# . Statement of Applicability NEN 7510:2017

November 2020

**Version**
2.1

**Classification**
Public

## . Document index

| | |
|---|---|
| **Author** | Unit QIS |
| **Document name** | Statement of Applicability NEN 7510:2017 |
| **Date** | November 2020 |
| **Distribution** | Public |

### Document history

| Version | Explanation | Author | Date |
|---|---|---|---|
| **0.1** | First new draft | team.blue NL | 2020-10-09 |
| **0.2** | Reviewed and updated | team.blue NL | 2020-10-19 |
| **1.0** | Finalized | team.blue NL | 2020-10-27 |
| **1.1** | Minor updates | team.blue NL | 2020-10-30 |
| **2.0** | Finalized | team.blue NL | 2020-11-06 |
| **2.1** | Added last feedback | team.blue NL | 2020-11-23 |

## Contents

## Introduction

This document contains the Statement of Applicability (hereinafter SoA) for the certification of the NEN7510:2017 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 NEN7510:2017 standard. 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, November 2020

## Scope

NEN 7510-1:2017: 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 register of processing V1.5, d.d. 26-07-2019 and the Statement of Applicability version 1.0 2021.

## Statement of Applicability

### Table Clarification

Columns 1-3 show the description and reference to the NEN7510:2017 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

| NEN 7510:2017 Controls | | | | |
|---|---|---|---|---|
| **Clause** | **Control Objectives NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| **5 Security Policies** | **A5.1 Management direction for information security** | | | |
| | A5.1.1 Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door hetmanagement wordt goedgekeurd, wordtgepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen | BR/BP | TBNL-POL-030 | Management Systems Policy<br>The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | A5.1.2 Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan. | BR/BP | TBNL-POL-030 | Management Systems Policy |
| | | | | |
| **Clause** | **Control Objectives NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| **6 Organization of information security** | **A6.1 Internal organization** | | | |
| | A6.1.1 Organisaties moeten:<br>a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen<br>b) over een informatiebeveiligingsmanagementforum (IBMF) beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie, zoals beschreven in B3 en B4 van bijlage B (6.1.1) in NEN 7510-2.<br>Er moet minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie.<br>Het gezondheidsinformatie-beveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen.<br>(Het is meestal het effectiefst als het forum vergadert op een tijdstip halverwege tussen twee vergaderingen van het bestuursorgaan waaraan het forum rapporteert. Zo kunnen urgente zaken binnen een korte periode in een | BR/BP | TBNL-POL-030 | Management Systems Policy |

| | | | | |
|---|---|---|---|---|
| | geschikte vergadering worden besproken.)<br>Er moet een formele verklaring van het toepassings-gebied worden geproduceerd waarin de grens wordt gedefinieerd van nalevingsactiviteiten wat betreft mensen, processen, plekken, platformen en toepassingen. | | | |
| | A6.1.2 Organisaties moeten, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden scheiden teneinde de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie. | BR/RP | TBNL-POL-007 | Access Control Policy<br>The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | 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 | TBNL-POL-030 | Management Systems Policy |
| | A6.1.5 Zorgspecifieke beheersmaatregel<br>Bij het management van projecten moet de patiëntveiligheid als projectrisico in aanmerking worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie. | 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 NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| **7 Human resource security** | **A7.1 Prior to employment** | | | |
| | A7.1 .1 Organisaties moeten minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie verifiëren.<br>Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband moeten een verificatie omvatten van de toepasselijke kwalificaties voor zorgverleners, indien er sprake is van accreditatie voor de beroepsgroep op basis van die kwalificaties (bijv. artsen, verplegend personeel enz.) | BR/BP/LR | TBNL-POL-030 | Management Systems Policy |

