Technisch beveiligingsbeleid
2025-2029

Versieblad

Versiedatum:	28-05-2025
Goedgekeurd door:	
Classificatie:	Intern

Documenttitel	Technisch beveiligingsbeleid
Versie	1
Datum	
Status	Definitief
Classificatie	Intern document
Proceseigenaar	Stan Peters / Anthony Verwijst
Documentbeheerder	Stan Peters / Anthony Verwijst

Wijzigingshistorie			
Versie	**Datum**	**Gewijzigd door**	**Beschrijving wijziging**

Inhoud

1. Over dit beleidsdocument

1.1 Doel, toepassingsgebied en gebruikers

Dit technisch beleid is gericht op het definiëren van het doel, de richting, de principes en de basisregels voor Informatiebeveiliging binnen de technische omgevingen van de organisatie. Naast dit technisch beleid heeft de organisatie ook een informatiebeveiligings- en privacybeleid opgesteld voor alle medewerkers.
Dit technisch beleid is van toepassing op het toepassingsgebied (de scope) van het Managementsysteem voor Informatiebeveiliging (ISMS), zoals bepaald in informatiebeveiligings- en privacybeleid en het strategie document van de organisatie.
Gebruikers van dit document zijn alle technische werknemers van de organisatie, als ook de relevante externe partijen.

1.2 Gerefereerde documenten

ISO/IEC 27001 norm, clausule 5.2
ISMS-documentatie (IBP/AVG beleidsplan, Strategiebeleid)
Informatiebeveiligings- en privacybeleid

1.3 Geldigheid en documentbeheer

Dit document is geldig vanaf de definitieve versie datum.
De eigenaren van dit document zijn de Privacy en Security Officer en het hoofd ICT van de organisatie. Deze dienen het document te minstens één keer per jaar te beoordelen en indien nodig bij te werken.
Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dient het aantal incidenten in verband met het niet volgen van dit beleid, en het aantal incidenten in verband met het ontbreken van beleid, in ogenschouw te worden genomen.

1.4 Goedkeuring van dit het beleid

Hierbij bevestigt het CvB (Commissie van Bestuur van Optimus) de geldigheid van dit beleid.

[Naam CvB]

[Plaats, datum]

2. Beveiliging van informatie

Basisterminologie Informatiebeveiliging

Informatiebeveiliging - behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie
Vertrouwelijkheid - kenmerk van de informatie dat deze alleen beschikbaar is voor bevoegde personen of systemen.
Integriteit – kenmerk van de informatie dat de informatie alleen op voorgeschreven wijze kan worden gewijzigd door bevoegde personen of systemen.
Beschikbaarheid – kenmerk van de informatie dat de informatie beschikbaar is voor bevoegde personen als de informatie nodig is.
Veerkracht - het vermogen van de stichting 's IT-infrastructuur om snel te reageren en te herstellen van verstoringen die invloed hebben op de digitale functies van het bestuurskantoor en de basisscholen.
Managementsysteem voor Informatiebeveiliging (ISMS) – deel van het gehele managementproces dat zorg draagt voor de planning, implementatie, het onderhoud, de beoordeling, en het verbeteren van de informatiebeveiliging.
Informatiesystemen - Bevatten alle servers (geen servers) en clients, netwerkinfrastructuur, systeem en ondersteuning bij programmeren, gegevens en andere computer subsystemen en onderdelen die eigendom zijn van of worden gebruikt door de organisatie of die onder de verantwoordelijkheid van de organisatie vallen. Het gebruik van informatiesystemen bevat alle interne en externe diensten, zoals internettoegang, e-mail, enz.
Bedrijfsmiddelen - in de context van dit beleid wordt de term bedrijfsmiddelen toegepast op informatie systemen en andere informatie/apparatuur, inclusief papieren documenten, mobiele telefoons, draagbare computers, media voor gegevensopslag, enz.
Domeinbeheerder: Leidinggevende van een domein. Bijvoorbeeld een schooldirecteur, hoofd HRM, hoofd beheer of hoofd ICT.

3. Betrokkenheid van het management bij dit beleid

ISO: De directie moet leiderschap en betrokkenheid tonen met betrekking tot het managementsysteem voor informatiebeveiliging door te bewerkstelligen dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en aansluiten bij de strategische richting van de organisatie.

3.1 Ondersteuning en uitvoering (ISO27001 – A5.1.1)

Het College van Bestuur verklaart dat het alle fasen van de implementatie van het Information Security Management System (ISMS) en de voortdurende verbetering ervan zal ondersteunen met passende middelen, zodat alle doelen en doelstellingen van dit beleid worden bereikt, evenals aan alle geïdentificeerde eisen wordt voldaan.

Het College van Bestuur ziet het als zijn taak ervoor te zorgen dat alle personen die een technische rol hebben in het ISMS, op de hoogte zijn van dit beleid. Daarom zal het College van Bestuur ervoor zorgen dat dit beleid wordt gepubliceerd voor alle relevante medewerkers en relevante externe partijen.

De Privacy en Security Officer, samen met het hoofd ICT, zal de opvolging en effectiviteit van dit beleid evalueren en rapporteren aan het College van Bestuur.

3.2 Eisen ten aanzien van dit beleid (ISO27001 – A7.2.1)

Het College van Bestuur verlangt van alle (technische) werknemers en relevante externe partijen die betrokken zijn bij het Information Security Management System (ISMS), dat zij beveiligingsmaatregelen toepassen in overeenstemming met het vastgestelde beleid en de vastgestelde procedures van de organisatie.

3.3 Naleving van informatie-beveiligingsbeleid en normen (ISO27001 – A18.2.2)

Domeinbeheerders dienen ervoor te zorgen dat alle beveiligingsprocedures die onder hun verantwoordelijkheid vallen, correct worden uitgevoerd om te voldoen aan het beveiligingsbeleid en de -normen.

3.4 Opleiding en training (ISO27001 – A7.2.2)

Het College van Bestuur ziet het als zijn verantwoordelijkheid ervoor te zorgen dat werknemers van de organisatie, en indien van toepassing, ingehuurd personeel en externe gebruikers, geschikte training en regelmatige bijscholing ontvangen met betrekking tot het beleid en de procedures van de organisatie die relevant zijn voor hun functie.

3.5 Disciplinair proces (ISO27001 – A7.2.3)

Naleving betekent dat we dagelijks toezicht houden op de naleving van ons beleid en onze richtlijnen. Leidinggevenden en proceseigenaren spelen hierbij een belangrijke rol door hun medewerkers aan te spreken op eventuele tekortkomingen. We besteden actief aandacht aan Informatiebeveiliging en privacy (IBP) via verschillende methoden, zoals bij aanstelling, tijdens functioneringsgesprekken, met behulp van een organisatiebrede gedragscode, en via periodieke bewustwordingscampagnes. De Functionaris voor Gegevensbescherming (FG) speelt een cruciale rol in het toezicht op de naleving van de AVG en heeft toegang tot de voortgang van het IBP-beleid.
Als de naleving van dit beleid ernstig tekortschiet, kan Stichting Optimus Onderwijs passende sancties opleggen aan de verantwoordelijke medewerkers binnen de kaders van de CAO en de wettelijke mogelijkheden.

4. Beleid voor Toegangsbeveiliging (A.9)

Toegangsbeveiliging heeft tot doel ervoor te zorgen dat alleen gebruikers die daartoe gerechtigd zijn toegang krijgen tot voorzieningen en gegevens, terwijl anderen de toegang wordt geweigerd. Het hoofddoel is om ervoor te zorgen dat het lezen, toevoegen, wijzigen en verwijderen van gegevens en programma's alleen kan worden uitgevoerd door geautoriseerde gebruikers en onder gecontroleerde omstandigheden.

Toegangsbeveiliging omvat alle aspecten van informatievoorziening, inclusief computers, netwerken, werkstations, systeem- en toepassingssoftware, en gegevens.

4.1 Bedrijfseisen voor toegangsbeveiliging (A9.1)

4.1.1 Algemeen (ISO27001-A9.1.1)

ISO: Er moet toegangsbeleid worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.

Het verlenen van toegang wordt geleid door de autorisatiematrix van de organisatie, waarin de rechten (fysiek en logisch) per rol zijn vastgelegd. In situaties waarin een medewerker meerdere rollen heeft, kunnen conflicterende rechten ontstaan. In dat geval gelden de rechten die aan de hoogste rol zijn toegekend als leidend. Het toegangsbeleid wordt hieronder verder toegelicht.

4.1.2 Functiescheiding (ISO27001-A6.1.2)

ISO: Taken en verantwoordelijkheidsgebieden moeten worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

Functiescheiding is een manier om het risico van onopzettelijk of opzettelijk misbruik van systemen te verminderen. Let erop dat geen enkele persoon toegang kan krijgen tot bedrijfsmiddelen of ze kan wijzigen of gebruiken zonder autorisatie of detectie. Zorg ervoor dat het initiëren van een activiteit gescheiden is van de autorisatie ervan en denk bij het ontwerpen van maatregelen ook aan mogelijke samenspanning.

Let op de scheiding tussen IT-functies en gebruikersfuncties en tussen applicatie-ontwikkelfuncties en beheersfuncties.
Waar functiescheiding moeilijk kan worden toegepast, zijn andere beheersmaatregelen zoals het controleren van activiteiten, 'audit trails' en supervisie door het CvB te overwegen. Het is belangrijk dat de beveiligingsaudit onafhankelijk worden uitgevoerd door de Privacy en Security Officer. Deze behoort periodiek een controle uit te voeren en de resultaten te rapporteren aan het CvB.

4.1.3 Toegang tot netwerken en netwerkdiensten (ISO27001-A9.1.2)

ISO: Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

Ongeautoriseerde en onvoldoende beveiligde verbindingen met netwerkdiensten kunnen de gehele organisatie schaden. Deze beheersmaatregel is vooral van belang voor netwerkverbindingen naar gevoelige of kritische bedrijfstoepassingen, of naar gebruikers op locaties met een verhoogd risico, bijvoorbeeld openbare of externe locaties die buiten de invloed van het beveiligingsbeheer en de beheersmaatregelen van de organisatie vallen.

- Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn (Functiescheiding).
- Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten.

