

TOEGEPASTE INFORMATICA: BEVEILIGING VAN DATA EN INFORMATIE

- 1 Tijdens je stage ga je in gesprek met de DPO of veiligheidsverantwoordelijke van het bedrijf. Samen probeer je een antwoord te vinden op onderstaande vragen. Werk deze opdracht volledig uit tijdens je stageweek. Laat je oplossing nalezen door de DPO of veiligheidsverantwoordelijke. Vraag dat hij elk blad parafeert of tekent.

LEERPLANDOELSTELLINGEN	
LPD 46	De belangrijkste richtlijnen ter bescherming van persoonsgegevens toelichten en toepassen op concrete voorbeelden.
LPD 47	De belangrijkste risico's en gevaren binnen een informatiesysteem toelichten onder meer malware, hacking, inbreuk tegen bedrijfsregels, cloudtoepassingen, doorgeven van gegevens binnen een website.
LPD 48	Een informatieveiligheidsplan voor een concrete situatie opstellen.

2 Persoonsgegevens

- Welke personeelsgegevens worden in de firma verwerkt?
- Verklaar welke gegevens onder de GDPR-richtlijnen vallen? Waarom, waarom niet?
- Hoe komt de firma aan deze gegevens?
- Hoe werd de toestemming gegeven? En is deze conform met de GDPR-wetgeving? Motiveer je antwoord.
- Met wie worden ze gedeeld en waarom?
- Hoelang, nadat het personeelslid het bedrijf heeft verlaten, worden deze persoonsgegevens bewaard? Is dit in orde met de GDPR? Motiveer je antwoord.
- Worden er nog andere persoonsgegevens verwerkt in het bedrijf? Zo ja, welke en waarom?

3 Beveiliging van data

PDCA

In een bedrijf moet er regelmatig nieuwe software geïnstalleerd worden. Hierbij moet uiteraard rekening gehouden worden met de gevolgen van introductie van een nieuwe softwareversie in het bedrijf. Hoe pakt het bedrijf dit aan? **Stel een PDCA cyclus op.**

4 Veiligheidsactieplan voor het bedrijf

Vraag het veiligheidsactieplan van het bedrijf op. Voeg een kopie toe aan je oplossing. Misschien vind je hierin reeds antwoorden voor fiche 3: ruimten en apparatuur uit het **Toetsingskader Informatiebeveiliging.**

Fysieke beveiliging en beveiliging van de omgeving

Fiche 3: ruimten en apparatuur (.../0,5 per onderdeel per ficheonderdeel)

Beoordeel de onderdelen 3.1 tot en met 3.15. Dit doe je door het maturiteitsniveau te bepalen op basis van:

- Beoordelingen van personen binnen de firma, eigen bevindingen
- Welke documenten zijn aanwezig in de firma? (Geef een korte omschrijving. Indien de firma dit toelaat, voeg een kopie van dit document toe.)
- Eigen waarnemingen ter plaatse
- Formuleer 1 extra aanbeveling

Verbetersleutel

Persoonsgegevens (.../16)		
Welke personeelsgegevens worden allemaal in de firma verwerkt? Opsomming gegevens	/2	E-mail, Telefoon, naam, adres, persoonlijke gegevens, zoals financiële data, ...
Verklaar welke gegevens onder de GDPR-richtlijnen vallen? Waarom, waarom niet? Verklaring.	/4	Alle persoonsgegevens van personeel vallen onder de richtlijnen van de GDPR, waarom? Omdat het personeelsgegevens zijn.
Waar komen deze gegevens vandaan? Omschrijving	/2	Via verschillende bronnen, meestal van het personeelslid zelf.
Hoe werd de toestemming gegeven? En is deze conform met de GDPR-wetgeving? Omschrijving	/2	De verwerkingen gebeuren niet op basis van toestemming maar op basis van noodzakelijkheid voor de uitvoering van het arbeidscontract of gerechtvaardigd belang.
Met wie worden ze gedeeld en waarom? Omschrijving (.../1) Wie (.../1) Waarom (.../1)	/3	Ze worden met de verwerker gedeeld, bv. Als hun een getuigt moet worden, verzekeringen.
Hoelang, nadat het personeelslid het bedrijf heeft verlaten, worden deze persoonsgegevens bewaard? Is dit in orde met de GDPR?	/1	5 jaar na de arbeidsovereenkomst. Dit is in orde met de GDPR.
Worden er nog andere persoonsgegevens verwerkt in het bedrijf? Zo ja, welke en waarom? Opsomming gegevens (.../1) Waarom (.../1)	/2	Ja, persoonsgegevens van klanten, leveranciers. welke? klantnummer, taal, adres, naam, telefoon. waarom: zodat ze aan de hand van deze gegevens hun werk kunnen doen.

