INFORMATIEBEVEILIGINGSHANDREIKING MKB PARTNERS VAN WERKORGANISATIE BUCH

Colofon

Uitgever

Team Security Werkorganisatie BUCH

Datum

December 2021

Versie

1

Documentbeheer

Functie	Actie	Datum	Versie
CISO/ISO	Opstellen Informatiebeveiligingshandreiking MKB partners van werkorganisatie BUCH	06-12-2021	1

Inhoud

1. Inleiding

Dit document is opgesteld door werkorganisatie BUCH voor leveranciers en (keten)partners waarmee zij samenwerken. Indien er voor de werkorganisatie (persoons)gegevens worden verwerkt door leveranciers, en de leverancier verwerker is, is werkorganisatie BUCH verantwoordelijk voor deze (persoons)gegevens. Er wordt dan verwacht dat een partner deugdelijk omgaat met deze (persoons)gegevens en deze partner voldoet aan de geldende wet- en regelgeving op het gebied van privacy en informatiebeveiliging. Een passende beveiliging is hier verplicht onderdeel van. Om de bedrijven handvatten te geven om een deugdelijke beveiliging van informatie aan te tonen en op een juiste manier in te richten is deze informatiebeveiligingshandreiking opgesteld.

2. Informatiebeveiliging op basis van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

Om te bepalen welke mate van beveiliging vereist is voor het verwerken van (persoons)gegevens, data en processen, moeten deze eerst geclassificeerd worden. Classificeer data, processen en technische infrastructuur door middel van een vragenlijst, waaruit blijkt welk risico men loopt bij inbreuk op een van de BIV onderwerpen. Neem hiervoor de Baselinetoets van de IBD (informatiebeveiligingsdienst) als voorbeeld. Bepaal aan de hand van beveiligingsniveaus welke beveiligingsmaatregelen genomen moeten worden voor de verwerking van (persoons)gegevens, informatie en processen binnen de organisatie. In bijlage 1 is een overzicht te zien van alle maatregelen voor basisbeveiligingsniveau 1 en 2. Wanneer data of processen door de Baselinetoets geclassificeerd worden met basisbeveiligingsniveau 2, moeten zowel alle maatregelen van basisbeveiligingsniveau 1 als basisbeveiligingsniveau 2 genomen worden.

3. Continu verbeteren van informatiebeveiliging op basis van Plan Do Check Act (Demming PDCA-Cyclus).

Om in controle te kunnen zijn van het proces van informatiebeveiliging en om de organisatie te verzekeren van een continu proces van verbetering is de PDCA cyclus van Demming een waardevolle tool. In dit proces worden de acties en implementaties op het gebied van informatiebeveiliging gepland en gecontroleerd uitgevoerd. Laat de acties en implementaties toetsten door gebruik te maken van een gestandaardiseerde checklist die getoetst wordt door een derde partij (bijvoorbeeld door een accountant gelijk met de jaarlijkse controle op de boekhouding). Op- en aanmerkingen in de toetsing worden dan gepland voor de volgende periode waarmee de cyclus opnieuw start en waarmee het proces van continu verbeteren aantoonbaar kan worden gemaakt.

4. Vier lagen van informatiebeveiliging

4.1. Beleid

Er dient een informatiebeveiligingsbeleid te zijn dat is goedgekeurd door de directie. Dit beleid is gecommuniceerd binnen de organisatie en met de relevante externen. Het beleid moet actueel en relevant zijn. Het beleid moet toezien op beveiliging van persoonlijke IT-middelen (ook thuiswerken). Leveranciersmanagement moet een integraal onderdeel zijn van het informatiebeveiligingsbeleid. Informatiebeveiliging dient een verplicht onderdeel te zijn van projectbeheer, ongeacht het soort project. Toegang dient geregeld te zijn in een duidelijk proces waarin naar voren komt dat authenticatie en rechten worden verleend op basis van functierollen. Idealiter hangende aan een in- en uitdienstprocedure. Wijzigingen (mutaties) dienen regelmatig gerapporteerd te worden aan het management. Het proces van bewaren en uitgifte van autorisatiesleutels (wachtwoorden) en elektronische sleutels (SSL-certificaten VPN-sleutels) moeten in een beleid gevat zijn en controleerbaar zijn.

