Statement Of Applicability

Datum van vastelling: 04/03/2018

nr.	Clausule ISO/IEC 27001:2013 Annex A controls	Controle	Van toepas	reden uitsluiting	Status	Uitleg of referentie naar controle
A.5	Informatieveiligheidsbeleid					
A.5.1	Beleidssturing voor informatieveiligheid	[2]				
A.5.1.1	Beleid voor informatieveiligheid	Een set van beleidsplannen voor informatiebeveiliging wordt vastgesteld, goedgekeurd door het management, gepubliceerd en meegedeeld aan medewerkers en relevante externe partijen.	ja		4. Beheerd en meetbaar	Het beleid omtrent informatieveiligheid zet de lijnen uit om 'Information Security' te benaderen. Het informatieveiligheidsbeleid bestaat uit de manual voor het ISMS met het actieplan en het onthaal- en instructiehandboek waarbij het beleid omtrent informatieveiligheid uitgewerkt wordt. Dit is goedgekeurd door de CEO. De beleidsverklaring wordt gecommuniceerd op de website en de server. Daarnaast wordt de beleidsverklaring opgenomen in het informatieveiligheidsbeleid in het onthaal- en instructiehandboek zodat alle stakeholders van Trustteam op de hoogte zijn.
A.5.1.2	Beoordeling informatieveiligheidsbeleid	Het informatiebeveiligingsbeleid wordt op geregelde tijdstippen beoordeeld of als er belangrijke wijzigingen voordoen om de continue geschiktheid, adequaatheid en doeltreffendheid ervan te garanderen.	ja		3. Gedefinieerd proces	De ISMS manager ziet toe op de opvolging en de bijsturing van het informatieveiligheidsbeleid. Dit wordt jaarlijks gereviewed op basis van interne audits, legal compliance check, check van de Statement of Applicability en de directiebeoordeling. Alle wijzigingen aan het beleidsplan worden goedgekeurd door de CEO. Dit beleid wordt beoordeeld in het ISMS team dat driemaandelijks samen komt om een vaste agenda te bespreken.
A.6	Organisatie van informatiebeveiliging					
A.6.1	Interne organisatie					
A.6.1.1	Rollen en verantwoordelijkheden informatieveiligheid	Alle verantwoordelijkheden omtrent informatiebeveiliging worden vastgesteld en toegewezen.	ja		3. Gedefinieerd proces	De rollen, verantwoordelijkheden en bevoegdheden zijn gekaderd binnen het organogram van de organisatie. Alle verantwoordelijkheden omtrent informatieveiligheid zijn omschreven in de functiematrix. Alle rollen en verantwoordelijkheden van werknemers, onderaannemers en stakeholders zijn bepaald en gedocumenteerd in het informatieveiligheidsbeleid en in de ISMS Manual Follow-up.
A.6.1.2	Scheiding van taken	Tegenstrijdige taken en bevoegdheden moeten worden gescheiden om de mogelijkheden voor ongeoorloofde of onbedoelde wijziging of misbruik van de data van de organisatie te verminderen.	ja		3. Gedefinieerd proces	Er is een organogram opgemaakt met bijhorende functiematrix waardoor alle taken opgesplitst zijn tussen personen en iedereen op de hoogte is van elkaars verantwoordelijkheden.
A.6.1.3	Contact met overheidsinstanties	De nodige contacten met de relevante autoriteiten worden gehandhaafd.	ja		3. Gedefinieerd proces	In de stakeholdersmatrix worden de aanpak en aandachtspunten bepaald om contact te onderhouden met de federale overheid door middel van het jaarrapport en de Europese overheidsinstanties d.m.v. communicatie naar de privacycommissie in kader van de GDPR wetgeving. Dit is geregistreerd onder de vorm van een communicatieplan (wat, wie en wanneer wordt er gecommuniceerd?) in de stakeholdersmatrix.
A.6.1.4	Contact met stakeholders	De nodige contacten met belangengroepen en andere gespecialiseerde security forums en beroepsorganisaties worden gehandhaafd.	ja		3. Gedefinieerd proces	In de stakeholdersmatrix worden de aanpak en aandachtspunten bepaald voor elke stakeholder en zijn relatie tot het ISMS. Daarnaast nemen we een communicatieplan (wat, wie en wanneer wordt er gecommuniceerd?) op in de stakeholdersmatrix voor elke gedefinieerde stakeholder.
A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging wordt ook meegenomen in het projectmanagement, ongeacht het type van het project.	ja		4. Beheerd en meetbaar	Door middel van een apart ondersteunend proces van projectmanagement zorgt Trustteam ervoor dat elk project voldoende opgevolgd wordt door de projectleider om het niveau van informatieveiligheid te waarborgen.
A.6.2	Mobiele apparatuur en teleworking					
A.6.2.1	Beleid mobiele apparatuur	Een beleid en ondersteunende veiligheidsmaatregelen worden genomen om de risico's geïntroduceerd door het gebruik van mobiele apparaten te beheren.	ja		3. Gedefinieerd proces	Er is een beleid en procedure opgesteld om de mogelijke risico's bij het gebruik van mobiele apparatuur te ondervangen. Deze is opgenomen in het onthaal- en instructiehandboek.
A.6.2.2	Teleworking	Een beleid en ondersteunende veiligheidsmaatregelen moeten worden geïmplementeerd om informatie te beschermen waartoe toegang verschaft wordt of dat verwerkt of opgeslagen wordt bij telewerken.	ja		3. Gedefinieerd proces	Thuis werken wordt uiterst zelden toegepast binnen Trustteam. Bepaalde medewerkers werken wel op locatie. Daarvoor zijn beveiligde verbindingen met de data van Trustteam opgesteld en zijn er passende regels vooropgeseteld die opgenomen zijn als procedure in het onthaal- en instructiehandboek.