Beveiliging van data (.../4)		
Stel een PDCA-cyclus op ivm het introduceren van nieuwe software. PDCA	/4	Zie onderaan het blad.
Veiligheidsactieplan voor het bedrijf (.../30)		
Fiche 3: ruimten en apparatuur Welk maatregelen zijn reeds van toepassing in de firma?	/30 (0,5 per punt per onderdeel)	

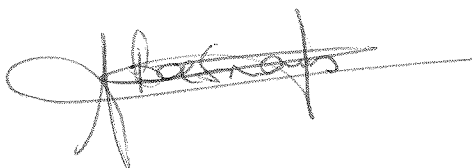
PDCA cyclus:

plan: Er wordt gepland wanneer er nieuwe software zal worden geïntegreerd.

DO: Er wordt de software met een pilot group getest (de IT afdeling)

check: De software wordt door een paar weken getest. Om zo fouten te ontdekken en op te lossen.

Act: Als alles goed verlopen is en alle fouten zijn uit de software kan de software geïntegreerd worden op elke computer.



3. Ruimten en apparatuur

Nr.	ISO27002	Statement
3.1	6.2.1.2	Beleid voor mobiele apparatuur: Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.
3.2	8.3.2	Verwijderen van media: Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
3.3	11.1.1	Fysieke beveiligingszone: Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
3.4	11.1.2	Fysieke toegangsbeveiliging: Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen: Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.
3.6	11.1.4	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
3.7	11.1.5	Werken in beveiligde gebieden: Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
3.8	11.1.6	Laad- en loslocatie: Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.
3.9	11.2.1	Plaatsing en bescherming van apparatuur: Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.
3.10	11.2.2	Nutsvoorzieningen: Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door onregeligheden in nutsvoorzieningen.
3.11	11.2.3	Beveiliging van bekabeling: Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.
3.12	11.2.4	Onderhoud van apparatuur: Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
3.13	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein: Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur: Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
3.15	12.4.4	Kloksynchronisatie: De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.

3.1 Beleid voor mobiele apparatuur 6.2.1.2

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 6.2.1.2
MBO controledoelstelling: Beleid voor mobiele apparatuur		
Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.		
Toelichting:		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Verantwoordelijkheid en verantwoording zijn niet gedefinieerd. Medewerkers nemen op eigen initiatief en op reactieve wijze verantwoordelijkheid voor kwesties.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Men neemt verantwoordelijkheid en wordt ter verantwoording geroepen, zelfs als dit niet formeel is geregeld. Bij problemen is echter vaak onduidelijk wie er verantwoordelijk is, en men is geneigd de schuld door te schuiven.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Er is een formele verantwoordelijkheid- en verantwoordingsstructuur en het is duidelijk wie waar verantwoordelijk voor is. Die persoon heeft echter vaak niet de volledige bevoegdheid om zijn verantwoordelijkheden volledig te kunnen uitoefenen. Evidence: 1. Kopie van organogram met opgenomen de verantwoordelijkheden en rapportagestructuur; 2. Formele functiebeschrijvingen.	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Er is een aanvaarde structuur voor verantwoordelijkheid en verantwoording en de betreffende personen kunnen zich van hun verantwoordelijkheden kwijten. Positieve actie wordt stelselmatig beloond om de betrokkenen te motiveren. Evidence in aanvulling op 3: 1. Kopie van een geaccordeerde mandatenregeling waaruit de bevoegdheden van de beveiligingsfunctionarissen blijkt.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De verantwoordelijken hebben de vrijheid om, binnen hun mandaat, besluiten en maatregelen te nemen. De verantwoordelijkheidsstructuur is tot op het laagste niveau ingebed in de organisatie. Evidence in aanvulling op 4: 1. Kopie van werkinstructies of processchema's waaruit blijkt dat op alle niveaus beveiligingstaken kunnen worden uitgevoerd en hoe eventuele escalaties/opschaling zijn ingeregeld.	
Beoordeling (aanwezig, datum en locatie):		
Bevindingen:		
<ul style="list-style-type: none"> • Documenten: • Interviews: • Waarneming ter plaatse: 		
Aanbevelingen:		