In het informatiebeveiligingsbeleid moet aandacht zijn voor het kundig en ethisch behandelen van kwetsbare gegevens (bewustwordingsprogramma, verwerking van data, login, wachtwoorden, mobiele apparatuur in onbeschermde omgevingen). Het informatiebeveiligingsbeleid dient toe te zien op het gebruik van analoge en digitale informatie buiten de beveiligingsmaatregelen en buiten het terrein van de organisatie (onderweg of thuis). Er moeten beleidsregels zijn ten aanzien van informatiekoppelingen en dataoverdracht (intern en extern). Beveiligingsincidenten moeten direct op een passende wijze worden gemeld, zowel door medewerkers als door relevante leveranciers en ketenpartners. Er moet aantoonbaar en periodiek controle zijn op de zelf opgelegde maatregelen en procedures in het beleid (PDCA-cyclus).

4.2. Processen

In het kader van informatiebeveiliging is de aanwezigheid en beschrijving van een aantal IT processen van groot belang. De toegang en autorisatie op systemen, applicaties en data waarin kwetsbare- of persoonsgegevens worden verwerkt dienen op een gecontroleerde wijze te worden verleent, middels een toegang- en autorisatieproces. Dit is bij voorkeur een rolgebaseerd proces. Dit proces is idealiter gekoppeld aan een in- en uitdienstprocedure. Incidentprocessen waarin op aantoonbare wijze IT-beveiligingsincidenten wordt bijgehouden en wijzigingsprocessen waarin op aantoonbare wijze veranderingen gecontroleerd worden uitgevoerd zijn van essentieel belang. Daarnaast zijn op operationeel vlak vastgelegde beheerprocessen zoals wachtwoord-, back-up-, restore-, patch-, encryptie- en systemmanagement een vereiste. Veilige en vastgelegde informatie met betrekking tot monitoring, logging, en rapportages zijn onmisbaar voor systeembeheer om controle uit te oefenen op de genoemde processen.

4.3. IT Hardware

Indien de eigen organisatie niet beschikt over relevant en actueel geschoold IT-personeel, dan selecteert de organisatie een leverancier die IT-hardware levert waarvan zij officieel dealer is. Deze partij wordt als eerste ingelicht over mogelijke kwetsbaarheden in IT-producten door de fabrikanten waarvan zij officieel leverancier zijn. Het personeel van deze organisaties zijn door de fabrikanten relevant en actueel geschoold. Bij installatie en configuratie van IT-producten zullen deze leveranciers in staat zijn garant te staan voor de geleverde producten en diensten. Zorg bij de installatie van bekabeling, firewalls, switches, WIFI-Accesspoints, 3/4/5G apparatuur altijd voor installatiecertificaten van de leverancier. Op deze manier is aantoonbaar dat de apparatuur deugdelijk is geïnstalleerd volgens fabrieksstandaarden en de laatste beveiligingsnormen.

4.4. IT Software

Indien de eigen organisatie niet beschikt over relevant en actueel geschoold IT-personeel, dan selecteert de organisatie een leverancier die IT-hardware levert waarvan zij officieel dealer is. De organisatie selecteert waar mogelijk software op basis van online diensten, oftewel Software As A Service (SaaS), bij ISO 27001 gecertificeerde partijen. Indien de organisatie niet beschik over geschoold IT–personeel, dan selecteert de organisatie voor werkpleksoftware ook een online werkplek of Cloud-werkplek oplossing. Selecteer voor de online werkplek of de Cloud werkplek bij voorkeur leveranciers die beschikken over een ISO27001-certificaat. Deze leveranciers zijn aantoonbaar “in controll” voor wat betreft ITIL en autorisatie- en authenticatie processen voor de door hun aangeboden platvormen. Organisaties die niet beschikken over relevant en actueel geschoold IT-personeel vormen te allen tijde een onaanvaardbaar risico. IT-infrastructuur en of software oplossingen in een ongecontroleerde omgeving zonder gecertificeerd beheer of alleen onder ad-hoc beheer vormen te allen tijde een onaanvaardbaar risico.

Bijlage 1: Informatiebeveiligingsmaatregelen basisbeveiligingsniveau 1 en 2

In onderstaande tabel zijn alle maatregelen uitgewerkt die geïmplementeerd dienen te worden bij de verwerking van (persoons)gegevens, data, processen en/of informatiesystemen met het basisbeveiligingsniveau 1 of 2. Wanneer data of processen door de Baselinetoets geclassificeerd worden met basisbeveiligingsniveau 2, moeten zowel alle maatregelen van basisbeveiligingsniveau 1 als basisbeveiligingsniveau 2 genomen worden. In de blauwe kolommen zijn alle maatregelen voor basisbeveiligingsniveau 1 weergegeven. Maatregelen voor basisbeveiligingsniveau 2 zijn in de groene kolommen weergegeven.