4.2 Beheer van toegangsrechten van gebruikers (A9.2)

4.2.1 Registratie en uitschrijving van gebruikers (ISO27001-A9.2.1)

ISO: Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd en gebruikt om toewijzing van toegangsrechten mogelijk te maken.

Voor de inrichting hiervan gelden de volgende regels:

a. Medewerkers en leerlingen behoren vooraf te worden geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden (verantwoordelijkheid HRM als het is geautomatiseerd).
b. Indien van toepassing behoren authenticatiegegevens te worden bijgehouden in één passwordkluis zodat consistentie is gegarandeerd.
c. Op basis van een risicoafweging behoort te worden bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.

De procedure voor registratie en afmelden van gebruikers moet omvatten:

f. gebruik van unieke gebruikersidentificaties (ID) zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun handelingen; het gebruik van groepsidentificatie is alleen te overwegen als dat noodzakelijk is om bedrijfs- of operationele redenen en vraagt formele goedkeuring;
g. controleren dat de gebruiker door de systeemverantwoordelijke is geautoriseerd voor het gebruik van het informatiesysteem of de informatiedienst; afzonderlijke goedkeuring van het CvB met betrekking tot toegangsrechten kan ook terecht zijn;
h. periodieke controle op en verwijderen of blokkeren van overtollige gebruikers-ID's en –accounts. Resultaten behoren te worden gepresenteerd aan het CvB;
i. waarborgen dat overtollige gebruikers-ID's niet aan andere gebruikers worden uitgegeven.

4.2.2 Gebruikers toegang verlenen (ISO27001-A9.2.2)

ISO: Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

De procedure voor het verlenen van toegang behoort te omvatten:

a. controleren dat het toegewezen toegangsniveau geschikt is voor de bedrijfstoepassing en consistent is met het beveiligingsbeleid van de organisatie, bijvoorbeeld dat de functiescheiding niet in gevaar wordt gebracht;
b. gebruikers een bevestiging van hun toegangsrechten geven;
c. gebruikers verplichten een verklaring te ondertekenen waarin ze aangeven de voorwaarden voor de toegang te begrijpen;
d. waarborgen dat dienstverlenende bedrijven geen toegang verlenen totdat de autorisatieprocedures zijn voltooid;
e. een formele registratie bijhouden van alle personen die zijn geregistreerd;
f. onmiddellijk intrekken of blokkeren van toegangsrechten van gebruikers die van functie of rol zijn veranderd of de organisatie hebben verlaten;

4.2.3 Beheren van speciale toegangsrechten (ISO27001-A9.2.3)

ISO: Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.

Het onjuiste gebruik van speciale systeembeheerbevoegdheden, die elke voorziening of eigenschap van een informatiesysteem mogelijk maken waarmee de gebruiker de systeem- of toepassingsbeheersmaatregelen kan omzeilen, kan een belangrijke factor zijn die bijdraagt aan weigeringen van of veiligheidslekken in systemen.
Om informatiesystemen met meerdere gebruikers te beschermen tegen ongeautoriseerde toegang, is het raadzaam om een formeel autorisatieproces vast te stellen voor de toewijzing van speciale bevoegdheden.

Enkele richtlijnen hiervoor zijn:

a. Definieer speciale bevoegdheden voor elke systeemcomponent, zoals een besturingssysteem, databasesysteem en elke toepassing, en wijs deze toe aan specifieke gebruikers.
b. Wijzig wachtwoorden die door software- of hardware producenten zijn gemaakt tijdens de initiële installatie.
c. Wijs gebruikers alleen speciale bevoegdheden toe die strikt noodzakelijk zijn voor hun functie ('need-to-use') en alleen voor de duur van de gebeurtenis ('time to know'), in overeenstemming met het beleid voor logische toegangsbeveiliging.
d. Gebruik een autorisatieproces en registreer alle toegewezen speciale bevoegdheden; verleen geen bevoegdheden voordat dit autorisatieproces is voltooid.
e. Stimuleer de ontwikkeling en het gebruik van systeemroutines die het toekennen van speciale bevoegdheden aan gebruikers minimaliseren.
f. Moedig de ontwikkeling en het gebruik van software aan die de noodzaak voor het gebruik van speciale bevoegdheden minimaliseert.
g. Ken speciale bevoegdheden toe aan een ander gebruikers-ID dan degene die normaal wordt gebruikt.
h. Het naleven van deze richtlijnen kan helpen bij het beheren van speciale bevoegdheden en het verminderen van potentiële beveiligingsrisico's in informatiesystemen.

4.2.4 Beheer van geheime authenticatie-informatie van gebruikers (ISO27001-A9.2.4)

ISO: Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.

Wanneer gebruikerswachtwoorden worden toegewezen, dan dienen de volgende regels in acht te worden genomen:

a. Indien de gebruiker om een nieuw wachtwoord verzoekt, dan dient het wachtwoordenbeheersysteem de identiteit van de gebruiker te bepalen door [self service password reset in samenwerking met de Microsoft authenticator app].
b. De gebruiker dient de ontvangst van het wachtwoord te bevestigen door [het tijdelijk wachtwoord te wijzigen bij eerste inlog].
c. Gebruikers moeten het tijdelijke wachtwoorden van de eerste login op het systeem wijzigen.
d. Wachtwoorden behoren nooit te verlopen, dit is volgens de nieuwe standaard van Microsoft. Om de 360 dagen behoort de authenticator te worden geverifieerd.
e. Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt bijvoorbeeld de hashwaarde van het wachtwoord gecombineerd met een salt (statische willekeurige string) opgeslagen.
f. Gebruikers-gegenereerde wachtwoorden mogen door geen enkel kanaal worden verspreid (mondeling, geschreven of elektronische verspreiding, enz.)

g. Wachtwoorden moeten worden veranderd als er indicaties zijn dat de wachtwoorden of het systeem is gecompromitteerd - in dat geval dient een beveiligingsincident te worden gerapporteerd.

4.2.5 Beoordeling van toegangsrechten van gebruikers (ISO27001-A9.2.5)

ISO: Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.
Periodiek behoren de toegangsrechten van medewerkers te worden gecontroleerd. Als methode voor de beoordeling moet een steekproef genomen door de beheerder(s) van de toegangsrechten.

Het CvB kan ervoor kiezen om een uitgebreide interne controle te laten uitvoeren. De toezichtverantwoordelijke kan deze uit laten voeren door de interne accountantsdienst of een externe partij. Deze interne controle wordt niet door Systeem- en Domeineigenaren uitgevoerd om zoveel mogelijk beïnvloeding van het resultaat te beperken.

4.2.6 Toegangsrechten intrekken of aanpassen (ISO27001-A9.2.6)

ISO: 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.

a. Voor medewerkers is in het arbeidscontract vastgelegd welke verplichtingen ook na beëindiging van het dienstverband of bij functiewijziging nog van kracht blijven en voor hoe lang. Ook voor ingehuurd personeel (zowel in dienst van een derde bedrijf als individueel) is dit contractueel vastgelegd. Indien nodig wordt een geheimhoudingsverklaring ondertekend.
b. Het CvB heeft een procedure vastgesteld voor beëindiging van dienstverband, contract of overeenkomst waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten, innemen van bedrijfsmiddelen en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.
c. Het CvB heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.

4.3 Toegangsbeveiliging van systeem en toepassingen (A9.4)

4.3.1 Beperking toegang tot informatie (ISO27001-A9.4.1)

ISO: Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.

a. Toegang aan interne gebruikers tot informatie moet worden verstrekt op basis van de autorisatiematrix die door de proces-eigenaar en de applicatiebeheerder worden bijgehouden. In deze autorisatiematrix zijn mensen gekoppeld aan rollen, en zijn er rechten gekoppeld aan elke rol. Op deze wijze kan voor elke medewerker bepaald worden welke rechten er moeten worden ingesteld.
b. In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
c. Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
d. Bij extern gebruik vanuit een niet-vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.

e. Een beheerder gebruikt two-factor authenticatie voor het beheer van kritische apparaten. B.v. een sleutel tot beveiligde ruimte en een password of een token en een password.

4.3.2 Beveiligde inlogprocedures (ISO27001-A9.4.2)

ISO: Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.

a. Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.
b. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
c. Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
d. Nadat voor een gebruikersnaam 10 keer een foutief wachtwoord gegeven is, wordt het account minimaal 24 uur geblokkeerd. Indien er geen lockout periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.

4.3.3 Systeem voor wachtwoordenbeheer (ISO27001-A9.4.3)

ISO: Systemen voor wachtwoordbeheer moeten interactief zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

a. Wachtwoorden hebben een geldigheidsduur (zoals bij hoofdstuk Beheer van geheime authenticatie-informatie van gebruikers ISO27001-A.9.2.4 beschreven), daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
b. Systemen voor wachtwoordbeheer moeten automatisch controleren op goed gebruik van wachtwoorden (o.a. voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van het initieel wachtwoord).
c. indien een gebruiker een onjuist wachtwoord voor tien opeenvolgende keren invoert, dan dient het systeem het gebruikersaccount in kwestie te blokkeren.

Ten aanzien van de kwaliteit van (tijdelijke) wachtwoorden dient indien mogelijk het systeem af te dwingen dat gebruikers wachtwoorden kiezen die:

1. tenminste twaalf tekens gebruiken
2. tenminste één numeriek teken gebruiken
3. tenminste één hoofdletter en tenminste een kleine letter gebruiken
4. tenminste één special teken gebruiken
5. geen woord uit het woordenboek zijn , geen dialect of jargon woord van elke taal, evenmin een of meer van deze woorden achterstevoren geschreven
6. niet zijn gebaseerd op privégegevens (bijv. geboortedatum, adres, naam familielid, enz.)
7. de laatste drie keren niet zijn gebruikt

4.3.4 Speciale systeemhulpmiddelen gebruiken (ISO27001-A9.4.4)

Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.

5. Cryptografie (A.10)

Het beheer van cryptografische sleutels is van essentieel belang voor het effectieve gebruik van cryptografische technieken. ISO/IEC 11770 biedt aanvullende richtlijnen voor sleutelbeheer. Er zijn twee typen cryptografische technieken:

a. **Geheime sleuteltechnieken**: Hierbij gebruiken twee of meer partijen dezelfde sleutel voor zowel het versleutelen als het ontcijferen van gegevens. Deze sleutel moet geheim worden gehouden, omdat iedereen die toegang heeft tot de sleutel in staat is alle informatie die met deze sleutel is versleuteld te ontcijferen, of ongeautoriseerde gegevens te versleutelen met gebruik van de sleutel.
b. **Openbare sleuteltechnieken:** Elke gebruiker beschikt over een sleutelpaar, bestaande uit een openbare sleutel (die aan iedereen bekend kan worden gemaakt) en een persoonlijke sleutel (die geheim moet worden gehouden). Openbare sleuteltechnieken kunnen worden gebruikt voor encryptie en het maken van elektronische handtekeningen. Het risico van vervalsing van een elektronische handtekening wordt tegengegaan door het gebruik van een certificaat voor een openbare sleutel.

Cryptografische technieken kunnen ook worden ingezet voor het beschermen van cryptografische sleutels. Het kan nuttig zijn procedures op te stellen voor het omgaan met wettelijke verzoeken voor toegang tot cryptografische sleutels; bijvoorbeeld wanneer versleutelde informatie in ontcijferde vorm beschikbaar moet worden gesteld als bewijs in een rechtszaak.

5.1 Cryptografische beheersmaatregelen (A10.1)

5.1.1 Beleid voor het gebruik van cryptografische beheersmaatregelen (ISO27001-A10.1.1)

ISO: Er moet beleid worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

[Let op: in het beleid dat hier moet komen te staan, moet de nadruk liggen op de vraag welke DATA (classificatie) versleuteld moet zijn, niet zozeer op welke apparatuur.]

5.1.2 Sleutelbeheer (ISO27001-A10.1.2)

ISO: Er moet sleutelbeheer zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

a. Bescherm alle cryptografische sleutels tegen wijziging, verlies en vernietiging. Bescherm geheime en persoonlijke sleutels bovendien tegen onbevoegde openbaarmaking. Kies voor fysieke bescherming voor apparatuur die wordt gebruikt voor het genereren, opslaan en archiveren van sleutels.

b. Stel, om de kans te verminderen dat sleutels worden gecompromitteerd, vaste data vast voor activering en de-activering van sleutels, zodat de sleutels slechts gedurende een beperkte periode kunnen worden gebruikt. Laat deze periode afhangen van de omstandigheden waaronder de cryptografische beheersmaatregel wordt gebruikt en van het ingeschatte risico.

c. Besteed naast het zorgvuldig beheren van geheime en persoonlijke sleutels, ook aandacht aan de authenticiteit van openbare sleutels. Dit authenticatieproces kan

worden uitgevoerd met behulp van certificaten voor openbare sleutels die gewoonlijk worden uitgegeven door een erkende certificerende instantie die beschikt over geschikte beheersmaatregelen en procedures om de vereiste mate van betrouwbaarheid te kunnen leveren.

Baseer het sleutelbeheersysteem op een overeengekomen geheel van normen, procedures en beveiligingsmethoden voor:

d. het genereren van sleutels voor verschillende cryptografische systemen en toepassingen;
e. het genereren en verkrijgen van certificaten voor openbare sleutels;
f. het verspreiden van sleutels onder de beoogde gebruikers, waaronder een instructie hoe de sleutels na ontvangst behoort te worden geactiveerd;
g. het opslaan van sleutels, waaronder een instructie hoe bevoegde gebruikers toegang tot sleutels krijgen;
h. het wijzigen of actualiseren van sleutels, waaronder voorschriften met betrekking tot het moment waarop sleutels behoren te worden gewijzigd en hoe dit gebeurt;
i. het omgaan met sleutels die gecompromitteerd zijn;
j. het herroepen van sleutels, met inbegrip van instructies hoe sleutels behoren te worden ingetrokken of gedeactiveerd, bijvoorbeeld wanneer sleutels gecompromitteerd zijn of wanneer een gebruiker de organisatie verlaat (in welk geval de sleutels ook behoren te worden gearchiveerd);
k. het herstellen van sleutels die verloren of gecorrumpeerde zijn als onderdeel van het beheerproces van bedrijfscontinuïteit, bijvoorbeeld voor het herstellen van versleutelde informatie;
l. het archiveren van sleutels, bijvoorbeeld voor informatie die is gearchiveerd of waarvan een back-up is gemaakt;
m. het vernietigen van sleutels;
n. het registreren in een logbestand en beoordelen van activiteiten die verband houden met sleutelbeheer.

6. Fysieke beveiliging en beveiliging van de omgeving (A.11)

6.1 Apparatuur in computerruimtes (ISO27001-A11.2)

6.1.1 Plaatsing en bescherming van apparatuur (ISO27001-A11.2.1)

ISO: Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.

De volgende regels gelden voor apparatuur in computerruimtes (datacenters):

a. Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningsbeveiliging.
b. Standaard accounts in apparatuur worden gewijzigd en de bijbehorende standaard leveranciers wachtwoorden worden gewijzigd bij ingebruikname van apparatuur.
c. Gebouwen zijn beveiligd tegen de gevolgen van blikseminslag.
d. Eten en drinken zijn verboden in serverruimte (SER/MER).
e. Een informatiesysteem dient te voldoen aan de hoogste classificatie-eisen, conform de informatie die voor kan komen op het informatiesysteem bij het verwerken ervan. Indien dit niet mogelijk is wordt een gescheiden systeem gebruikt voor de informatieverwerking waaraan hogere eisen gesteld worden.

6.1.2 Beveiliging van bekabeling (ISO27001-A11.2.3)

ISO: Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.

a. leg elektriciteits- en telecommunicatiekabels voor IT-voorzieningen bij voorkeur ondergronds aan of bescherm deze afdoende op andere wijze;
b. bescherm netwerkkabels tegen ongeautoriseerd aftappen of beschadiging, bijvoorbeeld door ze in mantelbuizen of kabelgoten te leggen en zo min mogelijk door openbare ruimten te laten lopen;
c. houd netsnoeren gescheiden van communicatiekabels, of pas andere technieken toe om interferentie te voorkomen;
d. gebruik duidelijk identificeerbare markeringen op kabels en apparatuur om fouten bij bewerking te voorkomen, zoals het per ongeluk 'patchen' van de verkeerde netwerkkabels;
e. gebruik een gedocumenteerde patchlijst om de kans op fouten te verminderen;

Voor gevoelige of kritieke systemen kunnen verder de volgende beheersmaatregelen worden overwogen:

f. het installeren van gewapende kabelgoten en afgesloten ruimten of dozen voor inspectie- en eindpunten;
g. het gebruik van alternatieve routes en/of transmissiemedia om de juiste mate van beveiliging te leveren;
h. het gebruik van glasvezelkabels;
i. het gebruik van elektromagnetische afscherming om de kabels te beschermen, in het bijzonder waar medische apparatuur een hoog stralingsniveau kan veroorzaken;
j. het gebruik van detectievoorzieningen en fysieke inspectie om ongeautoriseerde apparatuur die op de bekabeling is aangesloten, op te sporen;

k. bewaakte toegang tot patchpanelen en kabelruimten.

6.1.3 Onderhoud van apparatuur (ISO27001-A11.2.4)

ISO: Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.

a. onderhoud apparatuur volgens de door de leverancier aanbevolen voorschriften en servicetijdstippen;
b. laat reparatie en onderhoud van apparatuur alleen uitvoeren door bevoegd onderhoudspersoneel;
c. houd registraties bij van alle vermeende of daadwerkelijke storingen en van alle preventieve en corrigerende onderhoudswerkzaamheden;
d. voer passende beheersmaatregelen in bij gepland onderhoud, daarbij in aanmerking nemend of het onderhoud wordt verricht door personeel op locatie of door extern personeel; verwijder waar nodig gevoelig materiaal van de apparatuur.

6.1.4 Verwijdering van bedrijfsmiddelen (ISO27001-A11.2.5)

ISO: Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

Verwijderbare opslagmedia

Voor het beheren van verwijderbare opslagmedia behoren de volgende richtlijnen te worden overwogen:

a. onderwerpspecifiek beleid inzake het beheer van verwijderbare opslagmedia vaststellen en dit onderwerpspecifieke beleid communiceren aan iedereen die verwijderbare opslagmedia gebruikt of hanteert;
b. indien nodig en haalbaar, goedkeuring vereisen om opslagmedia uit de organisatie te verwijderen en een registratie van dergelijke verwijderingen bijhouden om een audittraject te onderhouden;
c. alle opslagmedia opslaan in een veilige, beveiligde omgeving overeenkomstig de desbetreffende informatieclassificatie en beschermen tegen dreigingen van buitenaf (zoals warmte, vocht, luchtvochtigheid, elektronische velden of veroudering), overeenkomstig de specificaties van de fabrikant;
d. indien vertrouwelijkheid of integriteit van informatie belangrijke overwegingen zijn, cryptografische technieken gebruiken om informatie op verwijderbare media te beschermen;
e. om het risico te verkleinen dat opslagmedia in kwaliteit achteruitgaan terwijl de opgeslagen informatie nog nodig is, de informatie op nieuwe opslagmedia overbrengen voordat deze onleesbaar wordt;
f. van waardevolle informatie meerdere kopieën op afzonderlijke opslagmedia opslaan om het risico op toevallige beschadiging of verlies van informatie verder te beperken;
g. verwijderbare opslagmedia registreren om de kans dat informatie verloren gaat, te beperken;
h. poorten voor verwijderbare opslagmedia (bijv. SD-kaartsleuven en USB-poorten) alleen inschakelen indien er vanuit de organisatie een reden voor het gebruik ervan is;
i. als er behoefte is om verwijderbare opslagmedia te gebruiken, de overdracht van informatie op dergelijke opslagmedia monitoren;
j. informatie kan tijdens fysiek transport gevoelig zijn voor onbevoegde toegang, misbruik of beschadiging, bijvoorbeeld wanneer opslagmedia per post- of koeriersdienst worden verzonden.

6.1.5 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein (ISO27001-A11.2.6)

ISO: Apparatuur buiten de locaties moet worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.