3.2 Verwijderen van media 8.3.2

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 8.3.2
MBO controledoelstelling: Verwijderen van media Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.		
Toelichting: Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures. (9.2.6 gaat over opslag voorzieningen in een apparaat bv. harde schijf. 10.7.2 is gericht op mobiele/verwijderbare media, zoals USB sticks, geheugenkaarten, externe harddisks, disks, cards, tapes.)		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Naar eigen inzicht, op individueel niveau.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Werkafspraken, op operationeel niveau binnen bepaalde groepen (bottom-up).	
Volwassenheidsniveau 3 (gedefinieerd proces)	Aantoonbaar gebruik van good practices. Beleid, proces / procedurebeschrijvingen zijn aanwezig en vindbaar, communicatie hierover heeft plaatsgevonden. Evidence: <ol style="list-style-type: none"> Kopie procedurebeschrijving voor verwijderen van media; Kopie van informatie waaruit blijkt dat de organisatie conform het procedurebeschrijving heeft uitgevoerd. Te denken aan: <ul style="list-style-type: none"> kopie contractovereenkomst met een goedgekeurde verwijderbedrijf; kopie checklist bij het verwijderen van media; kopie van een registerlijst met alle verwijderde media's. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: <ol style="list-style-type: none"> Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	✓
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: <ol style="list-style-type: none"> Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	
Beoordeling (aanwezig, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: <i>Data op schijven worden verwijderd.</i> Waarneming ter plaatse: 		
Aanbevelingen:		

3.3 Fysieke beveiligingszone 11.1.1


Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.1
MBO controledoelstelling: Fysieke beveiligingszone Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.		
Toelichting: Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden. (Denk daarbij aan serverruimte, backup-ruimte, (MER) OTAP-straat en patchruimtes (SER). Denk ook aan kasten met persoonsdossiers, afgedrukte tentamenvragen enz.)		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Toegangsbeveiliging wordt naar bevind van zaken aangebracht door individuele medewerkers.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Er zijn praktijkafspraken gemaakt over toegangsbeveiligingsmaatregelen, op operationeel niveau.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Er is beleid en/of PvA voor het gebruik en de standaardisatie van toegangsbeveiligingsmaatregelen. Instrumenten worden gebruikt voor hun fundamentele doeleinden, wellicht niet helemaal in overeenstemming met beleid, architectuur en/of geïntegreerd. Evidence: <ol style="list-style-type: none"> Kopie overzicht van ruimten met specifieke toegangsbeveiliging, waarbij is aangetoond dat er toegangsbeveiligingen zijn; Waarneming ter plaatse. 	x
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. Evidence in aanvulling op 3: <ol style="list-style-type: none"> Verslagen van controles op de effectiviteit van de toegangsbeveiliging. 	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. Evidence in aanvulling op 4: <ol style="list-style-type: none"> Periodieke (jaarlijks/twee jaarlijks) evaluaties van de effectiviteit van de toegangsbeveiliging; Eventueel verbeterplannen. 	
Beoordeling (aanwezigen, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: vPN is aanwezig + op GSM extra code. Interviews: Dodegen en sommige plaatsen zijn on-veilig. Waarneming ter plaatse: Er zijn dodegen nodig om binnen te komen. 		
Aanbevelingen:		