Maatregelen Basisbeveiligingsniveau 1	**Maatregelen Basisbeveiligingsniveau 2**
Onderwerp	**Controls**
1. **Informatiebeveiligingsbeleid**	
1.1	- **Beleidsregels voor informatiebeveiliging:** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. - **Beoordeling van het informatiebeveiligingsbeleid:** Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
2. **Organiseren van informatiebeveiligingsbeleid**	
2.1 Interne organisatie	- **Rollen en verantwoordelijkheden bij informatiebeveiliging** Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. - **Scheiding van taken** Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
2.1 Interne organisatie	- **Contact met overheidsinstanties** Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden. - **Informatiebeveiliging in projectbeheer** Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.
2.2 Mobiele apparatuur en telewerken	- **Beleid voor mobiele apparatuur** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.
2.2 Mobiele apparatuur en telewerken	- **Telewerken** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.
3. **Veilig personeel**	
3.1 Voorafgaand aan dienstverband	- **Screening** Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en

	behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn. - **Arbeidsvoorwaarden** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.
3.2 Tijdens dienstverband en na beëindigen en wijzigen dienstverband	- **Directieverantwoordelijkheden** De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. - **Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. - **Disciplinaire procedure** Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.
4. **Beheer van bedrijfsmiddelen**	
4.1 Verantwoordelijkheid voor bedrijfsmiddelen	- **Inventariseren van bedrijfsmiddelen** Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden. - **Eigendom van bedrijfsmiddelen** Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben. - **Aanvaardbaar gebruik van bedrijfsmiddelen** Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd. - **Teruggeven van bedrijfsmiddelen** 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 terug te geven.
4.2 Informatieclassificatie	- **Classificatie van informatie** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. - **Informatie labelen** Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. - **Behandelen van bedrijfsmiddelen** Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met

	het informatieclassificatieschema dat is vastgesteld door de organisatie.
4.3 Behandelen van media	- **Beheer van verwijderbare media** Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.
4.3 Behandelen van media	- **Verwijderen van media** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures. - **Media fysiek overdragen** Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.
5. **Toegangsbeveiliging**	
5.1 Bedrijfseisen voor toegangsbeveiliging	- **Beleid voor toegangsbeveiliging** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. - **Toegang tot netwerken en netwerkdiensten** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
5.2 Beheer van toegangsrechten van gebruikers	- **Registratie en afmelden van gebruikers** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. - **Gebruikers toegang verlenen** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. - **Beheren van speciale toegangsrechten** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst. - **Beheer van geheime authenticatie-informatie van gebruikers** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. - **Beoordeling van toegangsrechten van gebruikers** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. - **Toegangsrechten intrekken of aanpassen** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
5.3 Verantwoordelijkheden van gebruikers	- **Geheime authenticatie-informatie gebruiken** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.
5.4 Toegangsbeveiliging van systeem en toepassing	- **Beperking toegang tot informatie** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. - **Beveiligde inlogprocedures**

	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure. - **Systeem voor wachtwoordbeheer** Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen. - **Speciale systeemhulpmiddelen gebruiken** Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd. - **Toegangsbeveiliging op programmabroncode** Toegang tot de programmabroncode behoort te worden beperkt
6. **Cryptografie**	
6.1 Cryptografisch sleutelbeheer	- **Sleutelbeheer** Er dient beleid te worden ontwikkeld en geïmplementeerd met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels welke de gehele levensduur van de cryptografische sleutels omvat.
6.1 Cryptografisch sleutelbeheer	- **Beleid inzake het gebruik van cryptografische beheersmaatregelen** Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
7. **Fysieke beveiliging en beveiliging van de omgeving**	
7.1 Fysieke beveiligingszone	- **Fysieke beveiligingszone** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten. - **Fysieke toegangsbeveiliging** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. - **Kantoren, ruimten en faciliteiten beveiligen** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. - **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.
7.1 Fysieke beveiligingszone	- **Werken in beveiligde gebieden** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast
7.2 Apparatuur	- **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. - **Nutsvoorzieningen** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen - **Beveiliging van bekabeling**

	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade. - **Onderhoud van apparatuur** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen. - **Verwijdering van bedrijfsmiddelen** Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring. - **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. - **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. - **Onbeheerde gebruikersapparatuur** Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is. - **'Clear desk'- en 'clear screen'-beleid** Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.
8. **Beveiliging bedrijfsvoering**	
8.1 Bedieningsprocedures en verantwoordelijkheden	- **Gedocumenteerde bedieningsprocedures** Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. - **Wijzigingsbeheer** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. - **Capaciteitsbeheer** Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen. - **Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.
8.2 Bescherming tegen malware	- **Beheersmaatregelen tegen malware** Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.
8.3 Back up	- **Back-up van informatie** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.