Apparatuur om informatie op te slaan of te verwerken omvat alle typen personal computers, tablet pc's, organizers, mobiele telefoons, 'smart cards', 'smart phones', papieren en andere informatiedragers die worden meegenomen in verband met thuiswerk of van de normale werkplek naar elders worden meegenomen. Denk ook aan apparatuur die wordt geplaatst bij instellingen waarmee wordt samengewerkt.

a. laat apparatuur en media buiten het terrein niet onbeheerd achter in openbare ruimten. Draagbare computers behoren tijdens het reizen als handbagage te worden vervoerd en behoren zo min mogelijk herkenbaar te zijn;
b. zorg dat de instructies van de fabrikant ter bescherming van de apparatuur te allen tijde worden opgevolgd, bijvoorbeeld bescherming tegen het blootstellen aan sterke elektromagnetische velden;

c. tref beheersmaatregelen voor thuiswerken aan de hand van een risicobeoordeling; pas waar van toepassing geschikte beheersmaatregelen toe, bijvoorbeeld afsluitbare archiefkasten, 'clear desk'-beleid, toegangsbeveiliging voor computers en beveiligde communicatie met het kantoor;

6.1.6 Veilig verwijderen of hergebruiken van apparatuur (ISO27001-A11.2.7)

ISO: Alle apparatuur die opslagmedia bevat, moet worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.

Beveiligd hergebruiken of verwijderen

Voor het beveiligd hergebruiken of verwijderen van opslagmedia behoren procedures te worden vastgesteld om het risico zo klein mogelijk te houden dat vertrouwelijke informatie bij onbevoegde personen terechtkomt. De procedures voor het beveiligd hergebruiken of verwijderen van opslagmedia die vertrouwelijke informatie bevatten, behoren in verhouding te staan tot de gevoeligheid van die informatie.

Met de volgende aspecten behoort rekening te worden gehouden:

a. indien het nodig is opslagmedia met vertrouwelijke informatie te hergebruiken binnen de organisatie: op beveiligde wijze voorafgaand aan het hergebruik gegevens wissen of opslagmedia formatteren;
b. opslagmedia met vertrouwelijke informatie op beveiligde wijze verwijderen als ze niet meer nodig zijn (bijv. door ze te vernietigen, versnipperen of de inhoud ervan op beveiligde wijze te wissen);
c. procedures instellen om media te identificeren waarvan het nodig kan zijn ze veilig te verwijderen;
d. veel organisaties bieden inzamelings- en verwijderingsdiensten aan voor opslagmedia. Een geschikte externe leverancier met toereikende beheersmaatregelen en ervaring behoort met zorg te worden gekozen;
e. de verwijdering van gevoelige zaken in een logbestand bijhouden om een audittraject te onderhouden;
f. bij het accumuleren van opslagmedia voor verwijdering rekening houden met het aggregatie-effect, waardoor een grote hoeveelheid niet-gevoelige informatie gevoelig kan worden. Er behoort een risicobeoordeling te worden uitgevoerd van beschadigde apparatuur die gevoelige gegevens bevat om vast te stellen of de media fysiek behoren te worden vernietigd in plaats van te worden gerepareerd of verwijderd.

7. Beveiliging bedrijfsvoering (A.12)

7.1 Bedieningsprocedures en verantwoordelijkheden (A12.1)

7.1.1 Gedocumenteerde bedieningsprocedures (ISO27001-A12.1.1)

ISO: Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.

Bedieningsprocedures maken aan de gebruikers en de beheerders op een voor hen aangepaste wijze duidelijk op welke wijze het product kan worden gebruikt en beheerd. Behandel bedieningsprocedures en de gedocumenteerde procedures voor systeemactiviteiten als formele documenten, en zorg voor goedkeuring van wijzigingen door de verantwoordelijke. Zorg voor consistentie in beheer van informatiesystemen door zoveel mogelijk gebruik van dezelfde procedures, gereedschappen en hulpmiddelen.

Er moeten gedocumenteerde procedures opgesteld worden voor systeemactiviteiten met betrekking tot informatieverwerkings- en communicatievoorzieningen, zoals opstart- en afsluitprocedures voor computers, back-ups, onderhoud van apparatuur, behandeling van media, beheer van computerruimten veiligheid. Geef daarin instructies voor een gedetailleerde uitvoering van elke taak, waaronder:

a. verwerking en behandeling van informatie;
b. back-ups ;
c. eisen ten aanzien van de planning, waaronder onderlinge verbondenheid met andere systemen, start van de eerste taak en beëindiging van de laatste taak;
d. instructies voor de afhandeling van fouten en andere uitzonderlijke situaties die zich tijdens de uitvoering van de taak kunnen voordoen, waaronder beperkingen in het gebruik van systeemhulpmiddelen;
e. contactpersonen voor onverwachte bedieningsmoeilijkheden of technische storingen;
f. instructies voor de behandeling van bijzondere uitvoer en media, zoals het gebruik van vertrouwelijke uitvoer;
g. procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen;
h. beheer van 'audit trail' en systeemlogbestand-informatie.

7.1.2 Wijzigingsbeheer (ISO27001-A12.1.2)

ISO: Veranderingen in de organisatie, bedrijfsprocessen, informatie-verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.

We zorgen dat wijzigingen in IT-voorzieningen en systemen altijd zorgvuldig worden beheerd om storingen in systemen of beveiliging te voorkomen.

Het proces voor wijzigingsbeheer omvat een risicobeoordeling, een analyse van de gevolgen van wijzigingen en een specificatie van de benodigde beveiligingsmaatregelen. Bij grote wijzigingen stellen we een plan met proces op. Dit proces waarborgt dat bestaande beveiligings- en beheersingsprocedures niet worden gecompromitteerd. Toegang wordt gegeven uitsluitend tot die onderdelen van het systeem die noodzakelijk zijn voor werkzaamheden, en wijzigingen worden vooraf overlegt.

Procedures voor wijzigingsbeheer vereisen dat er vooraf een gedetailleerd plan wordt opgesteld om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie in

informatieverwerkende faciliteiten en informatiesystemen te garanderen doorheen de gehele ontwikkelcyclus van systemen, vanaf de ontwerpfase tot en met alle daaropvolgende onderhoudsinspanningen. Afwijkingen van dit plan moeten zorgvuldig worden gedocumenteerd.

Waar mogelijk behoren de procedures voor wijzigingsbeheer voor ICT-infrastructuur en -software te
worden geïntegreerd.

De procedures voor wijzigingsbeheer behoren het volgende te omvatten:

a. het plannen en beoordelen van de potentiële impact van wijzigingen, waarbij alle afhankelijkheden in aanmerking worden genomen;
b. autorisatie van veranderingen;
c. ceranderingen aan relevante belanghebbenden communiceren;
d. tests en de aanvaarding van tests voor de veranderingen;
e. implementatie van veranderingen met inbegrip van inzetplannen;
f. nood- en voorzorgsoverwegingen, met inbegrip van vangnetprocedures;
g. registraties onderhouden van veranderingen waarin alle bovenstaande punten worden opgenomen;
h. waarborgen dat bedieningsdocumentatie en gebruikersprocedures indien nodig worden gewijzigd om ze toepasbaar te houden;
i. bewerkstelligen dat de plannen voor ICT-continuïteit en de respons- en herstelprocedures worden gewijzigd naarmate nodig is om passend te blijven.

7.1.3 Beleid voor Informatiebeveiliging in projectbeheer (ISO27001- A.6.1.5)

ISO: Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.

In projectbeheer behoren de volgende zaken worden meegenomen:

a. In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.
b. In standaarden voor analyse, ontwikkeling en testen van informatiesystemen wordt structureel aandacht besteed aan beveiligingsaspecten.
c. Bij aanschaf van producten wordt een proces gevolgd waarbij beveiliging een onderdeel is van de specificatie.
d. Waar het gaat om beveiligingsrelevante producten wordt de keuze voor een bepaald product verantwoord onderbouwd.
e. Er is expliciet aandacht voor leveranciers-accounts, hardcoded wachtwoorden en mogelijke ‘achterdeurtjes’.

7.1.4 Capaciteitsbeheer (ISO27001-A12.1.3)

ISO: Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.

In het kader van het realiseren van de beveiligingseis omtrent beschikbaarheid is het raadzaam de noodzakelijke capaciteit (nu en in de toekomst) van diverse zaken in het oog te houden, opdat tijdig corrigerende maatregelen kunnen worden genomen. Gedacht kan worden aan: onmisbaar personeel, stroomvoorziening, netwerk, bandbreedte, systeemgeheugen, schijfgeheugen en kosten.

Capaciteitseisen moeten vastgesteld worden voor elke nieuwe en bestaande activiteit.

a. Zorg voor afstemming daarop en controle van het systeem om de beschikbaarheid en doelmatigheid van de systemen te waarborgen en waar nodig te verbeteren.
b. Zorg voor detectiemaatregelen om problemen op tijd vast te stellen.
c. Betrek prognoses van toekomstige capaciteitsbehoeften bij nieuwe bedrijfs- en systeemeisen en huidige en geraamde trends in de informatieverwerkingscapaciteit van de organisatie.
d. Besteed bijzondere aandacht aan onderdelen met lange levertijden of hoge kosten.
e. Beheerders moeten het gebruik van de belangrijkste systeemonderdelen controleren en trends in het gebruik signaleren.

7.1.5 Scheiding van ontwikkel-, test- en productieomgevingen (ISO27001-A12.1.4)

Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.

a. Binnen Microsoft 365 (M365) kunnen alle medewerkers toegang krijgen tot het besturingssysteem en de applicaties, mits deze door Microsoft beschikbaar zijn gesteld en door de systeembeheerder zijn geactiveerd. Indien het een testomgeving betreft, wordt de autorisatie verleend op basis van de specifieke taken, functies en de doelstellingen van de test, en is deze tijdsgebonden.
b. Bij de leveranciersbeoordeling worden beveiligingsaspecten in overweging genomen.

7.2 Bescherming tegen malware (A.12.2)

7.2.1 Beheersmaatregelen tegen malware (ISO27001-12.2.1)

ISO: Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.

Baseer de bescherming tegen kwaadaardige programmatuur op het ontdekken en op herstelprogrammatuur, op een goed beveiligingsbewustzijn, toegangsbeveiliging van systemen en controle van wijzigingsbeheer.
Houd rekening met de mogelijke aanwezigheid van kwaadaardige programmatuur in versleutelde bestanden.