3.4 Fysieke toegangsbeveiliging 11.1.2

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.1
MBO controledoelstelling: Fysieke toegangsbeveiliging		
Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.		
Toelichting: Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten. (Het gaat hier eigenlijk om een classificatie van fysieke ruimte. Er wordt een indeling in zones voorgesteld, van openbaar (publiek toegankelijk), voor studenten, voor afdelingen/medewerkers (kantoorruimte), voor medewerkers t.b.v. werkzaamheden met speciale bevoegdheden (ruimte met kluis, infrastructuur, gevaarlijke stoffen).)		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Er is geen algemene regeling. Per zone zijn maatregelen genomen op individueel initiatief, maar niet noodzakelijk afgestemd op het belang van die zone of ruimte voor de organisatie/afdeling als geheel.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Zones en ruimtes zijn beschermd ongeveer in overeenstemming met hun belang voor de organisatie. De maatregelen sets per zone zijn niet op elkaar afgestemd, maar per afdeling zijn praktijkafspraken gemaakt.	✗
Volwassenheidsniveau 3 (gedefinieerd proces)	Op basis van good practices is de toegangsbeveiliging tot de beveiligde zones op grote lijnen uniform ingericht, gekoppeld aan het belang van die zone voor de organisatie. Er is een 'masterplan' toegangsbeveiliging of vergelijkbaar document, er is een Plan van Aanpak, en er zijn procesbeschrijvingen/procedures gepubliceerd en/of gecommuniceerd. Evidence: 1. Kopie beschrijving waarin is beschreven de inrichting van toegangsbeveiliging tot de beveiligde zones; 2. Kopie van informatie waaruit blijkt dat het beleid/procedure geüpdate wordt aan het actuele belang. Te denken aan; • twee meeste recente rapportages of analyses (datum en versienummer).	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. Evidence in aanvulling op 3: 1. Verslagen van audits op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. Evidence in aanvulling op 4: 1. Evaluaties van proces rond de beveiligingsmaatregelen.	

Beoordeling (aanwezig, datum en locatie):
Bevindingen: <ul style="list-style-type: none">• Documenten:• Interviews: ruimte zijn afgeboekt. badgen zijn verplicht.• Waarneming ter plaatse:
Aanbevelingen:

3.5 Kantoren, ruimten en faciliteiten beveiligen 11.1.3

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.1.3
MBO controledoelstelling: Kantoren, ruimten en faciliteiten beveiligen Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.		
Toelichting: Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Er zijn afsluitbare ruimtes. Sleutelbeheer op afdelingsniveau.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Er zijn praktijkafspraken over de verantwoordelijkheid van fysieke beveiliging van ruimtes en voorzieningen met bedrijf kritische gegevens, apparatuur, infrastructurele of facilitaire voorzieningen. Verantwoordelijkheden en bevoegdheden zijn niet eenduidig vastgelegd.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Good practices worden toegepast. Beleid, proces en procedures zijn gedefinieerd en gedocumenteerd, bevoegdheden en verantwoordelijkheden zijn vastgelegd. Evidence: <ol style="list-style-type: none"> Kopie overzicht van ruimten met specifieke toegangsbeveiliging; Kopie van adresboeken en interne telefoongidsen van de organisatie waarin locaties worden aangeduid met gevoelige IT voorzieningen, behoren niet vrij toegankelijk te zijn voor bezoekers; Waarneming ter plaatse. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. Evidence in aanvulling op 3: <ol style="list-style-type: none"> Verslagen van tests op de effectiviteit van de maatregelen. 	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. Evidence in aanvulling op 4: <ol style="list-style-type: none"> Evaluaties van het proces rond de fysieke beveiliging. 	
Beoordeling (aanwezig, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: <i>badger zijn verplicht om de kamers binnen te gaan</i> Waarneming ter plaatse: <i>waarneming</i> 		
Aanbevelingen:		