A.7	Veiligheid personeelszaken					
A.7.1	Voorafgaand aan de tewerkstelling					
A.7.1.1	Screening	Achtergrondcontroles van alle kandidaten voor werkgelegenheid, aannemers en andere derde partijen worden uitgevoerd in overeenstemming met de relevante wet- en regelgeving en ethiek, en evenredig aan de bedrijfseisen, de toegang tot informatie die samenhangt met de opdracht en de waargenomen risico's.	ja		4. Beheerd en meetbaar	Bij aanwerving wordt de checklist gevolgd om aan alle topics omtrent informatieveiligheid te voldoen die bij de beoogde functie hoort. De screening gebeurt door middel van refertentiechecks op basis van de CV. Eventueel kan daar een background check bij komen (bewijs van goede zeden) bij bepaalde functies.
A.7.1.2	Arbeidsvoorwaarden	De contractuele afspraken met werknemers en contractanten nemen zijn verantwoordelijkheden en deze van de organisatie op voor informatiebeveiliging.	ja		3. Gedefinieerd proces	In het arbeidscontract voor medewerkers wordt een artikel opgenomen omtrent informatieveiligheid en de bijhorende verantwoordelijkheden van de werknemer. Voor de samenwerking met de leverancier wordt dit opgenomen in de verwerkersovereenkomt of het afgesloten contract. Beiden wordt mee ondertekend bij aanvang van de tewerkstelling of samenwerking. Daarnaast zijn in het onthaal- en instructiehandboek alle policies en procedures opgenomen. Bij ontvangst wordt een formulier ondertekend waarin de ontvanger aangeeft dat de brochure werd ontvangen, gelezen, begrepen en voor akkoord onthaald werd.
A.7.2	Tijdens de tewerkstelling					

A.7.2.1	Directieverantwoordelijkheden	Het bestuur stelt medewerkers, aannemers en derde partijen aan om de veiligheid toe te passen in overeenstemming met het vastgestelde beleid en de procedures van de organisatie.	ja		5. Geoptimaliseerd	De ISMS manager is als staf opgenomen in het organogram. In de functiematrix worden alle verantwoordelijkheden, bevoegdheden en rollen van de directie en staf omschreven o.a. in het kader van het ISMS.
A.7.2.2	bewustzijn, opleiding en training t.a.v. informatieveiligheid	Alle medewerkers van de organisatie en, indien van toepassing, aannemers en derde partijen zullen passende bewustwordingstraining en regelmatige updates in organisatorisch beleid en procedures krijgen, voor zover deze relevant zijn voor hun functie.	ja		3. Gedefinieerd proces	Door middel van een opleiding ISMS worden alle betrokken medewerkers geïnformeerd en opgeleid. Alle gevolgde opleidingen worden geregistreerd en afgezet t.o.v. de vereiste opleidingen per functie en functionaris. Dit gebeurt in een competentiematrix Daarnaast wordt informatieveiligheid mee opgenomen in het onthaal- en instructiehandboek van de medewerkers. Ten derde is er voorzien in een campagne rond informatieveiligheid om in te spelen op de bewustwording van medewerkers en andere stakeholders.
A.7.2.3	Tuchtprocedure	Er moet een formele disciplinaire procedure zijn voor werknemers die een inbreuk op de beveiliging hebben begaan	ja		3. Gedefinieerd proces	Bij het overtreden of misbruik maken van de toegang tot informatie wordt het contract met de leverancier of medewerker verbroken. De verbrekingsvoorwaarden worden opgenomen in het leveranciers- of arbeidscontract en in het onthaal- en instructiehandboek.
A.7.3	Beëindigen of wijzigen van tewerkstelling					
A.7.3.1	Beëindigen of wijzigen van tewerkstellingsverantwoordelijkheden	Er moet een formele disciplinaire procedure zijn voor werknemers die een inbreuk op de beveiliging hebben gepleegd.	ja		4. Beheerd en meetbaar	Bij het einde van de tewerkstelling wordt de checklist 'einde tewerkstelling' gevolgd om alle toegang tot de informatie op een correcte wijze te veranderen of af te sluiten. Indien verantwoordelijkheden en plichten i.f.v. informatieveiligheid van kracht blijven na de tewerkstelling worden deze omschreven en opgelegd in het arbeidscontract.
A.8	Beheer van bedrijfsmiddelen					
A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen					
A.8.1.1	Inventaris van bedrijfsmiddelen	Middelen die verband houden met informatie en informatieverwerkingsfaciliteiten worden geïdentificeerd en in een inventaris van deze middelen bijgehouden.	ja		3. Gedefinieerd proces	Alle persoonsgegevens die binnen de processen van Trustteam aan bod komen zijn in kaart gebracht in de procesbeschrijvingen per proces. De behandeling en bescherming van al deze gegevens zijn gedefinieerd. Daarnaast zijn alle hardware van Trustteam in kaart gebracht in een inventaris van de bedrijfsmiddelen.
A.8.1.2	Eigendom van bedrijfsmiddelen	Middelen, opgenomen in de inventaris, moeten voorzien zijn van een eigenaar.	ja		3. Gedefinieerd proces	In de opgemaakte inventaris wordt vermeld dat de bedrijfsmiddelen eigendom zijn van Trustteam. Daarbij wordt de eigenaar van het bedrijfsmiddel vermeld en indien nodig zijn de vereisten naar onderhoud of updates mee opgenomen in de inventaris van bedrijfsmiddelen.
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van informatie en het gebruik van middelen in verband met de verwerking van informatie moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	ja		4. Beheerd en meetbaar	Het aanvaardbaar gebruik van de bedrijfsmiddelen wordt opgenomen in een deontologische code die opgenomen wordt in het arbeidscontract en het onthaal- en instructiehandboek.
A.8.1.4	Teruggeven van bedrijfsmiddelen	Alle medewerkers, aannemers en derde partijen zullen alle middelen van de organisatie in hun bezit teruggeven bij beëindiging van het dienstverband, contract of overeenkomst.	ja		4. Beheerd en meetbaar	Alle gebruikte assets van Trustteam worden bij het einde van de tewerkstelling of samenwerking volgens de checklist terugbezorgd aan Trustteam.