Bescherming moet verkregen worden door:

a. het beleid dat het gebruik van ongeautoriseerde programmatuur verbiedt (zie algemeen beleid);
b. Leveranciers van systeem- en applicatieprogrammatuur brengen geregeld ‘patches’ uit om fouten aan hun producten te verbeteren. Het is van belang alert te blijven op nieuwe ‘patches’.
c. regelmatige beoordeling van de programmatuur en de inhoud van de gegevens van systemen waarmee kritieke bedrijfsprocessen worden ondersteund; de aanwezigheid van niet-goedgekeurde bestanden of ongeautoriseerde wijzigingen formeel te onderzoeken;
d. installatie en regelmatige actualisering van programmatuur voor het ontdekken van kwaadaardige programmatuur en herstelprogrammatuur om computers en media te scannen, hetzij als voorzorgsmaatregel, hetzij op basis van routine; uitvoeren van controles waaronder:
    - controleren van bestanden op elektronische of optische media en bestanden die via netwerken zijn ontvangen, op kwaadaardige programmatuur voordat ze worden gebruikt;
    - controleren van e-mailbijlagen en gedownloade bestanden op kwaadaardige programmatuur voordat ze worden gebruikt; uitvoeren van deze controle op

verschillende plaatsen, bijvoorbeeld op e-mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie;
- controleren van webpagina's op kwaadaardige programmatuur;

e. kwaadaardige programmatuur op systemen, training in het gebruik ervan, rapportage en herstel van aanvallen met kwaadaardige programmatuur ;
f. opstellen van geschikte continuïteitsplannen voor herstel na aanvallen met kwaadaardige programmatuur, waaronder alle nodige voorzieningen voor back-ups van gegevens en programmatuur, evenals herstelmaatregelen;
g. implementeren van procedures om regelmatig informatie te verzamelen, zoals het abonneren op verzendlijsten en/of raadplegen van websites die informatie geven over nieuwe kwaadaardige programmatuur;
h. implementeren van procedures om alle informatie met betrekking tot kwaadaardige programmatuur te verifiëren en te waarborgen dat waarschuwingsberichten nauwkeurig en informatief zijn; beheerders laten waarborgen dat alle gekwalificeerde bronnen, bijvoorbeeld erkende bladen, betrouwbare internetsites of leveranciers van antivirusprogrammatuur, worden gebruikt om onderscheid te maken tussen vals alarm en werkelijke kwaadaardige programmatuur; alle gebruikers attent maken op het probleem van een vals alarm en laten weten wat ze bij ontvangst ervan moeten doen.

7.3 Back-up (A12.3)

7.3.1 Back-up van informatie (ISO27001-A12.3.1)

ISO: Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenkomst met een overeengekomen back-upbeleid.

Houd geschikte back-upvoorzieningen beschikbaar, zodat alle essentiële bedrijfsgegevens en programmatuur kunnen worden hersteld na een computercalamiteit of een defect medium.

a. definieer de eisen die aan back-up en herstel worden gesteld;
b. houd nauwkeurige en volledige registers van back-ups bij en gedocumenteerde herstelprocedures;
c. zorg dat de omvang (bijvoorbeeld volledige back-up of alleen van de wijzigingen) en frequentie van back-ups in overeenstemming zijn met de bedrijfseisen van de organisatie, de beveiligingseisen van de desbetreffende informatie en het kritieke karakter van de informatie voor de voortzetting van de bedrijfsvoering van de organisatie;
d. sla de back-ups op op een locatie die zich op zodanige afstand bevindt dat schade aan de back-up ten gevolge van een calamiteit op de hoofdlocatie onwaarschijnlijk is;
e. zorg voor fysieke bescherming van de back-ups en de ruimte waarin deze zijn opgeslagen volgens dezelfde normen die gelden voor de hoofdlocatie; de beveiligingseisen voor media op de hoofdlocatie gelden ook voor de back-uplocatie;
f. test de mogelijkheid om te herstellen vanuit reservekopieën regelmatig, om te waarborgen dat deze betrouwbaar zijn en in geval van nood kunnen worden gebruikt;
g. controleer en test herstelprocedures regelmatig om te waarborgen dat ze doeltreffend zijn en dat ze kunnen worden uitgevoerd binnen de daarvoor volgens operationele herstelprocedures gestelde tijd;
h. bescherm in gevallen waar vertrouwelijkheid van belang is, back-ups door middel van encryptie. Let er hierbij op, dat de back-up in geval van een calamiteit teruggeplaatst moet kunnen worden op een ander systeem. Dit stelt ook bijzondere eisen aan het beheer van de encryptiesleutels, om te voorkomen dat de informatie ontoegankelijk wordt.

Er kunnen situaties voorkomen waarin een leverancier verantwoordelijk is voor de back-up, het herstel, de back-upinstellingen, programma's en relevante gegevens.

Test procedures voor het maken van back-ups voor afzonderlijke systemen regelmatig om te waarborgen dat aan de eisen van het bedrijfscontinuïteitsplan wordt voldaan.

i. Zorg ervoor dat altijd tenminste twee back-ups beschikbaar zijn.
j. Zorg voor kritische systemen dat de procedures voor het maken van back-ups alle systeeminformatie, -toepassingen en gegevens omvatten die nodig zijn om het gehele systeem te herstellen na een calamiteit.

Back-upprocedures kunnen worden geautomatiseerd om het back-up- en herstelproces te vereenvoudigen. Dergelijke geautomatiseerde oplossingen behoren voldoende te worden getest, voor implementatie en met regelmatige tussenpozen.

7.4 Verslaglegging en monitoren (A12.4)

De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:

a. gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore.
b. gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit
c. handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.
d. beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services).
e. logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren aangesloten op een Security Information and Event Management Systeem

7.5 Beschermen van informatie in logbestanden (ISO27001-A12.4.2)

ISO: Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.

7.5.1 Logbestanden van beheerders en operators (ISO27001-A12.4.3)

ISO: Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.

Op basis van de resultaten van de risicobeoordeling, beslist de Privacy en Security Officer welke logs bewaard gaan worden op en voor welke systemen, en hoe lang ze zullen worden opgeslagen. Logs dienen te worden bewaard voor alle beheerders en systeembeheerders op gevoelige systemen.

Privacy en Security Officer is verantwoordelijk voor het periodiek controleren van de logs van automatisch gerapporteerde fouten, als ook voor het registreren van fouten gerapporteerd door gebruikers, om te analyseren waarom fouten optreden en om geschikte corrigerende

acties te nemen. [specifieke autorisaties kunnen worden gespecificeerd in het geval van een fout, als ook hoe registraties van fouten worden bewaard]

Privacy en Security Officer is verantwoordelijk voor het regelmatig bekijken van de logs om de activiteiten van de gebruikers, beheerders en systeembeheerders. De beoordeling wordt uitgevoerd binnen de door de Privacy en Security Officer voorgeschreven intervallen en selecteert de na te kijken registraties, en hoe de uit te voeren beoordeling zal worden vastgelegd. CvB dient te worden geïnformeerd over de resultaten van de beoordeling.

7.5.2 Kloksynchronisatie (ISO27001-A12.4.4)

ISO: De klokken van alle relevante informatie-verwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.

De juiste instelling van computerklokken is belangrijk om de nauwkeurigheid van auditlogs te waarborgen, die nodig kunnen zijn voor onderzoeken of als bewijs in juridische of disciplinaire zaken. Onnauwkeurige auditlogs kunnen dergelijke onderzoeken bemoeilijken en de geloofwaardigheid van dergelijk bewijs schaden. Een klok gekoppeld aan een radiotijdsignaal van een nationale atoomklok kan worden gebruikt als de hoofdklok voor logging systemen. Een netwerk-tijdprotocol kan worden gebruikt om alle servers in synchronisatie te houden met de hoofdklok.

7.6 Beheersing van operationele software (A12.5)

Actualiseer besturingssystemen alleen wanneer daar een dwingende reden voor is, bijvoorbeeld indien de huidige versie van het besturingssysteem niet langer de bedrijfseisen ondersteunt. Het enkele feit dat een nieuwe versie van het besturingssysteem beschikbaar is, is geen reden voor installeren van een upgrade. Nieuwe versies van besturingssystemen kunnen minder veilig zijn, minder stabiel en minder begrijpelijk dan de huidige systemen.

7.6.1 Software installeren op operationele systemen (ISO27001-A12.5.1)

ISO: Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.

Houd om het risico van corrumperen van productiesystemen tot een minimum te beperken rekening met de volgende richtlijnen om wijzigingen te beheersen:

a. het actualiseren van productieprogrammatuur, -toepassingen en -programmabibliotheken wordt uitsluitend uitgevoerd door ervaren beheerders na overleg met het CvB.
b. op productiesystemen is alleen goedgekeurde uitvoerbare programmatuur aanwezig.
c. toepassingen en besturingssysteemprogrammatuur worden geïmplementeerd na uitgebreide en succesvolle tests; er wordt o.a. getest op bruikbaarheid, beveiliging, effecten op andere systemen en gebruikersvriendelijkheid en de tests worden op losstaande systemen uitgevoerd;
d. er wordt een configuratiebeheerssysteem gebruikt om alle geïnstalleerde programmatuur en de systeemdocumentatie te kunnen beheersen;
e. er is een terugdraaistrategie vastgesteld voordat wijzigingen worden doorgevoerd;
f. er wordt een auditlogbestand bijgehouden van elke update van besturingsprogrammabibliotheken;
g. eerdere versies van de toepassingsprogrammatuur worden indien mogelijk bewaard voor noodgevallen;

Overige regels:

h. Programmatuur van leveranciers die in productiesystemen wordt gebruikt, worden op een niveau onderhouden dat door de leverancier wordt ondersteund. Na verloop van

tijd zullen programmatuurleveranciers de ondersteuning van oudere versies van de programmatuur staken. De organisatie onderkent de risico's van het vertrouwen op niet-ondersteunde programmatuur.

i. Bij ieder besluit over upgraden naar een nieuwe programmatuurversie wordt rekening gehouden met de bedrijfseisen voor de wijziging en de veiligheid van deze versie, d.w.z. de invoering van nieuwe beveiligingsfunctionaliteit of het aantal en de ernst van de beveiligingsproblemen die met deze versie samenhangen. Eventueel worden herstelprogramma's (patches) in de programmatuur geïmplementeerd om zwakke plekken in de beveiliging te verhelpen of te verminderen.
j. Geef leveranciers alleen fysieke of logische toegang wanneer dit noodzakelijk is voor ondersteunende diensten en altijd met navraag/toestemming van de verantwoordelijke domeinbeheerder/ directie. Controleer de activiteiten van de leverancier, in het bijzonder bij onderhoud op afstand.
k. Computerprogrammatuur kan soms steunen op extern geleverde programmatuur en modules: monitor en controleer in deze gevallen om onbevoegde wijzigingen te vermijden, waardoor zwakke plekken in de beveiliging zouden kunnen ontstaan.

