mett

Verklaring van Toepasselijkheid

NEN-ISO/IEC 27001; 2017

Versie 2.0, datum 29-11-2019
Review: 18-09-2023

Activatie Verklaring van Toepasselijkheid

Voor u ligt de definitieve Verklaring van Toepasselijkheid (VVT) van Mett B.V. waarin de borging is beschreven van het informatieveiligheidsbeleid conform NEN-ISO/IEC 27001; 2017. De VVT beschrijft het normenkader waar de organisatie zich aan committeert en beschrijft eventuele redenen van uitsluiting.

Scope

De VVT strekt zich uit over de volgende onderneming: Mett B.V. Deze VVT is bestemd voor alle werknemers van Mett en haar stakeholders. Het gehanteerde Information Security Management System (ISMS) is van toepassing op de bedrijfsprocessen.

Verantwoordelijkheden

De reikwijdte van de VVT is vastgesteld in samenspraak met het directieteam. Met het ondertekenen is het de verantwoordelijkheid van de directie om de maatregelen te treffen die noodzakelijkerwijs volgen uit het ISMS. Toetsing van het NEN-ISO/IEC 27001 ISMS vindt plaats door geaccrediteerde certificatie instelling. Om het ISMS doeltreffend en efficiënt te houden treft de organisatie jaarlijks de nodige maatregelen en acties met de benodigde resources.

Ondertekend namens het directieteam van Mett B.V.		
Naam	Jeroen Rispens	*Handtekening* 
Functie	Directeur Mett	
Plaats	Utrecht	
Datum	18-09-2023	

MET DE ONDERTEKENING ACTIVEERT EN BORGT METT B.V. HET NORMENKADER ALS VOLGT:

Normeisen niet van toepassing.

Er worden geen normeisen uitgesloten. Alle eisen zijn van toepassing voor de organisatie Mett B.V.

Normeisen van toepassing

De organisatie en omgeving zijn in kaart gebracht middels een context,- stakeholder- en risicoanalyse. Op basis van deze analyses is vastgesteld dat de normeisen in onderstaande tabel van toepassing zijn voor Mett. De tabel beschrijft naast de maatregelen ook de context die op de eis van toepassing is binnen Mett:

- Wet & regelgeving (W&R)
- Klant
- Operationeel
- Risico
- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Beleid
- Monitor

5 Informatiebeveiligingsbeleid

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
05.1 Aansturing door de directie van de informatiebeveiliging											
05.1.1 Beleidsregels voor informatiebeveiliging	X				X	X	X	X		Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Geïmplementeerd
05.1.2 Beoordelen van het informatiebeveiligingsbeleid				X		X	X		X	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Geïmplementeerd

6. Organiseren van informatiebeveiliging

Paragraaf	W&R	KLANT	OPER	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
06.1 Interne organisatie											
06.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	X		X	X		X	X			Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Geïmplementeerd
06.1.2 Scheiding van taken	X		X	X	X	X	X	X		Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Geïmplementeerd
06.1.3 Contact met overheidsinstanties		X			X					Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Geïmplementeerd
06.1.4 Contact met speciale belangengroepen	X	X				X	X			Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	Geïmplementeerd
06.1.5 Informatiebeveiliging in projectbeheer		X	X		X					Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	Geïmplementeerd
06.2 Mobiele apparaten en telewerken											

06.2.1 Beleid voor mobiele apparatuur	X	X	X	X		X	X	X		Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Geïmplementeerd
06.2.2 Telewerken		X	X			X	X	X		Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	Geïmplementeerd

7. Veilig personeel

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
07.1 Voorafgaand aan het dienstverband											
07.1.1 Screening	X					X	X			Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Geïmplementeerd
07.1.2 Arbeidsvoorwaarden	X					X	X			De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijk-heden voor informatiebeveiliging en die van de organisatie vermelden.	Geïmplementeerd
07.2 Tijdens het dienstverband											
07.2.1 Directieverantwoordelijkheden				X		X	X			De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en	Geïmplementeerd

										procedures van de organisatie.	
07.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	X		X	X		X	X	X		Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Geïmplementeerd
07.2.3 Disciplinaire procedure	X		X			X	X	X		Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Geïmplementeerd
07.3 Beëindiging en wijziging van dienstverband											
07.3.1 Beëindiging of wijziging van verantwoordelijheden van het dienstverband	X		X			X	X			Verantwoordelijk-heden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	Geïmplementeerd