A.8.2	Informatieclassificatie					
A.8.2.1	Classificeren van informatie	Informatie worden ingedeeld in termen van wettelijke voorschriften, waarde, kritikaliteit en gevoeligheid voor ongeoorloofde openbaarmaking of wijziging.	ja		4. Beheerd en meetbaar	Door middel van het uitvoeren van een risicoanalyse wordt alle informatie onderwopren aan de analyse volgens CIA en informatieveiligheidsrisico of calamiteit om op die mogelijke risico's in te spelen. In de procedure voor gegevens- en documentbeheersing in het procedurehandboek wordt aandacht besteed aan de behandeling van gegevens en documenten die beschermd moeten worden.
A.8.2.2	Informatie labelen	Een passende reeks procedures om informatie te labelen worden ontwikkeld en uitgevoerd in overeenstemming met de door de organisatie aangenomen informatie-indeling.	ja		3. Gedefinieerd proces	In de procedure voor gegevens- en documentbeheersing is een vuistregel vastgelegd om officiële documenten te labelen en ordenen binnen het ISMS. Door middel van een vaste mappenstructuur krijgt elk document zijn plaats binnen het ISMS. Daarnaast wordt de informatie beveiligd door specifieke toegangsrechten toe te kennen afhankelijk van de informatie.
A.8.2.3	Omgaan met bedrijfsmiddelen	Procedures voor de behandeling van bedrijfsmiddelen worden ontwikkeld en geïmplementeerd in overeenstemming met de door de organisatie aangenomen informatie-indeling.	ja		3. Gedefinieerd proces	Het omgaan met bedrijfsmiddelen wordt opgenomen in de procedure voor aanwerving en einde tewerkstelling. Door middel van het rechtenbeheer op informatie wordt er rekening gehouden met de cruciale bedrijfsmiddelen die toegang verschaffen tot vertrouwelijke informatie.
A.8.3	Omgaan met media					
A.8.3.1	Beheer van verwijderbare media	Procedures worden geïmplementeerd voor het beheer van verwijderbare media in overeenstemming met de door de organisatie aangenomen informatie-indeling.	ja		3. Gedefinieerd proces	De procedure voor het verwijderen van media is opgenomen in het onthaal- en instructiehandboek.
A.8.3.2	Verwijderen van media	Media moeten veilig worden verwijderd d.m.v. het gebruik van formele procedures wanneer zij niet langer nodig zijn.	ja		3. Gedefinieerd proces	De procedure voor het verwijderen van media is opgenomen in het onthaal- en instructiehandboek.
A.8.3.3	Fysieke overdracht van media	Media die informatie bevat, moet wordenbeschermd tegen ongeautoriseerde toegang, misbruik of beschadiging tijdens het transport.	ja		3. Gedefinieerd proces	De procedure die alle aandachtspunten in functie van de bescherming van informatie tijdens een informatieoverdracht omvat is opgenomen in het onthaal- en instructiehandboek.
A.9	Toegangsbeveiliging					
A.9.1	Bedrijfseisen voor toegangsbeveiliging					
A.9.1.1	Toegangsbeveiligingsbeleid	Een toegangscontrole beleid moet worden opgesteld, gedocumenteerd en beoordeeld op basis van zakelijke en informatiebeveiligingseisen.	ja		3. Gedefinieerd proces	Door middel van toegangsrechtenbeheer wordt nagegaan wie toegang krijgt tot welke informatie.
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers mogen alleen worden voorzien van toegang tot het netwerk en de netwerkdiensten waarvoor zij speciaal gemachtigd zijn om te gebruiken.	ja		3. Gedefinieerd proces	Bij aanwerving van medewerkers wordt de checklist van aanwerving doorlopen waarbij verwezen wordt naar het rechtenbeheer om deze persoon op die manier toegang te geven tot de juiste netwerken en servers.
A.9.2	Beheer gebruikerstoegang					

A.9.2.1	Registratie en uitschrijven gebruikers	Een formeel gebruikersregistratie- en de-registratieproces wordt uitgevoerd om de toewijzing van toegangsrechten mogelijk te maken.	ja		3. Gedefinieerd proces	Alle gebruikers hebben een account die beveiligd is met een wachtwoord. Elke account geeft specifieke toegang tot specifieke documenten en databases. Deze toegang wordt vastgelegd in een rechtenmatrix. Er wordt een onderscheid gemaakt tussen leesrecht en schrijfrecht indien van toepassing.
A.9.2.2	Gebruikerstoegang voorzien	Een formele gebruikerstoegang voorzieningsproces worden uitgevoerd om de toegangsrechten toe te kennen of in te trekken voor elk type gebruiker en voor alle systemen en diensten.	ja		3. Gedefinieerd proces	De rechtenmatrix wordt gebruikt om te bepalen wie welke toegang en welke rechten krijgt.
A.9.2.3	Beheer van bijzondere toegangsrechten	De toewijzing en het gebruik van bevoorrechte toegangsrechten worden beperkt en gecontroleerd.	ja		3. Gedefinieerd proces	De toegang tot specifieke mappen, serveronderdelen en databases wordt bepaald volgens de functie waarin iemand tewerkgesteld is. Deze bepalingen zijn vastgelegd in de rechtenmatrix.
A.9.2.4	Beheer van geheime identificatie-informatie van gebruikers	De toewijzing van geheime idintificatie-informatie wordt gecontroleerd door middel van een formeel proces.	ja		3. Gedefinieerd proces	Alle vereisten voor het opmaken en gebruiken van wachtwoorden is vastgelegd in de procedure wachtwoorden die opgenomen is in het onthaal- en instructiehandboek.
A.9.2.5	Beoordeling toegangsrechten gebruikers	Eigenaars van bedrijfsmiddelen herzien de toegangsrechten van de gebruikers op regelmatige tijdstippen.	ja		3. Gedefinieerd proces	Alle vereisten voor het opmaken en gebruiken van wachtwoorden is vastgelegd in de procedure wachtwoorden die opgenomen is in het onthaal- en instructiehandboek. De toegang is vastgelegd in een rechtenmatrix.