7.7 Beheer van technische kwetsbaarheden (A12.6)

7.7.1 Beheer van technische kwetsbaarheden (ISO27001-A12.6.1)

ISO: 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.

Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.

Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).

Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.

7.7.2 Beperkingen op software-installatie

ISO: Regels betreffend de installatie van software door gebruikers moeten vastgesteld en ingevoerd worden.

In specifieke gevallen, zoals voor het testen van een softwareapplicatie of het gebruik van een softwaretool, kunnen individuele gebruikers naast systeembeheerders extra toegangsrechten verkrijgen om de software te installeren. Een dergelijk verzoek moet worden ingediend bij de systeembeheerder, die overlegt met de Privacy en Security Officer alvorens goedkeuring te verlenen.

De volgende richtlijnen behoren in overweging te worden genomen om wijzigingen en de installatie van software op operationele systemen op beveiligde wijze te beheren:

a. updates van operationele software alleen laten uitvoeren door daartoe opgeleide beheerders met passende beheerdersrechten;

b. garanderen dat er alleen goedgekeurde uitvoerbare code, en geen ontwikkelcode of compilers, op operationele systemen wordt geïnstalleerd;
c. software pas installeren en updaten na uitgebreide en geslaagde tests;
d. alle bijbehorende programmabronbibliotheken updaten;
e. een configuratiebeheerssysteem gebruiken om alle operationele software en systeemdocumentatie te beheersen;
f. een roll-backstrategie definiëren alvorens wijzigingen te implementeren;
g. een auditlogbestand bijhouden van alle updates van operationele software;
h. oude versies van software, samen met alle vereiste informatie en parameters, procedures, configuratiedetails archiveren en software als noodmaatregel ondersteunen zolang de software nodig is om gearchiveerde gegevens te lezen of te verwerken.

Bij beslissingen om te upgraden naar een nieuwe versie behoort rekening te worden gehouden met de bedrijfseisen die gelden voor de verandering en de veiligheid van de versie (bijv. de introductie van nieuwe informatiebeveiligingsfunctionaliteit of het aantal en de ernst van kwetsbaarheden in de
informatiebeveiliging die zich bij de huidige versie voordoen).

Softwarepatches behoren te worden toegepast als ze kunnen bijdragen aan het verwijderen of verminderen van kwetsbaarheden in de informatiebeveiliging.

Computersoftware kan gebruikmaken van extern geleverde software en pakketten (bijv. softwareprogramma's met modules die op externe locaties worden gehost). Deze behoren te worden gemonitord en beheerst om ongeautoriseerde wijzigingen te vermijden omdat ze tot kwetsbaarheden in de informatiebeveiliging kunnen leiden.

Software van leveranciers die in productiesystemen wordt gebruikt, behoort te worden onderhouden op een niveau dat door de leverancier wordt ondersteund. Na verloop van tijd zullen softwareleveranciers stoppen met het ondersteunen van oudere softwareversies. De organisatie behoort de risico’s van het gebruiken van niet-ondersteunde software te overwegen.

In operationele systemen toegepaste opensourcesoftware behoort op de stand van de meest recente geschikte uitgave van de software te worden onderhouden. Het is mogelijk dat opensourcecode na verloop van tijd niet meer wordt onderhouden, maar nog steeds beschikbaar is in een opensourcesoftwarebewaarplaats.

De organisatie behoort ook rekening te houden met de risico's van het in operationele systemen gebruiken van opensourcesoftware die niet meer wordt onderhouden.

Wanneer leveranciers betrokken zijn bij het installeren of updaten van software, behoort fysieke of logische toegang alleen te worden verleend wanneer dat nodig is en met passende autorisatie.
De activiteiten van de leverancier behoren te worden gemonitord. De organisatie behoort strikte regels te definiëren en ten uitvoer te brengen met betrekking tot de soorten software die gebruikers kunnen installeren.

Het beginsel van het ‘least privilege’ (minste voorrechten) behoort te worden toegepast op de installatie van software op operationele systemen.

De organisatie behoort vast te leggen welke soorten software mogen worden geïnstalleerd (bijv. updates en beveiligingspatches voor bestaande software) en welke verboden zijn (bijv. software uitsluitend voor persoonlijk gebruik en software waarvan de herkomst met betrekking tot de potentiële kwaadaardigheid onbekend of verdacht is). Deze voorrechten behoren te worden verleend op basis van de rollen van de betrokken gebruikers.

7.8 Overwegingen betreffende audits van informatiesystemen (A12.7)

ISO: Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, moeten zorgvuldig worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

Denk hierbij aan het uitvoeren van interne en externe audits, en neem daarbij de volgende richtlijnen in acht:

a. bewerkstellig dat de persoon/personen die de audit uitvoert/uitvoeren geen belangen heeft/hebben bij de activiteiten die worden geaudit.
b. beperk de controles van programmatuur en gegevens tot alleen-lezen-toegang ('read-only');
c. laat andere toegang dan 'alleen lezen' uitsluitend toe voor geïsoleerde kopieën van systeembestanden, die na beëindiging van de audit weer worden gewist, of op een juiste wijze worden beschermd indien de audit-documentatie dit vereist;
d. controleer alle toegang, leg die vast in een logbestand om een 'reference trail' te produceren; overweeg voor kritische gegevens of systemen een 'reference trail' met tijdregistratie;
e. stel hulpmiddelen voor de uitvoering van de controles expliciet vast en stel ze beschikbaar;
f. kom eisen voor bijzondere of aanvullende verwerking overeen en stel ze vast;

8. Communicatiebeveiliging (A.13)

8.1 Beheer van netwerkbeveiliging (ISO27001-A13.1)

8.1.1 Beheersmaatregelen voor netwerken (ISO27001-A13.1.1)

ISO: Netwerken moeten adequaat worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

Aanbevelingen voor netwerkbeheerders voor het waarborgen van de beveiliging van informatie in netwerken en van aangesloten diensten tegen ongeoorloofde toegang:

a. scheid de operationele verantwoordelijkheid voor netwerken waar nodig van de verantwoordelijkheid voor computerbewerkingen;
b. stel verantwoordelijkheden en procedures vast voor het beheer van apparatuur op afstand, waaronder apparatuur in gebruikersruimten;
c. tref extra beheersmaatregelen om de vertrouwelijkheid en integriteit te waarborgen van gegevens die via openbare netwerken en over draadloze netwerken worden verzonden en om de aangesloten systemen en toepassingen te beschermen; ook kunnen extra beheersmaatregelen nodig zijn om de beschikbaarheid van netwerkdiensten en aangesloten computers te handhaven;
d. pas een passende registratie en controle toe om handelingen die van belang zijn voor de beveiliging te kunnen vastleggen;
e. zorg voor nauwkeurige coördinatie van beheeractiviteiten om de dienstverlening aan de organisatie te optimaliseren en om te waarborgen dat beveiligingsmaatregelen consistent worden toegepast over de informatie-verwerkende infrastructuur als geheel.

8.1.2 Beveiliging van netwerkdiensten (ISO27001-A13.1.2)

ISO: Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

Tot de netwerkdiensten worden gerekend het leveren van aansluitingen, private netwerkdiensten, netwerken met toegevoegde waarde en beheerde beveiligingsoplossingen zoals firewalls en 'intrusion detection'. Deze diensten kunnen uiteenlopen van eenvoudige onbeheerde bandbreedte tot en met complexe aanbiedingen met toegevoegde waarde. Beveiligingskenmerken van netwerkdiensten zijn:

a. technologie toegepast voor de beveiliging van netwerkdiensten, zoals authenticatie, encryptie en gebruikmaken van VLAN.
b. technische parameters vereist voor beveiligde verbinding met de netwerkdiensten in overeenstemming met de beveiligings- en netwerkaansluitingsregels;
c. procedures voor het gebruik van netwerkdiensten om de toegang tot netwerkdiensten of toepassingen, waar nodig, te beperken.
d. Indien de netwerkdiensten zijn uitbesteed, dan dienen de vereisten in een overeenkomst te worden vastgelegd (zie algemeen Informatiebeveilligingsbeleid).
e. Bepaal de kundigheid van de aanbieder van netwerkdiensten om overeengekomen diensten op een veilige manier te beheren en controleer deze regelmatig. Verlang het recht op audit.

f. Stel de beveiligingsprocedures vast die voor bepaalde diensten nodig zijn, zoals beveiligingskenmerken, dienstverleningsniveaus en eisen voor beheer. Stel zeker dat de leveranciers van netwerkdiensten de verlangde maatregelen implementeren.
g. Indien er leerlinggegevens worden verwerkt is het van belang zorgvuldig na te gaan welke gevolgen het wegvallen van netwerkdiensten kan hebben op de dienstverlening.

8.1.3 Scheiding in netwerken (ISO27001-A13.1.3)

Groepen van informatiediensten, -gebruikers en –systemen moeten in netwerken worden gescheiden.

a. Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.
b. Van systemen wordt bijgehouden in welke zone ze staan.
c. Elke zone heeft een gedefinieerd beveiligingsniveau. Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
d. Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.
e. Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).

Om inkomend verkeer van draagbare apparaten te scheiden, installeer een unieke firewallregels(beleid) op, statische routes, Virtuele Local Area Networks (VLAN), enz.

9. Acquisitie, ontwikkeling en onderhoud van informatiesystemen

9.1 Beveiligingseisen voor informatiesystemen (A14.1)

Om te zorgen dat informatiebeveiliging een integraal onderdeel is van de gehele levensloop van informatiesystemen. Dit geldt ook voor dienstverlening via internet.