8. Beheer van bedrijfsmiddelen

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
08.1 Verantwoordelijkheid voor bedrijfsmiddelen											
08.1.1. Inventariseren van bedrijfsmiddelen			X	X	X	X	X		X	Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	Geïmplementeerd
08.1.2 Eigendom van bedrijfsmiddelen			X	X	X					Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Geïmplementeerd
08.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen			X		X			X	X	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd. Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	Geïmplementeerd

08.1.4 Teruggeven van bedrijfsmiddelen			X		X			X	X	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	Geïmplementeerd
08.2 Informatieclassificatie											
08.2.1 Classificatie van informatie	X	X	X	X		X	X	X		Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Geïmplementeerd
08.2.2. Informatie labelen						X	X	X		Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatie-schema dat is vastgesteld door de organisatie.	Geïmplementeerd
08.2.3. Behandelen van bedrijfsmiddelen	X	X	X	X		X	X			Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatie-	Geïmplementeerd

										schema dat is vastgesteld door de organisatie.	
08.3 Behandelen van media											
	X	X	X	X	X	X	X	X		Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Geïmplementeerd
	X	X	X	X		X	X	X		Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures	Geïmplementeerd
		X	X	X			X	X		Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Geïmplementeerd

9. Toegangsbeveiliging

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
09.1 Bedrijfseisen voor toegangsbeveiliging											
09.1.1 Beleid voor toegangsbeveiliging	X	X	X	X	X		X	X		Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligings-eisen.	Geïmplementeerd
09.1.2 Toegang tot netwerken en netwerkdiensten		X	X	X		X		X		Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Geïmplementeerd
09.2 Beheer van toegangsrechten van gebruikers											
09.2.1 Registratie en uitschrijving van gebruikers	X	X	X	X	X	X				Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Geïmplementeerd
09.2.2 Gebruikers toegang verlenen	X	X	X	X	X	X		X		Een formele gebruikerstoegangs-verleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Geïmplementeerd
09.2.3 Beheren van speciale toegangsrechten				X		X		X		Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Geïmplementeerd

09.2.4 Beheer van geheime authenticatie-informatie van gebruikers		X		X		X	X	X		Beheer van geheime authenticatie-informatie van gebruikers	Geïmplementeerd
09.2.5 Beoordeling van toegangsrechten van gebruikers		X	X	X		X		X		Beoordeling van toegangsrechten van gebruikers	Geïmplementeerd
09.2.6 Toegangsrechten intrekken of aanpassen		X	X	X		X				De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	Geïmplementeerd
09.3 Gebruiksersverant-woordelijkheden											
09.3.1 Geheime authenticatie-informatie gebruiken	X	X	X	X		X		X		Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Geïmplementeerd
09.4 Toegangsbeveiliging van systeem en toepassing											
09.4.1 Beperking toegang tot informatie		X	X	X		X		X		Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	Geïmplementeerd
09.4.2 Beveiligde inlogprocedures		X	X			X	X	X		Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Geïmplementeerd
09.4.3. Systeem voor wachtwoordbeheer		X	X	X		X		X		Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Geïmplementeerd

09.4.4 Speciale systeemhulpmiddelen gebruiken			X	X	X	X	X	X		Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	Geïmplementeerd
09.4.5. Toegangsbeveiliging op programmabroncode				X		X	X	X		Toegang tot de programmabroncode moet worden beperkt.	Geïmplementeerd

10. Cryptografie

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
10.1 Cryptografische beheersmaatregelen											
10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen						X	X	X		Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Geïmplementeerd
10.1.2 Sleutelbeheer						X	X	X		Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	Geïmplementeerd

11. Fysieke beveiliging en beveiliging van de omgeving

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
11.1 Beveiligde gebieden											
11.1.1 Fysieke beveiligingszone			X	X	X		X	X		Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	Geïmplementeerd
11.1.2 Fysieke toegangsbeveiliging		X	X		X		X	X		Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Geïmplementeerd
11.1.3 Kantoren, ruimten en faciliteiten beveiligen		X	X	X	X		X	X		Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Geïmplementeerd
11.1.4 Beschermen tegen bedreigingen van buitenaf			X		X		X	X		Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Geïmplementeerd
11.1.5 Werken in beveiligde gebieden			X		X		X	X		Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Geïmplementeerd
11.1.6 Laad- en loslocatie			X	X	X			X		Toegangspunten zoals laad- en loslocaties en andere	Geïmplementeerd

										punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	
11.2 Apparatuur											
11.2.1 Plaatsing en bescherming van apparatuur	X	X	X	X	X			X		Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Geïmplementeerd
11.2.2 Nutsvoorzieningen			X		X		X			Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Geïmplementeerd
11.2.3 Beveiliging van bekabeling			X	X	X		X			Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Geïmplementeerd
11.2.4 Onderhoud van apparatuur			X		X				X	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Geïmplementeerd
11.2.5 Verwijdering van bedrijfsmiddelen		X	X		X	X		X		Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Geïmplementeerd