A.9.2.6	Beoordeling of aanpassing toegangsrechten	De toegangsrechten van alle medewerkers en derde partijen tot informatie en informatieverwerkingsvoorzieningen moeten bij beëindiging van het dienstverband, contract of overeenkomst, worden verwijderd of aangepast bij verandering.	ja		3. Gedefinieerd proces	Alle toegang tot bepaalde documenten of databases bij medewerkers, leveranciers of andere stakeholders worden opgeheven bij het einde van de tewerkstelling of samenwerking. Indien het gaat om een verandering in de tewerkstelling of samenwerking worden ook de toegangsrechten bijgewerkt. Deze toegang wordt vastgelegd in een rechtenmatrix.
A.9.3	Gebruikersverantwoordelijkheden					
A.9.3.1	Gebruik van geheime identificatie-informatie	Gebruikers zijn verplicht om de praktijken van de organisatie te volgen in het gebruik van geheime identificatie-informatie.	ja		4. Beheerd en meetbaar	De medewerkers moeten de bestaande policies en procedures opvolgen. Deze worden opgenomen in het onthaal- en instructiehandboek. Deze moet ondertekend worden. Daarnaast wordt dit opgenomen in het arbeidscontranct en bij de checklist bij aanwerving zodat alle eisen bij opstart in rekening gebracht kunnen worden. Door middel van een interne opleiding ISMS worden alle praktijken kenbaar gemaakt, uitgelegd en opgevolgd. Daarnaast worden er interne audits uitgevoerd om de opvolging van de na te leven policies en procedures na te gaan.
A.9.4	Toegangsbeveiliging van systemen en applicaties					
A.9.4.1	Beperking toegang tot informatie	Toegang tot informatie en de toepassing van systeemfuncties wordt beperkt in overeenstemming met het toegangscontrolebeleid.	ja		4. Beheerd en meetbaar	Samen met het opmaken van het organogram en de functiematrix werd nagegaan welke rollen toegang krijgen tot welke informatie (op de server, in databases, enzovoort) = rechtenbeheer. Deze regels worden vastgelegd in een matrix zodat nieuwe medewerkers onmiddellijk toegang krijgen tot de juiste gegevens.
A.9.4.2	Beveiligde inlogprocedures	Indien vereist door het toegangscontrolebeleid, wordt de toegang tot systemen en toepassingen gecontroleerd door een beveiligde log-on procedure.	ja		5. Geoptimaliseerd	Elke computer, database, … is adequaat beveiligd
A.9.4.3	Systeem voor wachtwoordbeheer	Het wachtwoordbeleid is interactief en draagt zorg voor de kwaliteit van wachtwoorden.	ja		4. Beheerd en meetbaar	Is opgenomen in een procedure en kenbaar gemaakt aan alle medewerkers.
A.9.4.4	Bijzondere systeemhulpmiddelen gebruiken	Het gebruik van hulpprogramma's die in staat zijn om systemen en applicatie controles te overtreffen zou kunnen worden beperkt en streng gecontroleerd.	ja		3. Gedefinieerd proces	Enkel programma's en software die aan de door Trustteam gestelde vereisten voldoen, worden aangekocht voor intern gebruik of voor klanten.
A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de broncode van een programma wordt beperkt.	ja		3. Gedefinieerd proces	Is vastgelegd dmv functie- en rechtenmatrix. Ontwikkeling is mee opgenomen in de van toepassing zijnde procesbeschrijvingen
A.10	Cryptografie					
A.10.1	Cryptografische controles					
A.10.1.1	Beleid inzake gebruik van cryptografische controles	Een beleid inzake het gebruik van cryptografische controles voor de bescherming van gegevens worden ontwikkeld en uitgevoerd.	ja		4. Beheerd en meetbaar	Is opgenomen in een procedure en kenbaar gemaakt aan alle medewerkers.
A.10.1.2	Sleutelbeleid	Een beleid op het gebruik, de beveiliging en de levensduur van de cryptografische sleutels worden ontwikkeld en geïmplementeerd door hun hele levenscyclus.	ja		4. Beheerd en meetbaar	Is opgenomen in een procedure en kenbaar gemaakt aan alle medewerkers.
A.11	Fysicke en omgevingsbeveiliging					
A.11.1	Beveiligde omgeving					
A.11.1.1	Fysieke beveiligingsperimeter	Veiligheidsperimeters worden gedefinieerd en gebruikt om gebieden die ofwel gevoelige of kritieke informatie en informatieverwerkingsfaciliteiten bevatten te beschermen.	ja		5. Geoptimaliseerd	Wordt toegepast.
A.11.1.2	Fysieke ingangscontrole	Beveiligde gebieden worden door passende controles bij binnenkomst beschermd om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	ja		5. Geoptimaliseerd	Wordt toegepast.
A.11.1.3	Beveiliging van kantoren, ruimtes en faciliteiten	Fysieke beveiliging voor kantoren, kamers en faciliteiten worden ontwikkeld en toegepast.	ja		5. Geoptimaliseerd	Wordt toegepast.
A.11.1.4	Bescherming tegen externe en omgevingsgerelateerde bedreigingen	Fysieke bescherming tegen natuurrampen, kwaadaardige aanvallen of ongelukken moeten zo worden ontworpen en toegepast.	ja		5. Geoptimaliseerd	Wordt toegepast.
A.11.1.5	Werken in een beveiligde omgeving	Procedures voor het werken in veilige gebieden worden ontworpen en toegepast.	ja		3. Gedefinieerd proces	De procedure is beschreven en wordt toegepast.

A.11.1.6	Laad- en losruimte	Toegangspunten, zoals de levering- en laadplaatsen van gebieden en andere plaatsen waar onbevoegden het terrein kunnen betreden, moeten worden gecontroleerd en, indien mogelijk, geïsoleerd van informatieverwerkingsfaciliteiten om onbevoegde toegang te voorkomen.	ja		5. Geoptimaliseerd	Wordt toegepast.
A.11.2	Uitrusting					
A.11.2.1	Situering en bescherming van de uitrusting	De apparatuur moet worden geplaatst en beschermd om de risico's van de bedreigingen voor het milieu en de risico's en kansen voor onbevoegde toegang te beperken.	ja		4. Beheerd en meetbaar	Wordt toegepast.