| | | | | |
|---|---|---|---|---|
| | Als een persoon wordt ingehuurd voor een specifieke beveiligingsfunctie, moet de organisatie zich ervan vergewissen dat:<br>a) de kandidaat over de nodige competentie beschikt om de beveiligingsfunctie te vervullen;<br>b) de functie de kandidaat toevertrouwd kan worden, in het bijzonder als de functie cruciaal is voor de organisatie. | | | |
| | A7.1.2 Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, moeten die betrokkenheid in relevante functieomschrijvingen vastleggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, moeten ook in relevante functieom-schrijvingen worden vastgelegd.<br>Er moet speciale aandacht worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband zoals vervangers, studenten, stagiairs enz. | BR/BP/LR | TBNL-POL-030 | Management Systems Policy |
| | **A7.2 During employment** | | | |
| | A7.2.1 Management responsibilities | BR/BP | TBNL-POL-030 | Management Systems Policy |
| | A7.2.2 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleid en -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde-contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken. Werknemers van de organisatie en, waar relevant, derdecontractanten moeten worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging. | BR/BP | TBNL-POL-030 | Management Systems Policy |
| | A7.2.3 Disciplinary process | BR/BP | TBNL-POL-030 | Management Systems Policy |

| | | | | |
|---|---|---|---|---|
| | **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 NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| **8 Asset management** | **A8.1 Responsibilities for assets** | | | |
| | A8.1.1 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten:<br>a) verantwoording afleggen over informatie-bedrijfsmiddelen (d.w.z. een inventaris<br>bijhouden van dergelijke bedrijfsmiddelen);<br>b) een eigenaar hebben aangewezen voor deze<br>informatiebedrijfsmiddelen (zie 8.1.2);<br>c) regels hebben voor het aanvaardbare gebruik van<br>deze bedrijfsmiddelen die geïdentificeerd,<br>gedocumenteerd en geïmplementeerd worden. | BR/BP | TBNL-POL-030 | Management Systems Policy<br><br>The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | A8.1.2 Ownership of assets | BR/BP | TBNL-POL-030 | Management Systems Policy |
| | A8.1.3 Acceptable use of assets | BR/BP | TBNL-POL-006 | Acceptable Use Policy |
| | A8.1.4 Teruggeven van bedrijfsmiddelen;<br>Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, teruggeven en erop toezien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was. | BR/BP | TBNL-POL-006 | Acceptable Use Policy |
| | **A8.2 Information classification** | | | |
| | A8.2.1 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren. | BR/BP | TBNL-POL-013 | Information Classification Policy |
| | A8.2.2 Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de gebruikers wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is vanaf het systeem (bijv. bij het opstarten of inloggen), enmoeten papieren output als vertrouwelijk labelen | N/A | N/A | We do not make direct use of health information systems |

| | | | | |
|---|---|---|---|---|
| | als die output persoonlijke gezondheidsinformatie bevat. | | | |
| | A8.2.3 Handling of assets | BR/BP/LR | TBNL-POL-006 | Acceptable Use Policy |
| | **A8.3 Media handling** | | | |
| | A8.3.1 Media die persoonlijke gezondheidsinformatie bevatten moeten fysiek worden beschermd of de gegevens ervan moeten versleuteld worden. De status en locatie van media die niet-versleutelde persoonlijke gezondheidsinformatie bevatten, moeten gemonitord worden. | BR/BP/LR | TBNL-POL-006 | Acceptable Use Policy<br>Sidenote, we do not manage health information systems ourselves |
| | A8.3.2 Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anders moeten de media wor-den vernietigd als ze niet meer gebruikt hoeven te worden. | RRA/LR | TBNL-POL-006 | Acceptable Use Policy<br>The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | A8.3.3 Physical media transfer | BR/BP/LR | TBNL-POL-028 | Equipment Siting and Protection |
| | | | | |
| **Clause** | **Control Objectives NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| **9 Access control** | **A9.1 Business requirements of access control** | | | |
| | A9.1.1 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheids-informatiesystemen hun toegang tot persoonlijke gezondheidsinformatie beperken tot situaties:<br>a) waarin er een zorgrelatie bestaat tussen de gebruiker<br>en de persoon waarop de gegevens betrekking<br>hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt);<br>b) waarin de gebruiker een activiteit uitvoert namens de<br>persoon waarop de gegevens betrekking hebben;<br>c) waarin er specifieke gegevens nodig zijn om deze<br>activiteit te ondersteunen.<br>Organisaties die persoonlijke gezondheidsinformatie<br>verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld.<br>Het beleid van de organisatie met betrekking tot | BR/BP | TBNL-POL-007 | Access Control Policy<br>We do not have direct access to customer data. |

