5.2

[redacted]

Audit van de COVID19 organisatie op NEN 7510-1:2017 aspecten

GGD Zeeland

Versie rapport: V 1.1
Data audit: 17 & 18 maart 2021
Datum rapport: 7 april 2021
Audit en rapport: [redacted] CISSP, CIPP/e, Lead Auditor NEN 7510

Inhoudsopgave

Doel

Het beoordelen in hoeverre de COVID19 organisatie van de GGD Zeeland voldoet aan NEN 7510.

Scope

Binnen de scope van deze audit:
De toegang, gebruik en beheer van de applicaties CoronIT, HPZone en HPZone Lite t.b.v. de teststraten, vaccinatiestraat en het bron- en contactonderzoek. Hieronder valt ook de fysieke beveiliging van kantoorlocatie, testlocatie en vaccinatiestaat.

Buiten scope van deze audit:

- Het ontwerp, ontwikkelen en testen van de applicaties CoronIT, HPZone en HPZone Lite
- Beheer van de platformen waarop de applicaties CoronIT, HPZone en HPZone Lite zijn geïnstalleerd
- Het inrichten en beheer van de verbinding met de applicaties CoronIT, HPZone en HPZone Lite

Als normenkader wordt NEN 7510-1:2017 gebruikt. Daarnaast wordt op onderdelen gebruik gemaakt van het Auditkader Gedragslijn Toegangsbeveiliging digitale patiëntdossiers van de NVZ.

Bij het selecteren van de te toetsen NEN 7510 onderdelen, is als uitgangspunt gehanteerd dat er een dwarsdoorsnede moet zijn van:

- Procesmatige, organisatorische en technische maatregelen
- Preventieve, detecterende en repressieve maatregelen

Daarnaast is in de introductie meeting tussen opdrachtgever en opdrachtnemer (februari 2021) een aantal aandachtsgebieden ter sprake gekomen die verder/diepgaander onderzoek vergden.

Gezien het risicoprofiel van de COVID19 GGD Zeeland organisatie, de genoemde uitgangspunten en de tijdens de introductie meeting besproken onderwerpen, heeft de auditor in overleg met de GGD Zeeland besloten de volgende NEN 7510 onderdelen te toetsen:

- Awareness *)
- Screening
- Autorisatiebeheer en systemen voor wachtwoordbeheer *)
- Logging en Monitoring *)
- Fysieke toegang, inclusief “clear desk en clear screen”, bij bron- en contactonderzoek op test- en vaccinatielocaties
- Leveranciersmanagement, inclusief verwerkersovereenkomsten
- Beheer van mobile devices (laptops/tablets etc.)

- Tevens is ingegaan op de Governance rondom informatiebeveiliging en dan met name de mate waarin GGD Zeeland aansluit bij/afstemt met de vanuit de GGD GHOR NL gecoördineerde maatregelen t.b.v. HPZone, HPZone Lite en CoronIT

*) Op deze onderdelen is naast de NEN 7510 norm, Auditkader Gedragslijn Toegangsbeveiliging digitale patiëntdossiers van de NVZ gebruikt als leidraad.

NEN 7510 onderdelen die niet zijn getoetst:

- H 4 – H8, H10 (contextanalyse, risicoanalyse, uitvoeren risicobehandelplan, directiebeoordeling)
- A.5 – IB Beleid
- A.8.1 – Classificatie van informatie
- A.10.1.2 – Sleutelbeheer van cryptografische sleutels
- A.12, m.u.v. (wel behandeld) logging en monitoring, patching, backup/restore, beheer van technische kwetsbaarheden
- A.13.1 – Netwerkbeveiliging
- A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen (er wordt geen software ontwikkeld binnen de GGDZ)
- A.16 – Incident management (wel besproken: leren van incidenten door het bespreken van casuïstiek)
- A.17 - Continutity

Aanpak

Aan de hand van de norm NEN 7510 is beoordeeld of de organisatie aantoonbaar risico's in het kader van informatiebeveiliging (IB) identificeert en beheert op de in de scope genoemde onderdelen. Waarnemingen zijn gedaan en conclusies zijn getrokken op basis van interviews en observatie en zijn derhalve een steekproef die niet noodzakelijkerwijs een volledig beeld geeft.