A.11.2.2	Nutsvoorzieningen	De apparatuur moet worden beschermd tegen stroomstoringen en andere storingen veroorzaakt door storingen in het ondersteunen van nutsbedrijven.	ja		4. Beheerd en meetbaar	Wordt toegepast.
A.11.2.3	Beveiliging van bekabeling	Energie- en telecommunicatiebekabeling die gegevens vervoeren of informatiediensten ondersteunen worden beschermd tegen onderschepping of beschadiging.	ja		3. Gedefinieerd proces	Wordt toegepast.
A.11.2.4	Onderhoud van de uitrusting	Apparatuur moet correct worden gehandhaafd om de voortdurende beschikbaarheid en integriteit te garanderen.	ja		3. Gedefinieerd proces	Wordt toegepast.
A.11.2.5	Verwijderen van bedrijfsmiddelen	Apparatuur, informatie of software mag niet off-site worden meegenomen zonder voorafgaande toestemming.	ja		3. Gedefinieerd proces	De procedure is beschreven en wordt toegepast.
A.11.2.6	Beveiliging van uitrusting en bedrijfsmiddelen buiten het terrein	Beveiliging wordt toegepast op off-site bedrijfsmiddelen, waarbij rekening wordt gehouden met de verschillende risico's van het werken buiten de kantoren van de organisatie.	ja		3. Gedefinieerd proces	Wordt toegepast.
A.11.2.7	Veilig verwijderen of hergebruiken van uitrustingen	Alle onderdelen van de uitrusting die opslagmedia bevatten, moet worden gecontroleerd om ervoor te zorgen dat alle gevoelige gegevens en software onder licentie is verwijderd of veilig overgeschreven voorafgaand aan verwijdering of hergebruik.	ja		3. Gedefinieerd proces	Wordt toegepast.
A.11.2.8	Onbeheerde uitrusting	Gebruikers zorgen ervoor dat onbewaakte apparatuur op een passende wijze beschermd is.	ja		4. Beheerd en meetbaar	De procedure is beschreven en wordt toegepast.
A.11.2.9	Clear desk' en 'clear screen' beleid	Een duidelijke desk policy voor papier en verwijderbare opslagmedia en een helder scherm beleid worden vastgesteld voor verwerkingsinstanties.	ja		4. Beheerd en meetbaar	De procedure is beschreven en wordt toegepast.
A.12	Operationele veiligheid					
A.12.1	Operationele procedures en verantwoordelijkheden					
A.12.1.1	Gedocumenteerde operationele procedures	Operationele procedures moeten worden gedocumenteerd, onderhouden en ter beschikking gesteld van alle gebruikers die ze nodig hebben.	ja		4. Beheerd en meetbaar	Alle gemaakte procedures worden opgenomen in het procedurehandboek, de procesbeschrijving van het desbetreffend proces of het onthaal- en instructiehandboek die onder elke werknemer wordt verdeeld.
A.12.1.2	Veranderingsmanagement	Wijzigingen in de organisatie, bedrijfsprocessen, informatieverwerkingsfaciliteiten en systemen die informatiebeveiliging beïnvloeden, moeten worden gecontroleerd.	ja		4. Beheerd en meetbaar	De ISMS manager en de Interne ICT Manager volgen alles op in het kader van informatieveiligheid. Wanneer er iets verandert, wordt de procedure 'Management of Change' uit het procedurehandboek erbij genomen. Dat is een stappenplan met alle te nemen stappen bij een wijziging in de organistaie.
A.12.1.3	Capaciteitsbeheer	Het gebruik van de middelen moet worden gemonitord, afgestemd en projecties gemaakt van de toekomstige benodigde capaciteit om de vereiste prestaties van het systeem te waarborgen.	ja		4. Beheerd en meetbaar	De KPI's en de boordtabel worden besproken in ISMS team.
A.12.1.4	Scheiding van ontwikkeling, testing en productieomgevingen	Ontwikkelings-, testings- en operationele omgevingen worden gescheiden om de risico's van onbevoegde toegang of wijzigingen in de operationele omgeving te verminderen.	ja		5. Geoptimaliseerd	Wordt toegepast.
A.12.2	Bescherming tegen malware					
A.12.2.1	Controles tegen malware	Detectie, preventie en herstel controles om te beschermen tegen malware worden uitgevoerd in combinatie met een gepast bewustzijn bij de gebruiker.	ja		5. Geoptimaliseerd	Wordt toegepast.
A.12.3	Back-up					
A.12.3.1	Informatieback-up	Back-ups van de informatie, software en het systeem worden genomen en regelmatig getest in overeenstemming met een overeengekomen backup beleid of procedure.	ja		3. Gedefinieerd proces	Wordt toegepast.
A.12.4	Registreren en beoordelen					
A.12.4.1	Gebeurtenissen registreren	Event logs die activiteiten van gebruikers, uitzonderingen, fouten en informatiebeveiligingsgebeurtenissen registreert, worden geproduceerd, onderhouden en regelmatig beoordeeld.	ja		4. Beheerd en meetbaar	In het meldingsrigster voor afwijkingen, klachten en meldingen worden alle gebeurtenissen geregistreerd. De automatisch gelogde gegevens en de meldingen in het meldingsregister worden in het ISMS team besproken.
A.12.4.2	Beschermen van informatie in logbestanden	Logging faciliteiten en log gegevens worden beschermd tegen sabotage en toegang door onbevoegden.	ja		4. Beheerd en meetbaar	De geregistreerde logfiles worden bijgehouden op de server. De toegang tot de logfiles is bepaald door middel van de rechtenmatrix.
A.12.4.3	Beheerder en gebruiker van logbestanden	Systeembeheerder- en netbeheerdersactiviteiten worden geregistreerd en de logboeken worden beschermd en regelmatig beoordeeld.	ja		4. Beheerd en meetbaar	De geregistreerde logfiles worden bijgehouden op de server. De toegang tot de logfiles is bepaald door middel van de rechtenmatrix.
A.12.4.4	kloksynchronisatie	De klokken van alle relevante informatiesystemen binnen een organisatie of securitydomein worden gesynchroniseerd met één enkele tijdsbron.	ja		5. Geoptimaliseerd	De kloksynchronisatie is reeds van toepassing zodat alle systemen hetzelfde tijdstip aangeven.