| | | | | |
|---|---|---|---|---|
| | toegangscontrole moet worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol. Het toegangscontrolebeleid, als bestanddeel van het in | | | |
| | A9.1.2 Access to networks and network services | BR/BP/RRA | TBNL-POL-007 | Access Control Policy |
| | A9.2 User access management | | | |
| | A9.2.1 De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers moeten garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratiegegevens moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is. | 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 | TBNL-POL-007 | Access Control Policy |
| | A9.2.4 Management of secret authentication information of users | BR/BP | TBNL-POL-030 | Management Systems Policy |
| | A9.2.6 Alle organisaties die persoonlijke gezondheidsinformatie verwerken moeten voor elke vertrekkende afdelings- of tijdelijke medewerker, derde-contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaamheden als contractant of vrijwilliger de | N/A | N/A | The measure specific to medical services is identical to the ISO 27001:2013 requirement |

| | | | | |
|---|---|---|---|---|
| | toegangsrechten als gebruikers tot dergelijke informatie beëindigen. | | | |
| | **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 Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie moet geïsoleerd(en gescheiden) worden van de toegang tot informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie. | BR/BP/LR | TBNL-POL-007 | Access Control Policy |
| | A9.4.2 Secure log-on procedures | BR/BP/LR | TBNL-POL-007 | Access Control Policy |
| | 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 NEN 7510** | **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 NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| | **A11.1 Secure areas** | | | |

| | | | | |
|---|---|---|---|---|
| **11 Physical and environmental security** | A11.1.1 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gebruik maken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheidstoepassingen ondersteunen. Deze beveiligde gebieden moeten worden beschermd door passende beheersmaatregelen voor de fysieke toegang om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. | RRA | TBNL-POL-024 | Physical Access Policy<br>The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | A11.1.2 Physical entry controls | BR/BP | TBNL-POL-024 | Physical Access Policy |
| | A11.1.3 Securing offices, rooms and facilities | BR/BP | TBNL-POL-024 | Physical Access Policy |
| | A11.1.4 Protecting against external and environmental threats | BR/BP | TBNL-POL-029 | Security Cookbook |
| | A11.1.5 Working in secure areas | BR/BP | TBNL-POL-029 | Security Cookbook |
| | 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 | TBNL-POL-029 | Security Cookbook |
| | A11.2.4 Equipment maintenance | BR/BP/LR | TBNL-POL-028 | Equipment Siting and Protection |
| | A11.2.5 Organisaties die uitrusting, gegevens of software voor het ondersteunen van een zorgtoepassing met persoonlijke gezondheidsinformatie leveren of gebruiken, mogen niet toestaan dat die uitrusting, gegevens of software van de locatie wordt of worden verwijderd of er binnen wordt of worden verplaatst zonder dat de organisatie hiervoor haar goedkeuring heeft gegeven. | BR/BP/LR | TBNL-POL-028 | Equipment Siting and Protection |
| | A11.2.6 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit moet apparatuur omvatten die door werknemers op afstand wordt gebruikt, | BR/BP/LR | TBNL-POL-028 | Equipment Siting and Protection |

