysis	Yes
A.11.01.03	Securing offices, rooms and facilities	Risk analysis	Yes
A.11.01.04	Protecting against external and environmental threats	Risk analysis	Yes
A.11.01.05	Working in secure areas	Risk analysis	Yes
A.11.01.06	Delivery and loading areas	Risk analysis	Yes
A.11.02.01	Equipment siting and protection	Risk analysis	Yes
A.11.02.02	Supporting utilities	Risk analysis	Yes
A.11.02.03	Cabling security	Risk analysis	Yes
A.11.02.04	Equipment maintenance	Risk analysis	Yes
A.11.02.05	Removal of assets	Risk analysis	Yes
A.11.02.06	Security of equipment and assets off-premises	Risk analysis	Yes
A.11.02.07	Secure disposal or re-use of equipment	Risk analysis	Yes
A.11.02.08	Unattended user equipment	Risk analysis	Yes
A.11.02.09	Clear desk and clear screen policy	Risk analysis	Yes
A.12 Operations security			
A.12.01.01	Documented operating procedures	Risk analysis	Yes
A.12.01.02	Change management	Risk analysis	Yes
A.12.01.03	Capacity management	Risk analysis	Yes
A.12.01.04	Separation of development, testing and operational environments	Risk analysis	Yes
A.12.02.01	Controls against malware	Risk analysis	Yes
A.12.03.01	Information backup	Risk analysis	Yes
A.12.04.01	Event logging	Risk analysis	Yes
A.12.04.02	Protection of log information	Risk analysis	Yes

A.12.04.03	Administrator and operator logs	Risk analysis	Yes
A.12.04.04	Clock synchronisation	Risk analysis	Yes
A.12.05.01	Installation of software on operational systems	Risk analysis	Yes
A.12.06.01	Management of technical vulnerabilities	Risk analysis	Yes
A.12.06.02	Restrictions on software installation	Risk analysis	Yes
A.12.07.01	Information systems audit controls	Baseline	Yes
A.13 Communications security			
A.13.01.01	Network controls	Risk analysis	Yes
A.13.01.02	Security of network services	Risk analysis	Yes
A.13.01.03	Segregation in networks	Risk analysis	Yes
A.13.02.01	Information transfer policies and procedures	Baseline	Yes
A.13.02.02	Agreements on information transfer	Risk analysis	Yes
A.13.02.03	Electronic messaging	Risk analysis	Yes
A.13.02.04	Confidentiality or non-disclosure agreements	Risk analysis	Yes
A.14 System acquisition, development and maintenance			
A.14.01.01	Information security requirements analysis and specification	Risk analysis	Yes
A.14.01.02	Securing application services on public networks	Risk analysis	Yes
A.14.01.03	Protecting application services transactions	Risk analysis	Yes
A.14.02.01	Secure development policy	Risk analysis	Yes
A.14.02.02	System change control procedures	Risk analysis	Yes
A.14.02.03	Technical review of applications after operating platform changes	Risk analysis	Yes
A.14.02.04	Restrictions on changes to software packages	Risk analysis	Yes
A.14.02.05	Secure system engineering principles	Risk analysis	Yes
A.14.02.06	Secure development environment	Risk analysis	Yes
A.14.02.08	System security testing	Risk analysis	Yes
A.14.02.09	System acceptance testing	Risk analysis	Yes

A.14.03.01	Protection of test data	Risk analysis	Yes
A.15 Supplier relationships			
A.15.01.01	Information security policy for supplier relationships	Risk analysis	Yes
A.15.01.02	Addressing security within supplier agreements	Risk analysis	Yes
A.15.01.03	Information and communication technology supply chain	Risk analysis	Yes
A.15.02.01	Monitoring and review of supplier services	Risk analysis	Yes
A.15.02.02	Managing changes to supplier services	Risk analysis	Yes
A.16 Information security incident management			
A.16.01.01	Responsibilities and procedures	Baseline	Yes
A.16.01.02	Reporting information security events	Baseline	Yes
A.16.01.03	Reporting information security weaknesses	Baseline	Yes
A.16.01.04	Assessment of and decision on information security events	Baseline	Yes
A.16.01.05	Response to information security incidents	Baseline	Yes
A.16.01.06	Learning from information security incidents	Baseline	Yes
A.16.01.07	Collection of evidence	Baseline	Yes
A.17 Information security aspects of business continuity management			
A.17.01.01	Planning information security continuity	Baseline	Yes
A.17.01.02	Implementing information security continuity	Baseline	Yes
A.17.01.03	Verify, review and evaluate information security continuity	Baseline	Yes
A.17.02.01	Availability of information processing facilities	Baseline	Yes
A.18 Compliance; with internal requirements, such as policies, and with external requirements, such as laws			
A.18.01.01	Identification of applicable legislation and contractual requirements	Baseline	Yes
A.18.01.02	Intellectual property rights	Laws and regulations	Yes
A.18.01.03	Protection of records	Risk analysis	Yes
A.18.01.04	Privacy and protection of personally identifiable information	Laws and regulations	Yes
A.18.01.05	Regulation of cryptographic controls	Baseline	Yes

A.18.02.01	Independent review of information security	Baseline	Yes
A.18.02.02	Compliance with security policies and standards	Baseline	Yes
A.18.02.03	Technical compliance review	Baseline	Yes

6. Not Applicable measures

The following measures shall not apply to Parantion. However, they are included in the Annual Review and Risk Assessment.

Measure nr.	Measure description	Reason not applicable	Implemented
A.14.02.07	Outsourced development	Parantion does not outsource the development of software. Parantion does the development of its applications within the organisation itself.	No