A.12.5	Controle van de operationele software					
A.12.5.1	Software installeren op operationele systemen	Procedures worden uitgevoerd om de installatie van de software te controleren op operationele systemen.	ja		3. Gedefinieerd proces	Wordt toegepast.
A.12.6	Beheer van technische kwetsbaarheden					

A.12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen worden gebruikt moeten tijdig worden verkregen, blootstelling van de organisatie om dergelijke kwetsbaarheden geëvalueerd en passende maatregelen genomen om de bijbehorende risico's aan te pakken.	ja		4. Beheerd en meetbaar	Door middel van het uitvoeren van een risicoanalyse op alle processen van Trustteam is er een duidelijk beeld van de op te volgen maatregelen. Dit gebeurt via interne audits waarvoor een audit checklist is opgesteld.
A.12.6.2	Beperkingen op software-installatie	Regels voor de installatie van de software door de gebruikers worden vastgesteld en uitgevoerd.	ja		3. Gedefinieerd proces	Dit proces is beschreven en wordt toegepast.
A.12.7	Overwegingen audit informatiesystemen					
A.12.7.1	Controle op audit informatiesystemen	Controle-eisen en activiteiten met betrekking tot de verificatie van de operationele systemen moeten zorgvuldig worden gepland en afgesproken om verstoringen van de bedrijfsprocessen te minimaliseren.	ja		3. Gedefinieerd proces	Dit proces is beschreven en wordt toegepast. Interne en externe audits worden uitgevoerd.
A.13	Beveliging van communicatie					
A.13.1	Beheer netwerkbeveiliging					
A.13.1.1	Netwerkcontroles	Netwerken worden beheerd en gecontroleerd om informatie in systemen en applicaties te beschermen.	ja		4. Beheerd en meetbaar	De procedure is beschreven en wordt toegepast.
A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, service levels en beleidseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in de overeenkomsten met de netwerkdiensten, ongeacht of deze diensten in-house of uitbesteed zijn.	ja		4. Beheerd en meetbaar	De procedure is beschreven en wordt toegepast.
A.13.1.3	Scheiden van netwerken	Groepen van informatie-diensten, gebruikers en informatiesystemen worden gescheiden op netwerken.	ja		4. Beheerd en meetbaar	Wordt toegepast.
A.13.2	Informatietransfer					
A.13.2.1	Beleid en procedures voor informatietransfer	Formeel overdrachtsbeleid, procedures en controles moeten worden getroffen om de overdracht van informatie door middel van het gebruik van alle vormen van communicatiefaciliteiten te beschermen.	ja		3. Gedefinieerd proces	Er is een procedure waarin maatregelen opgenomen zijn om informatietransfer veilig te laten verlopen. Deze is gecommuniceerd en wordt toegepast
A.13.2.2	Overeenkomsten over informatietransfer	Overeenkomsten moeten de veilige overdracht van zakelijke informatie tussen de organisatie en externe partijen aanpakken.	ja		3. Gedefinieerd proces	Er is een procedure waarin maatregelen opgenomen zijn om informatietransfer veilig te laten verlopen. Deze is gecommuniceerd en wordt toegepast
A.13.2.3	Elektronische berichten	Informatie die betrokken zijn bij elektronische berichtenuitwisseling moet op passende wijze worden beschermd.	ja		4. Beheerd en meetbaar	Wordt toegepast.
A.13.2.4	Vertrouwelijkheid of geheimhoudingsverklaring	Vereisten voor de vertrouwelijkheid of non-disclosure overeenkomsten als gevolg van de behoeften van de organisatie voor de bescherming van gegevens worden geïdentificeerd, regelmatig herzien en gedocumenteerd.	ja		3. Gedefinieerd proces	De procedure is beschreven en wordt toegepast.
A.14	Systeem verwerven, ontwikkelen en onderhouden					
A.14.1	Beveiligingseisen voor informatiesystemen					
A.14.1.1	Analyseren en specifiëren beveiligingseisen	De eisen gerelateerd aan informatiebeveiliging worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen van bestaande informatiesystemen.	ja		5. Geoptimaliseerd	Voor het ISMS is er een manual compliance check uitgevoerd alsook een stakeholdersmatrix waarbij we de beveiligingseisen geanalyseerd en gespecificeerd hebben.
A.14.1.2	Beveiligen applicaties op openbare netwerken	Informatie die d.m.v. het gebruik van toepassingen over openbare netwerken passeren, worden beschermd tegen frauduleuze activiteiten, contractgeschillen en ongeoorloofde bekendmaking en modificatie.	ja		4. Beheerd en meetbaar	De procedure is beschreven en wordt toegepast.
A.14.1.3	Bescherming applicatietransacties	Informatie m.b.t. applicatietransacties worden beschermd om onvolledige overdracht, onjuiste routering, onbevoegde berichtwijziging, ongeoorloofde openbaarmaking, onbevoegde bericht kopies of herhaling te voorkomen.	ja		4. Beheerd en meetbaar	De procedure is beschreven en wordt toegepast.
A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen					
A.14.2.1	Ontwikkelingsbeleid i.f.v. veiligheid	Regels voor de ontwikkeling van software en systemen worden vastgesteld en toegepast op de ontwikkelingen binnen de organisatie.	ja		3. Gedefinieerd proces	Alle processen binnen Trustteam onderschrijven het informatieveiligheidsbeleid waardoor nieuwe ontwikkelingen getoetst worden aan de informatieveiligheidsvereisten. Dit is ook meegenomen in de 'software' processen.
A.14.2.2	Procedures van controles op systeemverandering	Wijzigingen in systemen binnen de ontwikkelingscyclus worden gecontroleerd door het gebruik van formele procedures van controles op systeemverandering.	ja		3. Gedefinieerd proces	Het ISMS team houdt de vinger aan de pols betreffende wijzigingen en veranderingen op vlak van informatieveiligheid. Dit is ook meegenomen in de 'software' processen.