11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein		X	X	X	X		X	X		Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Geïmplementeerd
11.2.7 Veilig verwijderen of hergebruiken van apparatuur			X				X	X		Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.	Geïmplementeerd
11.2.8 Onbeheerde gebruikersapparatuur		X	X	X		X	X	X		Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Geïmplementeerd
11.2.9 'Clear desk'- en 'clear screen'-beleid		X	X	X		X	X	X		Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	Geïmplementeerd

12. Beveiliging bedrijfsvoering

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
12.1 Bedieningsprocedures en verantwoordelijkheden											
12.1.1 Gedocumenteerde bedieningsprocedures		X	X		X					Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Geïmplementeerd
12.1.2 wijzigingsbeheer			X		X					Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	Geïmplementeerd
12.1.3 Capaciteitsbeheer			X	X	X				X	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Geïmplementeerd
12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen			X	X	X		X	X		Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Geïmplementeerd
12.2 Bescherming tegen malware											

12.2.1 Beheersmaatregelen tegen malware			X			X	X	X		Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Geïmplementeerd
12.3 Backup											
12.3.1 Back-up van informatie		X	X		X			X		Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Geïmplementeerd
12.4 Verslaglegging en monitoren											
12.4.1 Gebeurtenissen registreren		X	X						X	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligings gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Geïmplementeerd
12.4.2 Beschermen van informatie in logbestanden		X	X						X	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Geïmplementeerd
12.4.3 Logbestanden van beheerders en operators		X	X						X	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	Geïmplementeerd
12.4.4 Kloksynchronisatie								X		De klokken van alle relevante informatieverwerkende systemen binnen	Geïmplementeerd

										een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	
12.5 Beheersing van operationele software											
12.5.1 Software installeren op operationele systemen			X		X	X	X			Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	Geïmplementeerd
12.6 Beheer van technische kwetsbaarheden											
12.6.1 Beheer van technische kwetsbaarheden			X	X	X	X	X			Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	Geïmplementeerd
12.6.2 Beperkingen voor het installeren van software			X			X	X	X		Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	Geïmplementeerd
12.7 Overwegingen betreffende audits van informatiesystemen											
12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen		X	X		X					Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Geïmplementeerd

13. Communicatiebeveiliging

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
13.1 Beheer van netwerkbeveiliging											
13.1.1 Beheersmaatregelen voor netwerken		X	X	X	X	X	X			Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Geïmplementeerd
13.1.2 Beveiliging van netwerkdiensten		X	X	X	X	X	X			Beveiligings-mechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Geïmplementeerd
13.1.3 Scheiding in netwerken		X	X	X	X	X	X	X		Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Geïmplementeerd
13.2 Informatietransport											
13.2.1 Beleid en procedures voor informatietransport		X	X			X	X	X		Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteit en verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen	Geïmplementeerd

										voor transport van kracht zijn.	
13.2.2 Overeenkomsten over informatietransport		X	X			X	X			Overeenkomsten over informatietransport	Geïmplementeerd
13.2.3 Elektronische berichten		X	X	X		X	X	X		Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	Geïmplementeerd
13.2.4 Vertrouwelijkheids- of geheimhoudings overeenkomst	X	X	X	X	X	X	X	X		Eisen voor vertrouwelijkheids- of geheimhoudings-overeenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	Geïmplementeerd

14. Acquisitie, ontwikkeling en onderhoud van informatiesytemen

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
14.1 Beveiligingseisen voor informatiesystemen											
14.1.1 Analyse en specificatie van informatiebeveiligingseisen		X	X			X	X	X		De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Geïmplementeerd
14.1.2 Toepassingsdiensten op openbare netwerken beveiligen			X	X		X	X	X		Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Geïmplementeerd
14.1.3 Transacties van toepassingsdiensten beschermen			X	X		X	X	X		Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Geïmplementeerd
14.2 Beveiliging in ontwikkelings- en ondersteunende processen											
14.2.1 Beleid voor beveiligd ontwikkelen	X	X	X	X	X	X	X	X		Voor het ontwikkelen van software en systemen moeten regels worden	Geïmplementeerd

										vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	
14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen		X	X	X	X	X	X			Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	Geïmplementeerd
14.2.3 Technische beoordeling van toepassingen na wijzigingen bedieningsplatform			X	X		X	X			Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Geïmplementeerd
14.2.4 Beperkingen op wijzigingen aan softwarepakketten			X	X		X	X	X		Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	Geïmplementeerd
14.2.5 Principes voor engineering van beveiligde systemen			X	X		X	X	X		Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Geïmplementeerd
14.2.6 Beveiligde ontwikkelomgeving			X			X	X	X		Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Geïmplementeerd