9.1.1 Analyse en specificatie van beveiligingseisen (ISO27001-A14.1.1)

ISO: In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen moeten ook eisen voor beveiligingsmaatregelen worden opgenomen.

a. De beveiligingseisen voor informatiesystemen zijn bedoeld om voldoende beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te waarborgen. De vertrouwelijkheid mag niet worden geschonden, maar de maatregelen die met het oog op het handhaven van de vertrouwelijkheid worden getroffen, kunnen ook weer niet zo rigide zijn dat daardoor de beschikbaarheid in gevaar zou komen. Ontwerp daarom vertrouwelijkheidsmaatregelen en afscherming voor toepassingen zodanig dat de vereiste beschikbaarheid altijd wordt gewaarborgd.
b. Let op dat de eisen voor beveiligingsmaatregelen aangeven welke geautomatiseerde beheersmaatregelen in het systeem zijn ingebouwd, en wat de benodigde ondersteunende handmatige beheersmaatregelen zijn. Maak vergelijkbare afwegingen bij het beoordelen van programmatuur die is ontwikkeld of aangeschaft voor bedrijfstoepassingen.
c. Bewaak dat beveiligingseisen en -maatregelen een afspiegeling zijn van de waarde van de informatie voor het bedrijf en de mogelijke schade voor het bedrijf als gevolg van het falen of het ontbreken van beveiliging.
d. Zorg ervoor dat systeemeisen voor informatiebeveiliging en de processen voor het implementeren van de beveiliging al in een vroeg stadium in informatiesysteemprojecten worden geïntegreerd. Het is beduidend goedkoper beveiligingsmaatregelen tijdens de ontwerpfase te implementeren en te onderhouden dan tijdens of na de implementatie.
e. Zorg ervoor dat indien producten worden aangeschaft een formeel test- en inkoopproces wordt gevolgd. Neem in de contracten met de leverancier de vastgestelde beveiligingseisen op. Heroverweeg, waar de beveiligingsfunctionaliteit in een voorgesteld product niet voldoet aan de gestelde eis, het geïntroduceerde risico en de daarmee verbonden beheersmaatregelen alvorens het product aan te schaffen. Voer een aanvullende risicobeoordeling uit indien extra functionaliteit wordt geleverd die een beveiligingsrisico met zich mee kan brengen, om vast te stellen welke beheersmaatregelen nodig zijn om het risico tot een aanvaardbaar niveau te beperken en beoordeel op grond daarvan of er voordeel te behalen is uit de extra functionaliteit.

9.1.2 Toepassingsdiensten op openbare netwerken beveiligen (ISO27001-A14.1.2)

ISO: 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..

Zie het hoofdstuk over cryptografische beheersmaatregelen (ISO27001-A.10) in dit document.

Algemeen

Beveiligingseisen voor toepassingen behoren te worden geïdentificeerd en gespecificeerd. Deze eisen worden gewoonlijk aan de hand van een risicobeoordeling vastgesteld. De eisen behoren met ondersteuning van informatiebeveiligingsspecialisten te worden ontwikkeld.

Toepassingsbeveiligingseisen kunnen allerlei onderwerpen betreffen, afhankelijk van het doel van de toepassing.

Toepassingsbeveiligingseisen behoren het volgende te omvatten, al naargelang de situatie:

a. het niveau van vertrouwen in de identiteit van entiteiten [bijv. via authenticatie;
b. het identificeren van het door de toepassing te verwerken soort informatie en het classificatieniveau ervan;
c. de noodzaak van segmentatie van toegang en het niveau van toegang tot gegevens en functies in de toepassing;
d. weerstand tegen kwaadaardige aanvallen of onbedoelde verstoringen [bijv. bescherming tegen bufferoverflow of SQL-injecties];
e. wettelijke, statutaire en regelgevende eisen in het rechtsgebied waar de transactie wordt gegenereerd, verwerkt, voltooid of opgeslagen;
f. de noodzaak van privacy met betrekking tot alle betrokken partijen;
g. de eisen ten aanzien van bescherming van vertrouwelijke informatie;
h. bescherming van gegevens tijdens de verwerking, tijdens het transport en in ruste;
i. de noodzaak om communicatie tussen alle betrokken partijen op beveiligde wijze te versleutelen;
j. inputbeheersmaatregelen, waaronder integriteitscontroles en validatie van de invoer;
k. geautomatiseerde beheersmaatregelen (bijv. goedkeuringslimieten of dubbele goedkeuring);
l. outputbeheersmaatregelen, waarbij ook wordt nagedacht over wie er toegang kan hebben tot output en de autorisatie ervoor;
m. beperkingen met betrekking tot de inhoud van 'vrije tekstvelden', aangezien deze kunnen leiden tot ongecontroleerde opslag van vertrouwelijke gegevens (bijv. persoonsgegevens);
n. eisen die zijn afgeleid van het bedrijfsproces, zoals registreren en monitoren van transacties, eisen voor onweerlegbaarheid;
o. eisen die verplicht zijn gesteld door andere beheersmaatregelen met betrekking tot beveiliging (bijv. interfaces voor het registreren en monitoren of systemen voor het detecteren van lekken van gegevens);
p. het afhandelen van foutmeldingen.

Transactionele diensten

In aanvulling hierop behoort voor toepassingen die transactionele diensten tussen de organisatie en een partner aanbieden, het volgende in aanmerking te worden genomen bij het identificeren van informatiebeveiligingseisen:

a. de mate van vertrouwen die beide partijen eisen van elkaars beweerde identiteit;
b. de vereiste mate van vertrouwen in de integriteit van informatie die wordt uitgewisseld of verwerkt en de mechanismen voor het identificeren van integriteitsgebreken (bijv. cyclische redundantiecontrole, hashing, digitale handtekeningen);
c. autorisatieprocedures voor wie de inhoud van belangrijke transactiedocumenten kan goedkeuren, belangrijke transactiedocumenten in circulatie kan brengen of kan ondertekenen;
d. vertrouwelijkheid, integriteit, bewijs van verzending en ontvangst van belangrijke documenten en de onweerlegbaarheid (bijv. contracten in samenhang met inschrijvings- en contractprocedures);
e. de vertrouwelijkheid en integriteit van transacties (bijv. orders, gegevens betreffende afleveringsadressen en ontvangstbevestigingen);
f. eisen ten aanzien van hoelang een transactie vertrouwelijk moet blijven;
g. verzekerings- en andere contractuele eisen.

Toepassingen voor elektronisch bestellen en betalen

In aanvulling hierop behoort het volgende in aanmerking te worden genomen voor toepassingen waarbij er sprake is van elektronisch bestellen en betalen:

a. eisen om de vertrouwelijkheid en integriteit van orderinformatie in stand te houden;
b. de mate van verificatie die passend is voor controle van betalingsinformatie die door een klant is verstrekt;
c. verlies of vermenigvuldiging van transactie-informatie vermijden;
d. transactiegegevens buiten een publiek toegankelijke omgeving opslaan (bijv. op een opslagplatform op het intranet van de organisatie, in plaats van deze te bewaren en te tonen op direct vanuit internet toegankelijke elektronische opslagmedia);
e. als een vertrouwde instantie wordt gebruikt (bijv. voor het uitgeven en onderhouden van digitale handtekeningen of digitale certificaten), beveiliging integreren en inbedden in het gehele beheerproces van certificaten of handtekeningen.

Een aantal van de bovengenoemde aspecten kan worden opgepakt door toepassing van cryptografie, waarbij wettelijke eisen in aanmerking worden genomen

9.1.3 Transacties van toepassingsdiensten beschermen (ISO27001-A14.1.3)

ISO: 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..

Er bestaan allerhande vormen transacties die online kunnen worden uitgevoerd, bijvoorbeeld contractueel, financieel, planning van afspraken enz. Wetten, regels en voorschriften in het rechtsgebied waarin de transactie is gegenereerd, verwerkt, afgemaakt, en/of opgeslagen kunnen onderling verschillen.

Richtlijnen voor beveiliging van onlinetransacties zijn, afhankelijk van het risico:

a. het gebruik van elektronische handtekeningen door alle partijen die bij de transactie zijn betrokken;
b. alle aspecten van de transactie, dat wil zeggen waarborgen dat:
   - gebruikersgegevens van alle partijen geldig en gecontroleerd zijn;
   - de transactie vertrouwelijk blijft en
   - de privacy van alle betrokken partijen behouden blijft;
c. de communicatieroute tussen alle betrokken partijen versleuteld is;
d. de protocollen voor de communicatie tussen alle betrokken partijen beveiligd zijn;
e. waarborgen dat de opslag van de transactiedetails wordt gedaan buiten enige openbaar toegankelijke omgeving, bijvoorbeeld een opslagplatform op het intranet van de organisatie, en niet ondergebracht en toegankelijk op een opslagmedium dat direct via het internet toegankelijk is;
f. wanneer gebruik wordt gemaakt van een vertrouwde autoriteit (bijvoorbeeld voor het uitgeven en onderhouden van elektronische handtekeningen en/of digitale certificaten) de beveiliging is geïntegreerd en ingebed in de gehele keten van het certificaat/handtekeningbeheerproces.

De genomen beheersmaatregelen zullen in verhouding staan tot het risiconiveau dat hoort bij de vorm van onlinetransactie.

Het is belangrijk om vast te stellen of bij onlinetransacties gegevens zijn betrokken die persoonsinformatie bevatten. In dat geval is mogelijk aanvullende beveiliging nodig. Speciale aandacht vragen gegevens die betrekking hebben op declaraties, factuurregels, claims, vorderingen en andere gegevens waaruit persoonsinformatie kan worden afgeleid.

9.2 Beveiliging bij ontwikkelings- en ondersteuningsprocessen (A14.2)

Om zeker te stellen dat informatiebeveiliging wordt ontworpen, gerealiseerd en geïmplementeerd binnen de gehele levensloop van informatiesystemen.

9.2.1 Procedures voor wijzigingsbeheer met betrekking tot systemen (ISO27001-A14.2.2)

ISO: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.

Documenteer formele procedures voor wijzigingsbeheer van de operationele omgeving en dwing deze af om de kans op corrumperen van informatiesystemen tot een minimum te beperken. Bewerkstellig dat het invoeren van nieuwe systemen en belangrijke wijzigingen in bestaande systemen een formeel proces volgt van documentatie, specificatie, testen, kwaliteitscontrole en beheerde implementatie.