3.6 Beschermen tegen bedreigingen van buitenaf 11.1.4

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.1.4
MBO controledoelstelling: Beschermen tegen bedreigingen van buitenaf		
Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.		
Toelichting:		
Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Fysieke beveiligingsmaatregelen zijn bottom-up door gebouwenbeheer of facilitaire dienst getroffen, en op basis van externe eisen (brandweer, verzekering).	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Fysieke beveiligingsmaatregelen worden periodiek geïnspecteerd, bijvoorbeeld op initiatief van brandweer en verzekering (reactief).	✓
Volwassenheidsniveau 3 (gedefinieerd proces)	<p>Good practices worden toegepast. Beleid, proces en procedures zijn vastgelegd. O.a. fysieke beveiligingsmaatregelen worden periodiek geïnspecteerd op initiatief van centraal verantwoordelijke stafafdeling. Er is een plan van aanpak tbv implementatie aanbevelingen, management notulen waaruit blijkt dat risico's zijn geaccepteerd en/of maatregelen worden aangepast.</p> <p>Evidence:</p> <ol style="list-style-type: none"> Kopie beleid, procedurebeschrijving waarin beheersingsmaatregelen de fysieke bescherming tegen schade door brand, overstroming, aardbevingen, explosies, oproer en andere vorm van natuurlijke of menselijke calamiteiten zijn beschreven; Kopie van informatie waaruit blijkt dat beheersmaatregelen zijn geïmplementeerd om het risico van mogelijke gevaren te minimaliseren, bijvoorbeeld <ul style="list-style-type: none"> overzicht waar alle brandmelders en brandblusser staan; waarneming ter plaatse kopie plan van aanpak voor het oplossen tijdens menselijk calamiteiten kopie testrapporten van beveiligingsmiddelen. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	<p>Evidence in aanvulling op 3:</p> <ol style="list-style-type: none"> Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	
Volwassenheidsniveau 5 (Geoptimaliseerd)	<p>Evidence in aanvulling op 4:</p> <ol style="list-style-type: none"> Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	

Beoordeling (aanwezig, datum en locatie):
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: Er worden back ups gemaakt. Waarneming ter plaatse: Cloud is op andere site.
Aanbevelingen:

3.7 Werken in beveiligde gebieden 11.1.5

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.1.5
MBO controledoelstelling: Werken in beveiligde gebieden		
Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.		
Toelichting: Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Processen en werkwijzen worden op ad-hoc basis benaderd. Er is geen sprake van een vastomlijnd proces of beleid.	X
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Er zijn praktijkafspraken gemaakt. Medewerkers werken op basis van individuele instructies.	
Volwassenheidsniveau 3 (gedefinieerd proces)	<p>Good practices worden toegepast. Er is beleid, proces en procedures zijn vastgelegd. Voor belangrijke ruimtes zijn procedures en werkinstructies vastgesteld en gecommuniceerd.</p> <p>Evidence:</p> <ol style="list-style-type: none"> 1. Kopie procedure/ werkinstructies/ richtlijnen voor werken in beveiligde ruimtes; 2. Kopie van informatie waaruit blijkt dat de procedure, werkinstructies of richtlijnen is gecommuniceerd met de medewerkers. Te denken aan; <ul style="list-style-type: none"> • kopie intranet waarin is beschreven de "op te vragen informatie" m.b.t. fysieke maatregelen voor belangrijke ruimtes; 3. Kopie van informatie waaruit blijkt dat voor alle belangrijke ruimtes fysieke maatregelen zijn getroffen; 4. Waarneming ter plaatse. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	<p>Evidence in aanvulling op 3:</p> <ol style="list-style-type: none"> 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	
Volwassenheidsniveau 5 (Geoptimaliseerd)	<p>Evidence in aanvulling op 4:</p> <ol style="list-style-type: none"> 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	
Beoordeling (aanwezigen, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> • Documenten: • Interviews: <i>Niet echt aanwezig, enkel de badgen.</i> • Waarneming ter plaatse: 		
Aanbevelingen:		

3.8 Laad- en loslocatie 11.1.6

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.1.6
MBO controledoelstelling: Laad- en loslocatie Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.		
Toelichting: De toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, worden beheerst en indien mogelijk afgeschermd van IT-voorzieningen, om onbevoegde toegang te voorkomen. (Onderwijsinstellingen zijn per definitie publiek toegankelijk. Beveiliging van laad/lospunten zijn vooral gericht op het voorkomen van diefstal van geleverde of af te voeren goederen.)		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Ontvangst bij Laad en losruimtes wordt geïmproviseerd. toezicht is afhankelijk van situatie en individuele inschatting.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Toezicht en bewaking van laad- en losruimtes is in de praktijk belegd. Er is geen formeel beleid, wel praktijkafspraken op operationeel niveau.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Good practices worden toegepast. Beleid, proces en procedures zijn vastgelegd. O.a. het proces toezicht en bewaking van laad- en losruimtes is belegd. Er is een vastgesteld protocol voor goederenontvangst. Evidence: <ol style="list-style-type: none"> Kopie procedurebeschrijving voor openbare toegang en gebieden voor laden en lossen; Kopie van informatie waaruit blijkt dat de organisatie conform de procedurebeschrijving werken, te denken aan: <ul style="list-style-type: none"> kopie van een registratieboek; kopie overzicht waar fysieke beveiligingstools (bijv. camera's) zijn geplaatst bij openbare toegang en gebieden voor laden en lossen; Waarneming ter plaatse. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: <ol style="list-style-type: none"> Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	✓
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: <ol style="list-style-type: none"> Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	
Beoordeling (aanwezig, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: De computers staan afgeschermt / 2 sleutels nodig voor kleine machines te roken. Waarneming ter plaatse: goede beveiliging. 		

Aanbevelingen:

3.9 Plaatsing en bescherming van apparatuur 11.2.1


Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.2.1
MBO controledoelstelling: Plaatsing en bescherming van apparatuur Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.		
Toelichting: Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Plaatsing en beschermingsmaatregelen van bedrijf kritische apparatuur wordt bottom-up en op basis van individuele beoordeling uitgevoerd.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Plaatsing en beschermingsmaatregelen van bedrijf kritische apparatuur gebeurt op basis van praktijkafspraken op operationeel niveau.	>
Volwassenheidsniveau 3 (gedefinieerd proces)	Er is beleid en/of een PVA opgesteld waarin het proces en de instrumenten voor plaatsing van bedrijf kritische apparatuur zoveel mogelijk te standaardiseren en te automatiseren. Instrumenten worden gebruikt voor fundamentele doeleinden, mogelijk niet volledig in lijn met architectuur en mogelijk niet volledig geïntegreerd. Evidence: <ol style="list-style-type: none"> Kopie plan van aanpak waarin de beheersingsmaatregelen om het risico van mogelijk gevaren te minimaliseren; Kopie van informatie waaruit blijkt dat bedrijf kritische apparatuur is geplaatst en beschermd tegen schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang. Te denken aan: <ul style="list-style-type: none"> kopie overzicht van ruimten met specifieke toegangsbeveiliging; Waarneming ter plaatse. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: <ol style="list-style-type: none"> Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: <ol style="list-style-type: none"> Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	
Beoordeling (aanwezigen, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: server lokaal is afgesloten. 		

- | |
|---|
| <ul style="list-style-type: none">• Waarneming ter plaatse: oude toestellen worden vernietigd <p>Aanbevelingen:</p> |
|---|

3.10 Nutsvoorzieningen 11.2.2

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.2.2
MBO controledoelstelling: Nutsvoorzieningen Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.		
Toelichting: Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Op basis van best effort, bottom-up zijn een aantal tools geïnstalleerd, bijvoorbeeld een UPS in een patchkast.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Beschermingsmaatregelen zijn op operationeel niveau geïmplementeerd. Tools zijn gedocumenteerd, praktijkafspraken zijn gemaakt.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Apparatuur is technisch/geautomatiseerd beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen op basis van beleid en/of plan van aanpak. De gebruikte tooling is wellicht niet geheel in lijn met architectuur, beleid of PvA, en wellicht niet geheel geïntegreerd. Evidence: <ol style="list-style-type: none"> Kopie beleid of plan van aanpak waarin is beschreven hoe de apparatuur is beschermd tegen stroomuitval en andere storingen door onderbrekingen van nutsvoorzieningen; Kopie van informatie waaruit blijkt dat de apparatuur is beschermd tegen stroomuitval en andere storingen. Te denken aan: <ul style="list-style-type: none"> kopie onderhoudscontract voor inspectie nutsvoorzieningen; kopie testrapporten m.b.t. nutsvoorzieningen; kopie nutsvoorzieningen vs. verbruik van de systemen; Waarneming ter plaatse. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: <ol style="list-style-type: none"> Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	✓
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: <ol style="list-style-type: none"> Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	
Beoordeling (aanwezigen, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: ups, back up Waarneming ter plaatse: Netwerk werk niet. 		
Aanbevelingen:		