8.4 Verslaglegging en monitoring	- **Gebeurtenissen registreren** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. - **Beschermen van informatie in logbestanden** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. - **Logbestanden van beheerders en operators** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld. - **Kloksynchronisatie** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.
8.5 beheersing van operationele software	- **Software installeren op operationele systemen** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.
8.6 Beheersing van technische kwetsbaarheden	- **Beheer van technische kwetsbaarheden** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken. - **Beperkingen voor het installeren van software** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.
8.7 Overwegingen betreffende audits van informatiesysteme n	- **Beheersmaatregelen betreffende audits van informatiesystemen** Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren
9. **Communicatiebeveiliging**	
9.1 Beheer van netwerkbeveiliging	- **Beheersmaatregelen voor netwerken** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen. - **Beveiliging van netwerkdiensten** Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten. - **Scheiding in netwerken** Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.
9.2 Informatietransport	- **Beleid en procedures voor informatietransport** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn. - **Overeenkomsten over informatietransport**

	Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen. - **Elektronische berichten** Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd. - **Vertrouwelijkheids- of geheimhoudingsovereenkomst** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.
10. **Acquisitie, ontwikkeling en onderhoud van informatiesystemen**	
10.1 Beveiligingseisen voor informatiesysteme n	- **Analyse en specificatie van informatiebeveiligingseisen** De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen**.** - **Toepassingen op openbare netwerken beveiligen** Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging. - **Transacties van toepassingen beschermen** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.
10.2 Beveiliging in ontwikkelings- en ondersteunende processen	- **Beleid voor beveiligd ontwikkelen** Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast. - **Procedures voor wijzigingsbeheer met betrekking tot systemen** Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer. - **Principes voor engineering van beveiligde systemen** Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen. - **Beveiligde ontwikkelomgeving** Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling. - **Uitbestede softwareontwikkeling** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie. - **Testen van systeembeveiliging** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest. - **Systeemacceptatietests**

	Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
10.2 Beveiliging in ontwikkelings- en ondersteunende processen	- **Technische beoordeling van toepassingen na wijzigingen besturingsplatform** Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.
10.3 Testgegevens	- **Bescherming van testgegevens** Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.
11. **Leveranciersrelaties**	
11.1 Informatiebeveiliging in leveranciersrelaties	- **Informatiebeveiligingsbeleid voor leveranciersrelaties** Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd. - **Opnemen van beveiligingsaspecten in leveranciersovereenkomsten** Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt. - **Toeleveringsketen van informatie- en communicatietechnologie** Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.
11.2 Beheer van dienstverlening van leveranciers	- **Monitoring en beoordeling van dienstverlening van leveranciers** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.
11.2 Beheer van dienstverlening van leveranciers	- **Beheer van veranderingen in dienstverlening van leveranciers** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.
12. **Beheer van informatiebeveiliging**	
12.1 Beheer van informatiebeveiligingsincidenten en verbeteringen	- **Verantwoordelijkheden en procedures** Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen. - **Rapportage van informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. - **Rapportage van zwakke plekken in de informatiebeveiliging** Van medewerkers en contractanten die gebruikmaken van de

	informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren. - **Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten. - **Respons op informatiebeveiligingsincidenten** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
12.1 Beheer van informatiebeveiligingsincidenten en verbeteringen	- **Verzamelen van bewijsmateriaal** De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.
13. **Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**	
17.1 Informatiebeveiligingscontinuïteit	- **Informatiebeveiligingscontinuïteit plannen** De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen. - **Informatiebeveiligingscontinuïteit implementeren** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. - **Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren** De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.
17.2 Redundante componenten	- **Beschikbaarheid van informatie verwerkende faciliteiten** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.
14. **Naleving**	
14.1 Naleving wettelijke en contractuele eisen	- **Vaststellen van toepasselijke wetgeving en contractuele eisen** Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden. - **Privacy en bescherming van persoonsgegevens** Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. - **Voorschriften voor het gebruik van cryptografische beheersmaatregelen**

	Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.
14.1 Naleving wettelijke en contractuele eisen	- **Beschermen van registraties** Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.
14.2 Informatiebeveiligingsbeoordelingen	- **Onafhankelijke beoordeling van informatiebeveiliging** De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld. - **Naleving van beveiligingsbeleid en -normen** De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. - **Beoordeling van technische naleving** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging