Statement of Applicability
Proximus NXT Nederland B.V.

ISO27001:2022 & NEN7510-2024

1 Declaration ISO certification

Proximus NXT Nederland B.V.

ISO 27001:2022 & NEN7510-2024 Statement of Applicability

As a professional organization, we take seriously our commitment to protecting all our information, whether this information relates to staff members, clients, visitors, suppliers or others. Staff members must remain vigilant at all times, aware of the potential risks to information security that exist throughout our organization and our day-to-day business. This is an issue of fundamental concern to us all.

For that reason, we are engaged upon an active continuous program of improvement, aimed at ensuring that all information under our control remains as secure as possible. This program is fully in compliance with the International Standard ISO 27001:2022, Dutch legislation and our contractual obligations. As foundation of this program, we ensure that we maintain a comprehensive range of security policies and procedures, aimed at providing staff members with 'best practice' guidance on how to help protect our organization from the risks of disclosure, inaccuracy, incompleteness or unavailability of its information.

We urge every staff member to be fully conversant with, and to observe, all those policies that apply directly to them in their working life; and remind all managers that they must ensure that all policies are adequately implemented and enforced. Furthermore, we will be specifically asking all managers to conduct regular Risk Analysis reviews to ensure that the approved security measures remain effective in minimizing all potential threats, and that there are no major changes to either the ICT systems or the surrounding environment, that pose new risks.

Only by us taking responsibility for our own actions, we can truly aim to ensure that we achieve optimum levels of information security.

The Board of Directors of Proximus NXT Nederland B.V. confirms all in this Statement of Applicability identified controls related to the executed risk assessments, the justified exclusions and accepts the residual risks.

Utrecht, 8-07-2026

R. van Heek
Managing Director
Proximus NXT Nederland B.V.

2 Scope

2.1 Scope

The scope of the ISMS of Proximus NXT is:

“Consultancy, verkoop, levering, installatie, implementatie, beheer, service en beveiliging van IT-platforms.”

according to ISO27001:2022 & NEN7510-2024

2.2 Explanation

Applicable and **implemented**: Y/N

Applicable but not yet implemented: Y/(TBI)

HLT controls are health related controls and not applicable to ISO27001:2022

Reason Selection:

-	NA	Non-Applicable (Non existent in framework)
-	RRA	Result Risk Assessment
-	BR/BP	Business Requirements/Best Practices
-	SR/LR	Standard Requirements (ISO) 27001/Legal Requirements (e.g. AVG/GDPR)
-	CO	Contractual Obligations

2.3 Related Norms and documents

ISO 27002:2022 Code of Practice (NL: Code voor Informatiebeveiliging)

NEN7510-2024 -Medische informatica – Informatiebeveiliging in de zorg – Deel 1: Managementsysteem

ISMS policies and documents

3 Statement of Applicability

3.1 Introduction

The table below reflects all measures of the ISO27001:2022 and NEN7510-2024. The status of each measure is shown below in columns 'A27001' and 'NEN7510', where 'Y' means that the measure is implemented. When a measure is excluded/not implemented, an explanation is given under column 'Justification'.

3.2 Overview of measures (Annex A)

A.5 Organizational controls

Control	Description	A 27001	NEN7510	RRA	BR/BP	SR/LR	CO	Justification
A.5.1	Policies for information security	Y	Y			SR	CO	
A.5.2	Information security roles and responsibilities	Y	Y			SR		
A.5.3	Segregation of duties	Y	Y		BP	SR		
A.5.4	Management responsibilities	Y	Y			SR	CO	
A.5.5	Contact with authorities	Y	Y			SR/LR		
A.5.6	Contact with special interest groups	Y	Y		BP			
A.5.7	Threat intelligence	Y	Y		BP			
A.5.8	Information security in project management	Y	Y			SR		
A.5.9	Inventory of information and other associated assets	Y	Y			SR		
A.5.10	Acceptable use of information and other associated assets	Y	Y			SR		
A.5.11	Return of assets	Y	Y			SR		
A.5.12	Classification of information	Y	Y			SR		

A.5.13	Labeling of information	Y	Y		BP			
A.5.14	Information transfer	Y	Y			SR/LR	CO	
A.5.15	Access control	Y	Y			SR/LR		
A.5.16	Identity management	Y	Y		BP			
A.5.17	Authentication information	Y	Y		BP			
A.5.18	Access rights	Y	Y		BP		CO	
A.5.19	Information security in supplier relationships	Y	Y			SR	CO	
A.5.20	Addressing information security within supplier agreements	Y	Y		BP	LR	CO	
A.5.21	Managing information security in the information and communication technology (ICT) supply chain	Y	Y			LR	CO	
A.5.22	Monitoring, review and change management of supplier services	Y	Y		BP			
A.5.23	Information security for use of cloud services	Y	Y		BP			
A.5.24	Information security incident management planning and preparation	Y	Y		BP	SR/LR	CO	
A.5.25	Assessment and decision on information security events	Y	Y			SR		
A.5.26	Response to information security incidents	Y	Y			SR/LR	CO	
A.5.27	Learning from information security incidents	Y	Y			SR	CO	
A.5.28	Collection of evidence	Y	Y			SR/LR	CO	
A.5.29	Information security during disruption	Y	Y		BP		CO	
A.5.30	ICT readiness for business continuity	Y	Y		BR	SR	CO	

A.5.31	Legal, statutory, regulatory and contractual requirements	Y	Y			LR	CO	
A.5.32	Intellectual property rights	Y	Y			SR/LR	CO	
A.5.33	Protection of records	Y	Y			SR/LR	CO	
A.5.34	Privacy and protection of personal identifiable information (PII)	Y	Y			LR	CO	
A.5.35	Independent review of information security	Y	Y		BR	SR	CO	
A.5.36	Compliance with policies, rules and standards of information security	Y	Y		BR	SR		
A.5.37	Documented operating procedures	Y	Y			SR	CO	
A.5.38	HLT -Analyse en specificatie van informatiebeveiligingseisen	NA	Y			SR		
A.5.39	HLT-Zorgontvangers op unieke wijze identificeren	NA	N					PXS NXT werkt niet met patiënten en hoeft geen patienten te identificeren
A.5.40	HLT- Validatie van getoonde/geprinte gegevens	NA	N					PXS heeft geen toegang tot gezondheidsinformatie en wordt voorzien van versleuteling.
A.5.41	HLT- Openbaar beschikbare gezondheidsinformatie	NA	N					PXS heeft geen toegang tot gezondheidsinformatie en wordt voorzien van versleuteling.
A.5.42	HLT-Communicatie in noodsituaties	NA	N					PXS NXT is geen zorgorganisatie en staat niet onder toezicht van een zorg toezichthouder
A.5.43	HLT-Incidenten extern melden	NA	Y			LR	CO	

A.6 People controls

Control	Description	A 27001	NEN7510	RRA	BR/BP	SR/LR	CO	Justification
A.6.1	Screening	Y	Y		BR/BP	SR	CO	
A.6.2	Terms and conditions of employment	Y	Y		BP		CO	
A.6.3	Information security awareness, education and training	Y	Y		BP	SR	CO	
A.6.4	Disciplinary process	Y	Y		BR/BP			
A.6.5	Responsibilities after termination or change of employment	Y	Y		BP			
A.6.6	Confidentiality or non-disclosure agreements	Y	Y		BR	SR/LR		
A.6.7	Remote working	Y	Y		BP			
A.6.8	Information security event reporting	Y	Y			SR		
A.6.9	HLT-Managementtraining	NA	N			SR		Dit is gericht op zorgorganisaties. Training en awareness (6.3) geeft voldoende invulling.

A.7 Physical controls

Control	Description	A 27001	NEN7510	RRA	BR/BP	SR/LR	CO	Justification
A.7.1	Physical security perimeters	Y	Y		BP			
A.7.2	Physical entry	Y	Y		BP		CO	
A.7.3	Securing offices, rooms, and facilities	Y	Y			SR	CO	
A.7.4	Physical security monitoring	Y	Y		BP		CO	
A.7.5	Protecting against physical and environmental threats	Y	Y			SR/LR	CO	
A.7.6	Working in secure areas	Y	Y		BP	SR/LR		
A.7.7	Clear desk and clear screen	Y	Y			SR		
A.7.8	Equipment siting and protection	Y	Y		BP			
A.7.9	Security of assets off-premises	Y	Y		BP			
A.7.10	Storage media	Y	N		BP		CO	PXS NXT verwerkt geen zorginformatie op verwijderbare media
A.7.11	Supporting utilities	Y	Y		BP		CO	
A.7.12	Cabling security	Y	Y		BP			
A.7.13	Equipment maintenance	Y	Y					

A.7.14	Secure disposal or re-use of equipment	Y	Y		BP		CO	

A.8 Technological controls

Control	Description	A 27001	NEN7510	RRA	BR/BP	SR/LR	CO	Justification
A.8.1	User end point devices	Y	Y		BP			
A.8.2	Privileged access rights	Y	Y		BP		CO	
A.8.3	Information access restriction	Y	Y			SR	CO	
A.8.4	Access to source code	Y	Y				CO	
A.8.5	Secure authentication	Y	Y		BP		CO	
A.8.6	Capacity management	Y	Y		BP		CO	
A.8.7	Protection against malware	Y	Y			SR/LR	CO	
A.8.8	Management of technical vulnerabilities	Y	Y		BP			
A.8.9	Configuration management	Y	Y		BP	SR		
A.8.10	Information deletion	Y	Y			LR	CO	
A.8.11	Data masking	Y (TBI)	Y	RRA		LR		

A.8.12	Data leakage prevention	Y	Y			SL/LR		
A.8.13	Information backup	Y	Y			SR	CO	
A.8.14	Redundancy of information processing facilities	Y	Y		BP			
A.8.15	Logging	Y	Y			SR/LR	CO	
A.8.16	Monitoring activities	Y	Y		BR		CO	
A.8.17	Clock synchronization	Y	Y		BP			
A.8.18	Use of privileged utility programs	Y	Y		BP			
A.8.19	Installation of software on operational systems	Y	Y			SR		
A.8.20	Networks security	Y	Y		BP		CO	
A.8.21	Security of network services	Y	Y		BP		CO	
A.8.22	Segregation of networks	Y	Y		BP		CO	
A.8.23	Web filtering	Y	Y	RRA			CO	
A.8.24	Use of cryptography	Y	Y			SR		
A.8.25	Secure development life cycle	Y	Y			SR	CO	
A.8.26	Application security requirements	Y	Y		BP			

A.8.27	Secure system architecture and engineering principles	Y	Y		BR		CO	
A.8.28	Secure coding	Y	Y		BP		CO	
A.8.29	Security testing in development and acceptance	Y	Y		BR		CO	
A.8.30	Outsourced development	Y	Y		BR		CO	
A.8.31	Separation of development, test and production environment	Y	Y		BP		CO	
A.8.32	Change management	Y	Y			SR	CO	
A.8.33	Test information	Y	Y		BP			
A.8.34	Protection of information systems during audit testing	Y	Y			SR		
A.8.35	HLT-Zero trust beginselen	NA	N				CO	PXS NXT is geen zorgorganisatie Geen verzoek van zorgklanten om dit toe te passen.