3.11 Beveiliging van bekabeling 11.2.3

Cluster: Beleid en organisatie		ISO 27002 nummer: 11.2.3
MBO controledoelstelling: Beveiliging van bekabeling Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.		
Toelichting: Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd,		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Er zijn bottom-up enige beschermingsmaatregelen getroffen.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Er zijn op operationeel niveau werkafspraken omtrent gebruik en beschermingsmaatregelen voor bekabeling.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Er is gedocumenteerd welke typen/standaarden voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, en hoe deze tegen interceptie of beschadiging worden beschermd. Standaardgebruik, maar wellicht niet volledig conform architectuur en integratie policy. Evidence: <ol style="list-style-type: none"> Kopie beleid of plan van aanpak waarin de beheersingsmaatregelen zijn beschreven voor beveiligen van voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt tegen interceptie of beschadiging; Kopie van informatie waaruit blijkt dat de organisatie conform het beleid of plan van aanpak hebben uitgevoerd. Te denken aan: <ul style="list-style-type: none"> kopie testrapporten m.b.t. voedings- en telecommunicatiekabels; Waarneming ter plaatse. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: <ol style="list-style-type: none"> Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: <ol style="list-style-type: none"> Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	
Beoordeling (aanwezigen, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: server lokaal is goed beschermt. 		

- | | |
|---|--------------------------------|
| <ul style="list-style-type: none">• Waarneming ter plaatse: | Amper bescherming in de kamers |
| Aanbevelingen: | |

3.12 Onderhoud van apparatuur 11.2.4

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.2.4
MBO controledoelstelling: Onderhoud van apparatuur Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.		
Toelichting: Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Verantwoordelijkheid en verantwoording zijn niet gedefinieerd. Medewerkers nemen op eigen initiatief en op reactieve wijze verantwoordelijkheid voor kwesties. Het is onduidelijk welke onderhoudscontracten van toepassing zijn.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Men neemt verantwoordelijkheid en wordt ter verantwoording geroepen, ook als dit niet formeel is geregeld. Bij problemen is onduidelijk wie er verantwoordelijk is. Er is sprake van standaard onderhoudscontracten.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Er is een formele verantwoordelijkheid- en verantwoordingsstructuur (RASCI) en het is duidelijk wie waar verantwoordelijk voor is. Onderhoudscontracten zijn specifiek toegespitst op het belang van de apparatuur voor de organisatie. Evidence: 1. Kopie beleid voor classificatie, waarborgen en onderhouden van apparatuur; 2. Kopie van formele verantwoordelijkheid- en verantwoordingstructuur; 3. Kopie onderhoudscontracten van belangrijke apparatuur; 4. Kopie twee meeste recente rapporten die door een onderhoudsbedrijf zijn afgegeven.	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: 1. Er worden externe best practices en normen toegepast. Onderhoudsprocedures en contracten worden op elkaar afgestemd en geoptimaliseerd.	✓
Beoordeling (aanwezigen, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: security tool, roles worden gecombineerd de server opstellen worden enkel uitgevoerd door admin. Waarneming ter plaatse: 		
Aanbevelingen:		