Disclaimer

Deze interne audit is uitgevoerd met NEN 7510 als uitgangspunt. Het betrof geen certificeringsaudit, maar een audit op de meest risicovolle processen die binnen het COVID19 team worden uitgevoerd. De scope van deze audit was daarom beperkter ten opzichte van een NEN 7510 certificeringsaudit. Het aantal besteedde dagen is lager dan bij een reguliere NEN 7510 audit. Daarbij moet opgemerkt worden dat bij het bepalen van het aantal benodigde auditdagen, ook rekening is gehouden met het significante aantal medewerkers dat dezelfde taken uitvoert (bv afnemen van testen, uitvoeren BCO, vaccineren).

De uitkomsten in dit rapport zijn gebaseerd op deelwaarnemingen en steekproeven. Een andere audit kan tot andere resultaten en conclusies leiden.

Samenvatting

De Covid19 organisatie is recent ontstaan vanuit een crisis. [redacted] De algemene indruk is dat de organisatie bewust is van de risico's omtrent dataprivacy en daar ook naar handelt.

[redacted]

[redacted]

Tijdens de audit zijn gespreksverslagen gemaakt. Zie hiervoor Bijlage - gespreksverslagen

Conclusie

[redacted] Tijdens de audit heeft de GGDZ op de onderdelen awareness, screening, logische toegangsbeveiliging en device management aangetoond “in control te zijn”.