A.14.2.3	Technische beoordeling van applicaties na wijzigingen aan het operationeel platform	Wanneer operatieve platformen gewijzigd zijn, worden bedrijfskritische applicaties beoordeeld en getest om te zorgen dat er geen negatieve invloed is op de organisatorische operaties of beveiliging.	ja		3. Gedefinieerd proces	Dit is meegenomen in de 'software' processen
A.14.2.4	Beperkingen op wijzigingen in softwarepakketten	Wijzigingen aan softwarepakketten worden ontmoedigd, beperkt tot de noodzakelijke veranderingen en alle veranderingen zullen streng worden gecontroleerd.	ja		3. Gedefinieerd proces	Dit is meegenomen in de 'software' processen
A.14.2.5	Principes voor het ontwikkelen van beveiligde systemen	Principes voor het ontwikkelen van beveiligde systemen worden opgesteld, gedocumenteerd, onderhouden en toegepast op alle informatie systeem implementatie inspanningen.	ja		3. Gedefinieerd proces	Dit is meegenomen in de 'software' processen
A.14.2.6	Beveiligde ontwikkelomgeving	Organisaties stellen een adequaat beschermde ontwikkelomgeving voor systeemontwikkeling op en leveren integratie-inspanningen die de hele ontwikkelingscyclus van het systeem dekken.	ja		3. Gedefinieerd proces	Dit is meegenomen in de 'software' processen

A.14.2.7	Uitbestede softwareontwikkeling	De organisatie moet toezicht en controle houden op de activiteit van uitbestede systeemontwikkelingen.	ja		3. Gedefinieerd proces	Dit is meegenomen in de 'software' processen
A.14.2.8	Testen van de systeembeveiliging tijdens ontwikkeling	Het testen van de beveiligingsfunctionaliteit wordt uitgevoerd tijdens de ontwikkeling.	ja		3. Gedefinieerd proces	Dit is meegenomen in de 'software' processen
A.14.2.9	Systeemacceptatietests	Acceptatie testprogramma's en de bijbehorende criteria worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies.	ja		3. Gedefinieerd proces	Dit is meegenomen in de 'software' processen
A.14.3	Testgegevens					
A.14.3.1	Bescherming van testgegevens	Test gegevens zullen zorgvuldig worden gekozen, beschermd en gecontroleerd.	ja		3. Gedefinieerd proces	Dit is meegenomen in de 'software' processen
A.15	Leveranciersrelaties					
A.15.1	Informatieveiligheid in leveranciersrelaties					
A.15.1.1	Informatieveiligheidsbeleid in leveranciersrelaties	Informatiebeveiligingsvereisten voor het verminderen van de risico's die samenhangen met de toegang voor leverancier tot de bedrijfsmiddelen moet met de leverancier worden overeengekomen en gedocumenteerd.	ja		3. Gedefinieerd proces	Het informatieveiligheidsbeleid neemt ook leveranciers op. De verwerkersoveneenkomst moet worden ondertekend door alle leveranciers die gegevens van Trustteam verwerken Elke leverancier wordt jaarlijks beoordeeld op de voorgelegde eisen.
A.15.1.2	Veiligheid opnemen in leveranciersovereenkomst	Informatiebeveiligingsvereisten voor het verminderen van de risico's die samenhangen met de toegang voor leverancier tot de bedrijfsmiddelen moet met de leverancier worden overeengekomen en gedocumenteerd.	ja		3. Gedefinieerd proces	Er wordt aantoonbaarheid van het voldoen aan de eisen verwacht van de leveranciers door middel van het ondertekenen van de verwerkersovereenkomst of door het voorleggen van een certificaat ISO 27001.
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Alle relevante eisen omtrent informatiebeveiliging worden vastgesteld en overeengekomen met elke leverancier die gegevens van de organisatie kan openen, verwerken, opslaan en communiceren of die IT-infrastructuur componenten aanbiedt.	ja		3. Gedefinieerd proces	De eisen omtrent informatieveiligheid worden vastgelegd en ondertekend in de verwerkersovereenkomst.
A.15.2	Beheer dienstverlening van leveranciers					
A.15.2.1	Opvolgen en beoordelen van leveranciersdiensten	Organisaties zullen regelmatig toezicht, evaluatie en leveranciersaudits uitvoeren.	ja		3. Gedefinieerd proces	De leveranciersbeoordeling is opgenomen in het proces algemeen, financieel en HRM beleid.
A.15.2.2	Omgaan met veranderingen in leveranciersdiensten	Wijzigingen in de dienstverlening door leveranciers, met inbegrip van het behoud en de verbetering van het bestaande informatieveiligheidsbeleid, procedures en controles, worden beheerd, rekening houdend met het kritieke karakter van zakelijke informatie, systemen en processen omtrent de herbeoordeling van de risico's.	ja		3. Gedefinieerd proces	De leveranciersbeoordeling is opgenomen in het proces algemeen, financieel en HRM beleid.
A.16	Informatieveiligheidsincidentenbeheer					
A.16.1	Beheer van informatieveiligheidsincidenten en -verbeteringen					
A.16.1.1	Verantwoordelijkheden en procedures	Beheerstaken en procedures worden vastgesteld om een snelle, effectieve en ordelijke reactie op informatie beveiligingsincidenten te waarborgen.	ja		4. Beheerd en meetbaar	Alles wordt vastgelegd in de procedure voor incidenten en afwijkingen. Voor elk incident of afwijkingen worden er corrigerende maatregelen opgesteld. De ISMS manager volgt dit op.
A.16.1.2	Rapporteren van gebeurtenissen omtrent informatieveiligheid	Gebeurtenissen omtrent informatiebeveiliging moeten zo snel mogelijk worden gemeld door middel van een passende kanalen.	ja		4. Beheerd en meetbaar	Alles wordt vastgelegd in de procedure voor incidenten en afwijkingen. Voor elk incident of afwijkingen worden er corrigerende maatregelen opgesteld.
A.16.1.3	rapporteren van zwaktes omtrent informatieveiligheid	Werknemers en contractanten zijn verplicht om eventuele geconstateerde of vermoede tekortkomingen in het kader van informatiebeveiliging melden met behulp van de organisatie informatiesystemen en -diensten.	ja		4. Beheerd en meetbaar	Alles wordt vastgelegd in de procedure voor incidenten en afwijkingen. Voor elk incident of afwijkingen worden er corrigerende maatregelen opgesteld.