| | | | | |
|---|---|---|---|---|
| | zelfs indien dit gebruik permanent is (d.w.z. waar het een kernaspect is van de rol van de werknemer, zoals het geval is bij ambulancepersoneel, therapeuten enz.) | | | |
| | A11.2.7 Organisaties die gezondheidsinformatie verwerken, moeten alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig wissen of vernietigen als ze niet meer gebruikt hoeven te worden. | BR/BP/LR | TBNL-POL-028 | Equipment Siting and Protection<br>The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | A11.2.8 Unattended user equipment | BR/BP/LR | TBNL-POL-029 | Security Cookbook |
| | A11.2.9 Clear desk and clear screen policy | BR/BP/LR | TBNL-POL-029 | Security Cookbook |
| | | | | |
| **Clause** | **Control Objectives NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| **12 Operations security** | **A12.1 Operational procedures and responsibilities** | | | |
| | A12.1.1 Documented operating procedures | BR/BP | TBNL-POL-030 | Management Systems Policy |
| | A12.1.2 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigingsbeheersproces beheersen om de gepaste beheersing van host-toepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen. | 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 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten ontwikkel- en testomgevingen voor gezondheidsinformatiesyste-men die dergelijke informatie verwerken (fysiek of virtueel) scheiden van operationele omgevingen waar die gezondheidsinformatiesystemen gehost worden. Er moeten regels voor het migreren van software van de ontwikkel- naar een operationele status worden gedefinieerd en gedocumenteerd door de organisatie die de betroffen toepassing(en) host. | BR/BP | TBNL-POL-031 | Secure Development Policy |
| | **A12.2 Protection from malware** | | | |
| | A12.2.1 Organisaties die persoonlijke gezondheidsinformatie verwerken, | BR/BP | | Security Cookbook |

| | | | | |
|---|---|---|---|---|
| | moeten gepaste preventie-, detectie- en responsbeheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software, en passende bewustzijnstraining voor gebruikers implementeren. | | TBNL-POL-029 | The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | **A12.3 Backup** | | | |
| | A12.3.1 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten back-ups maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving opslaan om te garanderen dat de informatie in de toekomst beschikbaar is.<br>Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie. | N/A | N/A | N/A |
| | **A12.4 Logging and monitoring** | | | |
| | A12.4.1 Event logging | BR/BP/RRA | TBNL-POL-015 | Logging and Monitoring Policy |
| | A12.4.2 Auditverslagen moeten beveiligd zijn en niet gemanipuleerd kunnen worden. De toegang tot hulpmiddelen voor audits van systemen en audittrajecten moet worden beveiligd om misbruik of compromittering te voorkomen. | BR/BP/LR | TBNL-POL-015 | Logging and Monitoring Policy |
| | A12.4.3 Administrator and operator logs | BR/BP/LR | TBNL-POL-015 | Logging and Monitoring Policy |
| | A12.4.4 Gezondheidsinformatiesystemen die tijd-kritische activiteiten voor gedeelde zorg ondersteunen, moeten in tijdssynchronisatiediensten voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen. | BR/BP/LR | TBNL-POL-015 | Logging and Monitoring Policy<br>The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | **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 Audit Policy |

| Clause | Control Objectives NEN 7510 | 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 | BR/BP/RRA | TBNL-POL-023 | System Hardening Policy |
| | **A13.2 Information transfer** | | | |
| | A13.2.3 Electronic messaging | BR/BP | TBNL-POL-019 | Internal & External Communication Policy |
| | A13.2.4 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst moet van toepassing zijn op al het personeel dat toegang heeft tot gezondheidsinformatie | BR/BP | TBNL-POL-013 | Information Classification Policy |

| Clause | Control Objectives NEN 7510 | 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 |
| | A14.1.1.1 Zorgontvangers op unieke wijze identificeren;<br>Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten:<br>a) zekerstellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem;<br>b) in staat zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodgeval. | N/A | N/A | We do not provide health information systems |
| | A14.1.1.2 Validatie van ouputgegevens;<br>Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld. | N/A | N/A | We do not provide health information systems |