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Bijlage – Gespreksverslagen

Gespreksverslagen Auditverslag GGD Zeeland

Dag 1. Woensdag 17 maart

Locatie:
GGD Zeeland, team COVID-19
Stationspark 29
4462 DZ Goes

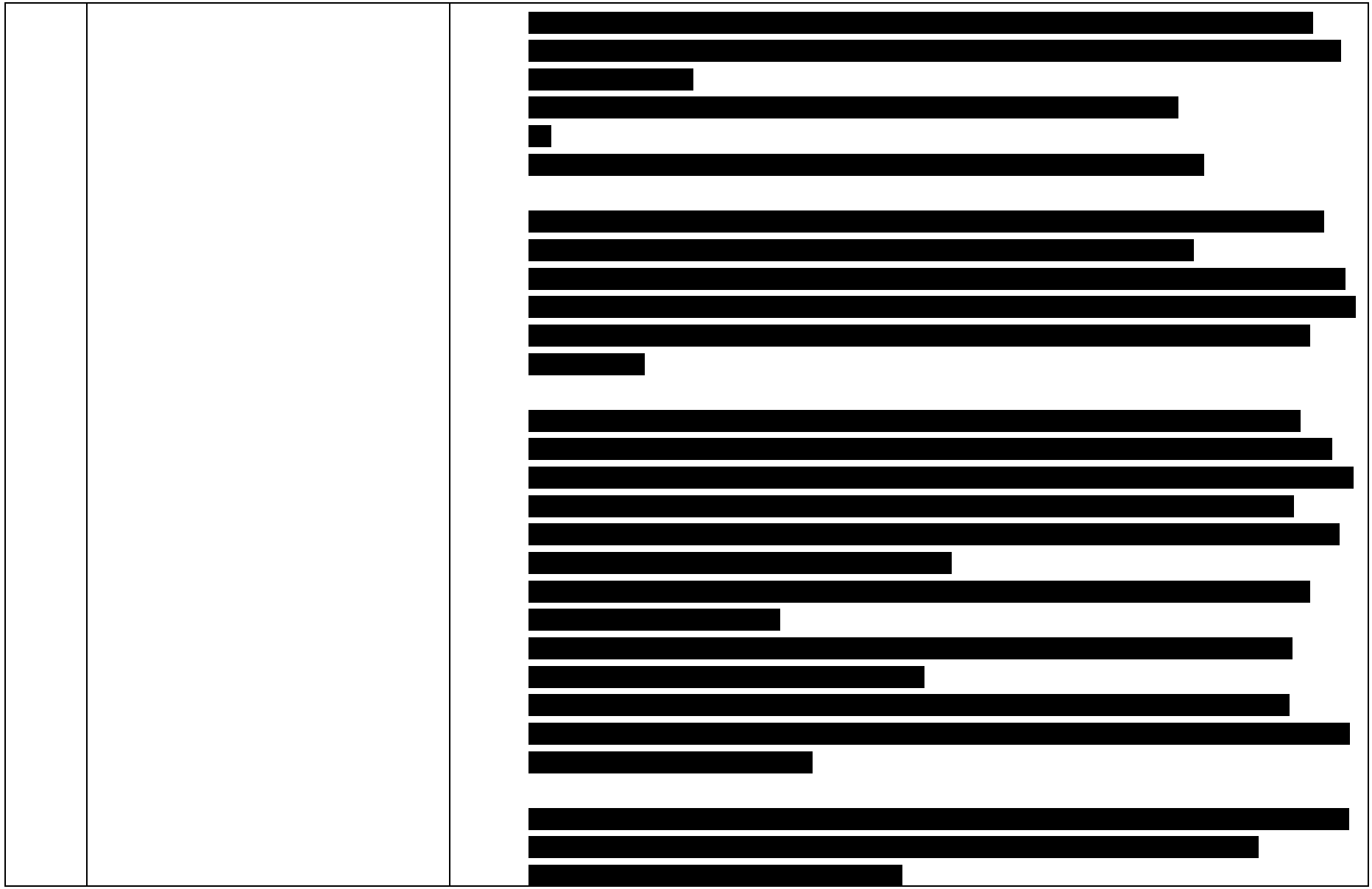
Dag 1: Stationspark, Goes

Geschat tijdstip	Onderdeel	notes
9.00 – 10.00	Awareness, instructies/ training Voor dit onderdeel wordt de **gedragslijn** toegang patiëntdossiers gebruikt, onderdeel "Bewustwording medewerkers	[redacted]

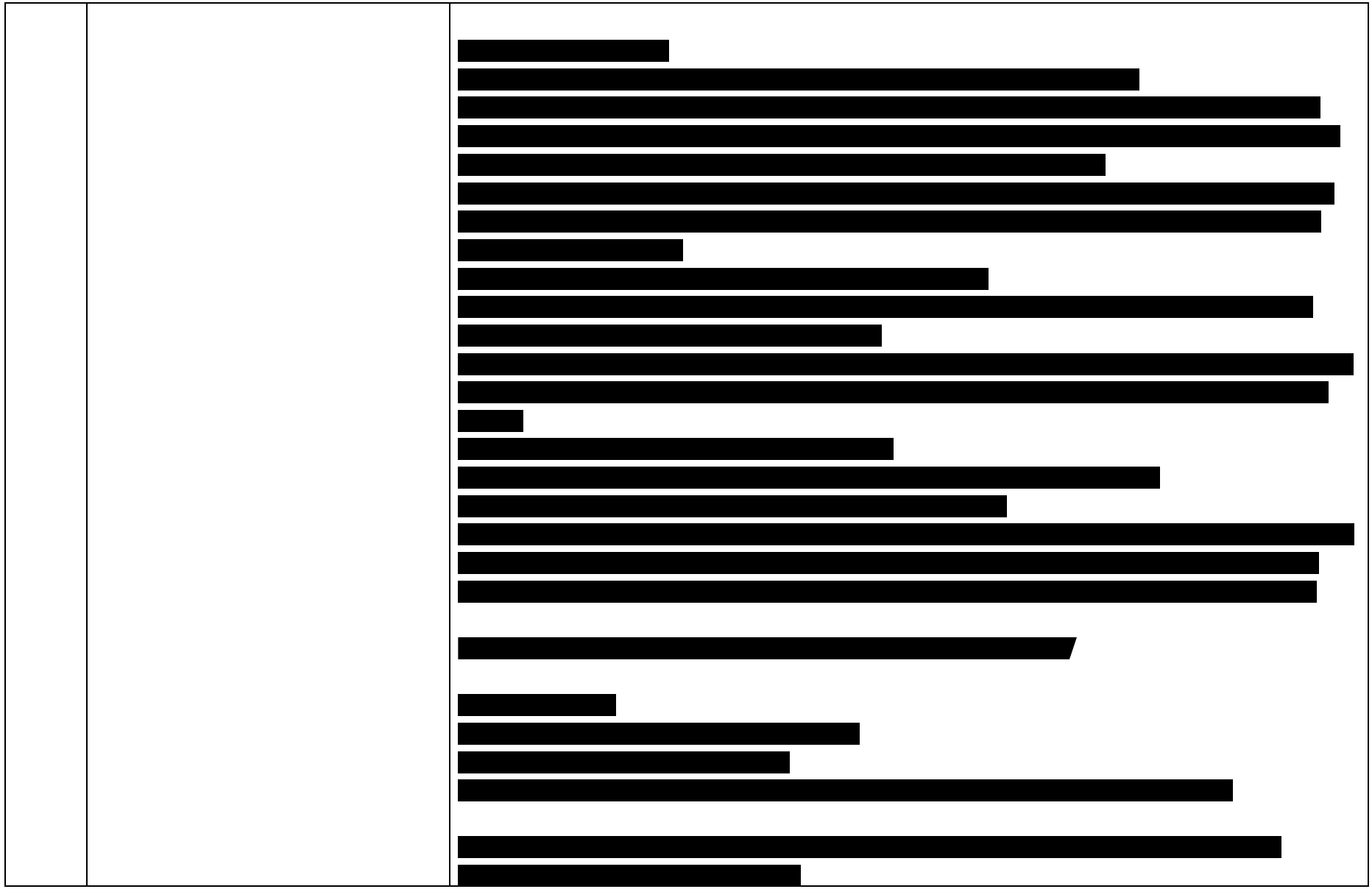
Geschat tijdstip	Onderdeel	notes
		[redacted]