3.13 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein 11.2.6

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.2.6
MBO controledoelstelling: Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.		
Toelichting: Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie. (Denk hier aan beveiligde/beheerde werkplekken en notebooks. Mobiele devices en BYOD wordt in toegangsbeleid meegenomen.)		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Beveiliging van beheerde werkplek/notebooks vindt by default / op individueel niveau plaats.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Bedrijfsmiddelen die worden verstrekt of uitgeleend, worden in de praktijk op uniforme wijze beveiligd.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Good practices worden toegepast. Beleid, proces en procedures zijn gedocumenteerd voor alle sleutelposities. Evidence: <ol style="list-style-type: none"> Kopie beleid of procedurebeschrijving voor beveiligen van apparatuur buiten de terreinen; Kopie van informatie waaruit blijkt dat de organisatie uitleen conform het beleid of procedurebeschrijving uitvoert. Denk bv aan: <ul style="list-style-type: none"> kopie verzekeringsovereenkomst; kopie e-mails, nieuwsbrief waaruit blijkt dat de medewerkers (organisatie) op de hoogte zijn gebracht over het beleid; Waarneming ter plaatse. 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: <ol style="list-style-type: none"> Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: <ol style="list-style-type: none"> Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	
Beoordeling (aanwezigen, datum en locatie):		
Bevindingen: <ul style="list-style-type: none"> Documenten: Interviews: Mobile device management en MPLS Waarneming ter plaatse: security tools 		
Aanbevelingen:		

3.14 Veilig verwijderen of hergebruiken van apparatuur

11.2.7

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 11.2.7
MBO controledoelstelling: Veilig verwijderen of hergebruiken van apparatuur Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.		
Toelichting: Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd. (Dit betreft informatie op zowel servers, werkplekken, beheerde/geleende notebooks, tablets, smartphones en ook eigen devices die worden hergebruikt of voor hergebruik worden afgevoerd.		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Individuele medewerkers classificeren zelf de gegevens die ze op mobiele media opslaan.	
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Er zijn praktijkafspraken hoe het afvoeren en hergebruik van bedrijfsmiddelen is geregeld.	
Volwassenheidsniveau 3 (gedefinieerd proces)	Good practices worden toegepast. Beleid, proces en procedures zijn gedocumenteerd voor alle sleutelposities. Afvoer en/of schonen van beheerde apparatuur door leveranciers is contractueel vastgelegd. Evidence: <ol style="list-style-type: none"> Kopie beleid of procedurebeschrijving voor veilig verwijderen of hergebruiken van apparatuur; Certificaten; Kopie van informatie waaruit blijkt dat de organisatie conform het beleid heeft uitgevoerd. Te denken aan: <ul style="list-style-type: none"> checklist die worden gebruikt bij het controleren van "veilig verwijderen of hergebruiken van apparatuur" en kopie van een aantal ingevulde checklisten; 	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: <ol style="list-style-type: none"> Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. 	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: <ol style="list-style-type: none"> Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. 	

Beoordeling (aanwezig, datum en locatie):
Bevindingen:
• Documenten:
• Interviews: De schijven worden gewipeed.
• Waarneming ter plaatse: Hardware wordt hergebruikt.
Aanbevelingen:

3.15 Kloksynchronisatie 12.4.4

Cluster: Ruimten en apparatuur		ISO 27002 nummer: 12.4.4
MBO controledoelstelling: Kloksynchronisatie De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdsbron.		
Toelichting: De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.		
Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Adhoc / initieel)	Operationeel, by default.	X
Volwassenheidsniveau 2 (herhaalbaar maar intuïtief)	Bottom-up, praktijkafspraken over gemaakt op operationeel niveau.	
Volwassenheidsniveau 3 (gedefinieerd proces)	De klokken van relevante informatiesystemen worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron. Evidence: 1. Kopie beleid en procedurebeschrijving voor het synchronisatie van systeemklokken; 2. Kopie van informatie waaruit blijkt dat de klokken van alle relevante informatiesystemen binnen de organisatie of beveiligingsdomein zijn gesynchroniseerd met overeengekomen nauwkeurige tijdsbron. Te denken aan: • kopie van welke tijdsbron (v.b. conform Coordinated Universal Time) die de organisatie gebruikt voor synchronisatie; 3. kopie van informatie waaruit blijkt dat de synchronisatie regelmatig plaats vindt. Te denken aan: • scherm print van het proces synchronisatie.	
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Evidence in aanvulling op 3: 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Evidence in aanvulling op 4: 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	
Beoordeling (aanwezig, datum en locatie):		
Bevindingen: • Documenten: • Interviews: 1 Time review • Waarneming ter plaatse: werknemers kunnen tijd niet veranderen.		
Aanbevelingen:		