| | | | | |
|---|---|---|---|---|
| | A14.1.2 Securing application services on public networks | BR/BP | TBNL-POL-031 | Secure Development Policy |
| | A14.1.3 Protecting application services transactions | BR/BP | TBNL-POL-031 | Secure Development Policy |
| | A14.1.3.1 Openbaar beschikbare gezondheidsinformatie;<br>Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden gearchiveerd.<br>De integriteit van openbaar beschikbare gezondheidsinformatie moet worden beschermd om<br>onbevoegde wijzigingen te voorkomen.<br>De bron (auteurschap) van openbaar beschikbare<br>gezondheidsinformatie moet worden vermeld en de<br>integriteit ervan moet worden beschermd. | N/A | N/A | We do not provide health information systems |
| | **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 | TBNL-POL-023 | System Hardening Policy |
| | A14.2.6 Secure development environment | BR/RP | TBNL-POL-031 | Secure Development Policy |
| | A14.2.7 Outsourced development | BR/RP | TBNL-POL-031 | Secure Development Policy |
| | A14.2.8 System security testing | BR/RP | TBNL-POL-022 | Security Testing Policy |
| | A14.2.9 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten acceptatiecriteria vaststellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies. Voorafgaand aan acceptatie moeten ze geschikte testen van het systeem uitvoeren. | BR/RP | TBNL-POL-031 | Secure Development Policy<br>The measure specific to medical services is identical to the ISO 27001:2013 requirement |
| | **A14.3 Test data** | | | |

| | | | | |
|---|---|---|---|---|
| | A14.3.1 Protecting of test data | BR/BP | TBNL-POL-031 | Secure Development Policy |
| | | | | |
| **Clause** | **Control Objectives NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| **15 Supplier relationships** | **A15.1 Information security in supplier relations** | | | |
| | A15.1.1 Organisaties die gezondheidsinformatie verwerken moeten de risico's in verband met toegang door externe partijen tot deze systemen of gegevens die zij bevatten, beoordelen en vervolgens beveiligingsbeheersmaatregelen implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen. | BR/RP | TBNL-POL-002 | Supplier Policy |
| | A15.1.2 Addressing security within supplier agreements | BR/RP | TBNL-POL-002 | Supplier Policy |
| | A15.1.3 Information and communication technology supply chain | BR/RP | TBNL-POL-002 | Supplier Policy |
| | **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 | BR/RP | TBNL-POL-002 | Supplier Policy |
| | | | | |
| **Clause** | **Control Objectives NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| **16 Information security incident management** | **A16.1 Management of information security incidents and improvements** | | | |
| | A16.1.1 Responsibilities and procedures | BR/RP | TBNL-POL-021 | Information Security Incident Management Policy |
| | A16.1.2 Organisaties die persoonlijke gezondheids-informatie verwerken, moeten verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vaststellen:<br>a) om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen;<br>b) om te garanderen dat er een doeltreffend en geprioriteerd escalatiepad is voor incidenten zodat in de juiste omstandigheden en tijdig een beroep kan worden gedaan op plannen voor crisismanagement en bedrijfscontinuïteitsmanagement;<br>c) om incidentgerelateerde auditverslagen en ander | BR/BP/LR | TBNL-POL-021 | Information Security Incident Management Policy |

| | | | | |
|---|---|---|---|---|
| | relevant bewijs te verzamelen en in stand te houden. | | | |
| | 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 NEN 7510** | **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 | BR/BP/LR | TBNL-POL-030 | Management Systems Policy |
| | 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 NEN 7510** | **Reasons for selection** | **Policy ID** | **Corresponding Policy** |
| | **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 Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de geïnformeerde toestemming van cliënten beheren. Waar mogelijk moet geïnformeerde toestemming van cliënten worden verkregen voordat persoonlijke gezondheidsinformatie per e-mail, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling. | BR/BP/LR | TBNL-POL-013 | Information Classification Policy |
| | 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 Audit Policy |
| | A18.2.2 Compliance with security policies and standards | BR/BP/LR | TBNL-POL-003 | Internal Audit Policy |
| | A18.2.3 Technical compliance review | BR/BP/LR | TBNL-POL-003 | Internal Audit Policy |