Geschat tijdstip	Onderdeel	notes
		[redacted]

10.00-13.00	Autorisatiesbeheer en systemen voor wachtwoordbeheer. Voor dit onderdeel wordt de **gedragslijn** toegang patiëntdossiers gebruikt, onderdelen Autorisaties en Authenticatie	[redacted]



		[redacted]
13:30 – 14:30	Onboarden van medewerkers (screening, uitreiken devices/ toegangscodes) Voor het beheer van mobile devices is op dag 2 ook tijd gereserveerd	[redacted]



		[redacted]
14:30 – 15:30	Fysieke toegang kantoor inclusief “clear desk en clear screen” (hoofdlocatie GGD Zeeland, team COVID-19 Stationspark 29 4462 DZ Goes	[redacted]

		[redacted]
15:30 – 17:30	Logging en monitoring, op basis van de gedragslijn toegang patiëntdossiers Voor dit onderdeel wordt de **gedragslijn** toegang patiëntdossiers gebruikt, onderdelen Logging en controle van logging	[redacted]

		[redacted]

		[redacted]

Dag 2, Donderdag 18 maart

Geschat tijdstip	Onderdeel	notes
8:30 – 10:30	Fysieke toegang inclusief “clear desk en clear screen” Teststraat Vlissingen **Testlocatie Vlissingen** **Sottegemstraat 56** **4382 EP Vlissingen**	[redacted]

Geschat tijdstip	Onderdeel	notes
		[redacted]
11:00 – 13:00	Fysieke toegang inclusief “clear desk en clear screen” • Teststraat 2 – Zeelandhallen • Vaccinatiestraat 1 – Zeelandhallen **Testlocatie/vaccinatielocatie Goes** **Da Vinciplein 1** **4462 GX Goes**	[redacted]

Geschat tijdstip	Onderdeel	notes
		V[redacted]

Geschat tijdstip	Onderdeel	notes
		[redacted]
1300 – 1330	Reistijd naar **GGD Zeeland, team COVID-19** **Stationspark 29** **4462 DZ Goes**	
13:30 – 15.00	Governance, GHOR NL projecten en leveranciersmanagement, inclusief verwerkersovereenkomsten	[redacted]

Geschat tijdstip	Onderdeel	notes
		[redacted]

Geschat tijdstip	Onderdeel	notes
		[redacted]
15:00 – 16:00	Beheer van mobile devices	[redacted]

Geschat tijdstip	Onderdeel	notes
		[redacted]

Geschat tijdstip	Onderdeel	notes
16:00 – 17:00	Steekproef op gebruik downloadknop HPZone 10 medewerkers/ beoordelen review *)	[redacted]

Geschat tijdstip	Onderdeel	notes
		[redacted]