14.2.7 Uitbestede softwareontwikkeling			X	X		X	X	X	X	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Geïmplementeerd
14.2.8 Testen van systeembeveiliging			X	X	X		X	X		Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Geïmplementeerd
14.2.9 Systeemacceptatietests			X	X	X		X	X		Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	Geïmplementeerd
14.3 Testdata											
14.3.1 Bescherming van testgegevens	X	X		X		X				Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Geïmplementeerd

15. Leveranciersrelaties

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
15.1 Informatiebeveiliging in leveranciersrelaties											
15.1.1 Informatiebeveiligings-beleid voor leveranciersrelaties	X		X	X		X	X	X		Met de leverancier moeten de informatiebeveiligings eisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	Geïmplementeerd
15.1.2 Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten			X	X		X	X			Alle relevante informatiebeveiligings eisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelement en ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Geïmplementeerd
15.1.3 Toeleveringsketen van informatie- en communicatietechnolog ie			X	X		X	X	X		Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligings risico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnol ogie	Geïmplementeerd

15.2 Beheer van dienstverlening van leveranciers											
15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers			X		X		X		X	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Geïmplementeerd
15.2.2 Beheer van veranderingen in dienstverlening van leveranciers			X		X		X		X	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Geïmplementeerd

16. Beheer van informatiebeveiligingsincidenten

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen											
16.1.1 Verantwoordelijkheden en procedures			X			X				Er moeten beheers-verantwoordelijk-heden en -procedures worden vastgesteld om te zorgen voor een snelle, doeltreffende en ordentelijke reactie op incidenten met informatiebeveiliging.	Geïmplementeerd
16.1.2 Rapportage van informatiebeveiligings gebeurtenissen			X			X				Informatiebeveiligings -gebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Geïmplementeerd
16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging			X			X	X	X	X	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Geïmplementeerd
16.1.4 Beoordeling van en besluitvorming over informatiebeveiligings gebeurtenissen			X			X	X			Informatiebeveiliging-gebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligings	Geïmplementeerd

										incidenten.	
16.1.5 Respons op informatiebeveiligings incidenten		X	X	X	X	X				Op informatiebeveiligings -incidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Geïmplementeerd
16.1.6 Lering uit informatiebeveiligings incidenten			X	X	X	X	X		X	Kennis die is verkregen door informatiebeveiliging-incidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Geïmplementeerd
16.1.7 Verzamelen van bewijsmateriaal		X	X							De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Geïmplementeerd

17. Informatiebeveiligingsaspecten van bedrijfs continuïteitsbeheer

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
17.1 Informatiebeveiligingscontinuïteit											
17.1.1 Informatiebeveiligings continuïteit plannen			X	X	X					De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligings -beheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Geïmplementeerd
17.1.2 Informatiebeveiliging-continuïteit implementeren		X	X	X	X	X	X			De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Geïmplementeerd
17.1.3 Informatiebeveiliging-continuïteit verifiëren, beoordelen en evalueren			X		X				X	De organisatie moet de ten behoeve van informatiebeveiligings continuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Geïmplementeerd
17.2 Redundante componenten											

17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten			X		X					Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Geïmplementeerd

18. Naleving

Paragraaf	W&R	KLANT	OPERATIONEEL	RISICO	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Beleid	Monitor	ISO 27001 maatregel	Status
18.1 Compliance met juridische standaarden											
18.1.1 Identificatie van toepasbare wet- en regelgeving	X	X	X	X		X	X			Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	Geïmplementeerd
18.1.2 Intellectueel eigendom rechten	X	X	X	X		X				Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigendomssoftware-producten te waarborgen moeten passende procedures worden geïmplementeerd.	Geïmplementeerd
18.1.3 Bescherming van records	X	X		X		X	X			Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Geïmplementeerd

18.1.4 Privacy en bescherming van persoonlijke data	X	X		X		X	X			Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Geïmplementeerd
18.1.5 Beheersmaatregel van cryptografische controls		X	X			X	X	X		Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Geïmplementeerd
18.2 Informatie veiligheid reviews											
18.2.1 onafhankelijke review van inform veiligheid						X	X	X		De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen , beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	Geïmplementeerd
18.2.2 Compliance met beleid en standaarden						X	X	X		De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheids gebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Geïmplementeerd
18.2.3 Technische compliance review						X	X		X	Informatiesystemen moeten regelmatig	Geïmplementeerd

										worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	