A.16.1.4	Evalueren en beslissingen nemen over gebeurtenissen omtrent informatieveiligheid	Gebeurtenissen omtrent Informatiebeveiliging worden geëvalueerd en daarna wordt beslist of ze als informatiebeveiligingsincidenten worden geclassificeerd.	ja		4. Beheerd en meetbaar	Alles wordt vastgelegd in de procedure voor incidenten en afwijkingen. Voor elk incident of afwijkingen worden er corrigerende maatregelen opgesteld.
A.16.1.5	Reactie op incidenten omtrent informatieveiligheid	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	ja		4. Beheerd en meetbaar	Alles wordt vastgelegd in de procedure voor incidenten en afwijkingen. Voor elk incident of afwijkingen worden er corrigerende maatregelen opgesteld.
A.16.1.6	Leren van incidenten omtrent informatieveiligheid	De kennis die is opgedaan met het analyseren en oplossen van informatiebeveiligingsincidenten moeten worden gebruikt om de kans op of de gevolgen van incidenten in de toekomst te verminderen.	ja		4. Beheerd en meetbaar	Alles wordt vastgelegd in de procedure voor incidenten en afwijkingen. Voor elk incident of afwijkingen worden er corrigerende maatregelen opgesteld.
A.16.1.7	Verzamelen van bewijzen	De organisatie moet procedures definiëren en toepassen voor de identificatie, inzameling, verwerving en het behoud van informatie, die als bewijs kunnen dienen.	ja		4. Beheerd en meetbaar	Alles wordt vastgelegd in de procedure voor incidenten en afwijkingen. Voor elk incident of afwijkingen worden er corrigerende maatregelen opgesteld.
A.17	Bedrijfscontinuïteitsbeheer omtrent informatieveiligheid					
A.17.1	Continuïteit in informatiebeveiliging					
A.17.1.1	Plannen van continuïteit in informatiebeveiliging	De organisatie stelt zijn eisen voor informatiebeveiliging en continuïteit van information security management in ongunstige omstandigheden, bijv. tijdens een crisis of ramp.	ja		3. Gedefinieerd proces	De procedure is beschreven en wordt toegepast.
A.17.1.2	Implementeren van continuïteit in informatiebeveiliging	De organisatie moet processen, procedures en controles vaststellen, documenteren, implementeren en onderhouden om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	ja		4. Beheerd en meetbaar	De procedure is beschreven en wordt toegepast.
A.17.1.3	Verifieer, beoordeel en evalueer continuïteit in informatieveiligheid	De organisatie dient de opstelling en de uitvoering van informatiebeveiliging continuïteitscontroles op regelmatige tijdstippen te controleren om ervoor te zorgen dat ze geldig en effectief zijn tijdens ongunstige omstandigheden.	ja		4. Beheerd en meetbaar	De procedure is beschreven en wordt toegepast.
A.17.2	Overbodigheid					

A.17.2.1	Beschikbaarheid van informatieverwerkingsfaciliteiten	Informatieverwerkingsfaciliteiten zullen met net voldoende overbodigheid worden uitgevoerd om aan de beschikbaarheidseisen te voldoen.	ja		2. Herbruikbaar maar op intuïtie	De termijnen worden bepaald in het verwerkingsregister.
A.18	Compliance					
A.18.1	Naleving legale en contractuele vereisten					
A.18.1.1	Identificatie van toepasbare wetten en contractuele verplichtingen	Alle relevante wettelijke, reglementaire, contractuele vereisten en de aanpak van de organisatie om aan deze eisen te voldoen, moeten expliciet worden geïdentificeerd, gedocumenteerd en up-to-date zijn voor elk informatiesysteem en de organisatie.	ja		4. Beheerd en meetbaar	Wordt opgevolgd.
A.18.1.2	Intellectuele eigendomsrechten	Passende procedures worden uitgevoerd om de naleving van wettelijke en contractuele vereisten met betrekking tot de intellectuele eigendomsrechten en het gebruik van gepatenteerde software producten te garanderen.	ja		4. Beheerd en meetbaar	Wordt opgevolgd.
A.18.1.3	Bescherming van archieven	De verzamelde gegevens worden beschermd tegen verlies, vernietiging, vervalsing, ongeoorloofde toegang en ongeoorloofde release, in overeenstemming met wettelijke, reglementaire, contractuele en zakelijke behoeften.	ja		4. Beheerd en meetbaar	Wordt opgevolgd.
A.18.1.4	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens moet worden verzekerd, zoals vereist in de relevante wet- en regelgeving, indien van toepassing.	ja		4. Beheerd en meetbaar	Wordt opgevolgd.
A.18.1.5	Voorschriften cryptografische controles	Cryptografische controles worden gebruikt in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	ja		4. Beheerd en meetbaar	Wordt opgevolgd.
A.18.2	Beoordelingen informatieveiligheid					
A.18.2.1	Onafhankelijke beoordeling informatieveiligheid	De aanpak van de organisatie voor het beheer van informatiebeveiliging en de uitvoering daarvan (dat wil zeggen de doelstellingen, controles, beleid, processen en procedures voor informatiebeveiliging) moet onafhankelijk en op geregelde tijdstippen worden beoordeeld of wanneer zich aanzienlijke veranderingen voordoen.	ja		3. Gedefinieerd proces	Wordt opgevolgd.
A.18.2.2	Naleving veiligheidsbeleid en -normen	Managers moeten regelmatig de naleving van informatieverwerking en procedures binnen hun gebied van verantwoordelijkheid nazien met het informatieveiligheidsbeleid, de normen en andere veiligheidseisen.	ja		4. Beheerd en meetbaar	Wordt opgevolgd.
A.18.2.3	Beoordeling technische naleving	Informatiesystemen worden regelmatig getoetst op naleving van informatiebeveiligingsbeleid van de organsatie en de normen.	ja		4. Beheerd en meetbaar	Wordt opgevolgd.