Integreer waar mogelijk procedures voor wijzigingsbeheer voor de operationele omgeving en voor toepassingsprogrammatuur. Zorg ervoor dat de wijzigingsprocedures de volgende punten omvatten:

a. bijhouden van een registratie van overeengekomen autorisatieniveaus;
b. waarborgen dat wijzigingen alleen worden doorgevoerd door bevoegde gebruikers;
c. beoordelen van beheersmaatregelen en integriteitsprocedures om te waarborgen dat deze niet door de wijzigingen gecompromitteerd worden;
d. identificatie van alle programmatuur die wijziging behoeven;
e. vooraf verkrijgen van formele goedkeuring voor gedetailleerde voorstellen;
f. waarborgen dat bevoegde gebruikers de wijzigingen aanvaarden voordat ze worden geïmplementeerd;
g. waarborgen dat de systeemdocumentatie na elke wijziging wordt geactualiseerd en dat oude documentatie wordt gearchiveerd of verwijderd;
h. versiebeheer uitvoeren voor alle programmatuur-updates;
i. bijhouden van een 'audit trail' van alle wijzigingsaanvragen;
j. waarborgen dat de bedrijfsdocumentatie en gebruikersprocedures worden veranderd zover noodzakelijk om toepasbaar te blijven;
k. waarborgen dat de implementatie van wijzigingen op het juiste moment plaatsvindt en de betrokken bedrijfsprocessen niet verstoort.

9.2.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem (ISO27001-A14.2.3)

ISO: Bij wijzigingen in besturingssystemen moeten bedrijfskritische toepassingen worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

Overweeg de volgende punten:

a. beoordelen van de toepassingbeheersmaatregelen en integriteitprocedures voor de toepassing om te waarborgen dat zij niet gecompromitteerd worden door de wijzigingen in het besturingssysteem;
b. waarborgen dat in het jaarlijkse onderhoudsplan en -budget rekening wordt gehouden met beoordeling en testen als gevolg van wijzigingen in het besturingssysteem;
c. waarborgen dat wijzigingen in het besturingssysteem tijdig worden aangekondigd, zodat de noodzakelijke tests en beoordelingen kunnen worden uitgevoerd voordat de wijzigingen worden geïmplementeerd;
d. waarborgen dat testplannen ontwikkeld worden of aanwezig zijn;

e. waarborgen dat de benodigde wijzigingen worden aangebracht in de bedrijfscontinuïteitsplannen (zie hoofdstuk 14).

Belast een speciale groep of persoon met de verantwoordelijkheid voor het controleren van zwakke plekken en van herstelprogramma's ('patches') en reparaties ('fixes') van leveranciers.

9.2.3 Beperkingen op wijzigingen in programmatuurpakketten (ISO27001-A14.2.4)

ISO: Wijzigingen in programmatuurpakketten moeten worden ontmoedigd, worden beperkt tot de noodzakelijke wijzigingen, en alle wijzigingen moeten strikt worden beheerst.

Gebruik zover mogelijk en praktisch uitvoerbaar kant-en-klaar geleverde (vendor supplied) programmatuur ongewijzigd. Houd waar wijzigingen in deze programmatuur noodzakelijk zijn rekening met de volgende punten:

a. het risico dat ingebouwde beheersmaatregelen en integriteitprocessen gecompromitteerd raken;
b. verkrijgen van toestemming van de leverancier;
c. de mogelijkheid de gewenste wijzigingen te verkrijgen van de leverancier, in de vorm van standaard programma-updates;
d. de impact op de organisatie als deze verantwoordelijk wordt gehouden voor toekomstig onderhoud van de programmatuur als gevolg van wijzigingen.

Overige regels:

e. Bewaar, indien wijzigingen noodzakelijk zijn, de oorspronkelijke programmatuur en breng de wijzigingen aan in een duidelijk gemarkeerde kopie.
f. Voer een beheerproces in voor programmatuur-updates om te waarborgen dat de meest recente goedgekeurde herstelprogramma's en updates van toepassingen voor alle goedgekeurde programmatuur zijn geïnstalleerd (zie 12.6.1).
g. Test en documenteer alle wijzigingen, zodat ze indien nodig opnieuw kunnen worden aangebracht in toekomstige upgrades van de programmatuur.
h. Laat indien vereist de testen valideren door een onafhankelijke beoordelingsinstantie.

9.2.4 Principes voor het bouwen van beveiligde systemen (ISO27001-A14.2.5)

ISO: Principes voor het bouwen van beveiligde systemen, moeten zijn vastgesteld, beschreven, onderhouden en worden toegepast.

a. Veilige informatie-systeem-engineeringprocedures gebaseerd op beveiligings-engineeringprincipes moeten worden opgesteld, gedocumenteerd en toegepast op interne informatie-systeem-engineeringactiviteiten.
b. Beveiliging moet worden ontworpen in alle architectuurlagen (business, data, applicaties en technologie) waarbij de behoefte aan informatiebeveiliging in balans wordt gebracht met de behoefte aan toegankelijkheid.
c. Nieuwe technologieën moeten worden geanalyseerd op beveiligingsrisico's en het ontwerp moet worden beoordeeld aan de hand van bekende aanvalspatronen.
d. Deze principes en de vastgestelde engineeringprocedures:
e. moeten regelmatig worden beoordeeld om ervoor te zorgen dat ze effectief bijdragen aan verbeterde normen van beveiliging binnen het engineeringproces.
f. moeten regelmatig worden beoordeeld om ervoor te zorgen dat ze up-to-date blijven in termen van het bestrijden van eventuele nieuwe potentiële bedreigingen en dat ze van toepassing blijven op vooruitgang in de toegepaste technologieën en oplossingen.

g. moeten worden toegepast, indien van toepassing, op uitbestede informatie-systemen via de contracten en andere bindende overeenkomsten tussen de organisatie en de leverancier aan wie de organisatie uitbesteedt. De organisatie moet bevestigen dat de striktheid van de beveiligings-engineeringprincipes van leveranciers vergelijkbaar is met die van henzelf.
h. Procedures voor applicatieontwikkeling moeten veilige engineeringtechnieken toepassen bij de ontwikkeling van applicaties die invoer- en uitvoerinterfaces hebben. Veilige engineeringtechnieken bieden richtlijnen voor gebruikersauthenticatietechnieken, beveiligde sessiecontrole en gegevensvalidatie, sanering en eliminatie van debugcodes.

9.2.5 Beveiligde ontwikkelingsomgeving (ISO27001-A14.2.6)

ISO: Organisatie moeten een beveiligde ontwikkelingsomgeving hebben ingericht voor de gehele levensloop van informatiesystemen.

De ontwikkelomgeving is een belangrijk onderdeel van een grote organisatie. Nieuwe IT-services moeten zich enerzijds ongestoord kunnen ontwikkelen, maar binnen de fasen van die ontwikkeling moet ongewenste beïnvloeding worden voorkomen. Ook de transitie van nieuwe functies naar het productiedomein moet gecontroleerd plaatsvinden. Vaak vindt de ontwikkeling van IT-services geheel of gedeeltelijk buiten de organisatie plaats.

Ontwikkeling van bedrijfsprocessen en IT-middelen moet kunnen plaatsvinden zonder ongewenste onderlinge beïnvloeding van de verschillende ontwikkelfasen en verantwoordelijkheden. In de ontwikkelomgeving gaat die beïnvloeding over de aantasting van de beoogde systeemintegriteit.
Binnen een zone kan data vrijelijk tussen systemen worden uitgewisseld. Wanneer echter uitwisseling tussen twee of meer zones nodig is, dan moet ergens een 'opening' worden gemaakt in de afscherming van de zones en dient er voor één of meerdere netwerkprotocollen een doorgang te worden gemaakt. Het openbreken van zones en rechtsreeks koppelen en uitwisselen van informatie introduceert een scala aan problemen, die beveiligingsrisico's kunnen veroorzaken:

Samengevat zijn de generieke problemen van koppelvlakken:
a. Het verschil in vertrouwensniveau van de zones vervalt bij een rechtstreekse (netwerk)koppeling waardoor het effectieve vertrouwensniveau gelijk is aan het laagste vertrouwensniveau van alle gekoppelde zones. Daardoor kan de vertrouwelijkheid van de informatie in zones met een oorspronkelijk hoger vertrouwensniveau niet meer worden gewaarborgd.
b. Rechtstreekse koppelingen van zones impliceert dat de individuele zones samengevoegd worden tot één logische zone. Daarbij vervalt de scheiding van verantwoordelijkheden voor de beveiliging binnen de individuele zones.
c. Met een rechtstreekse (netwerk)koppeling is er geen controle op- of beheersing mogelijk van de integriteit validiteit of classificatie van de uitgewisselde gegevens tussen de gekoppelde zones.

Per koppelvlak moeten de juiste beheersmaatregelen gekozen worden (zie ook: http://www.noraonline.nl/wiki/Patroon_voor_interne_koppelvlakken_voor_de_ontwikkelomgeving).

9.2.6 Uitbestede softwareontwikkeling (ISO27001-A14.2.7)

ISO: Uitbestede ontwikkeling van programmatuur moet onder supervisie staan van en worden gecontroleerd door de organisatie.
Houd, indien ontwikkeling van programmatuur wordt uitbesteed, rekening met de volgende punten:
a. licentieovereenkomsten, eigendom van de broncode en intellectuele eigendomsrechten;

b. certificatie van de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
c. zorgen voor een borg in geval een derde partij in gebreke blijft;
d. toegangsrechten voor het uitvoeren van een audit op de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
e. contractuele eisen voor de kwaliteit en beveiligingsfunctionaliteit van de broncode (o.a. escrow);
f. testen voorafgaand aan installatie, om eventuele kwaadaardige programmatuur te ontdekken.

9.2.7 Testen beveiligingsysteem (ISO27001-A14.2.8)

ISO: Beveiligingsfunctionaliteit moet getest worden tijdens systeemontwikkeling.

BELEID: ADEQUATE VERIFICATIEPROCEDURE
Alle verificaties moeten zijn uitgevoerd vóór de release.
Voordat het softwaresysteem wordt vrijgegeven, moeten alle verificaties zijn uitgevoerd op de versie van het softwaresysteem die zal worden vrijgegeven, en de verificatieresultaten mogen geen onaanvaardbare tekortkomingen onthullen in de beveiliging van het softwaresysteem.
Auditmethode: Bestudeer documentatie, zoals release-documentatie, testrapporten, rapporten van code reviews, enz.

9.2.8 Systeemacceptatie (ISO27001-A14.2.9)

ISO: Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.

Voor ingrijpende nieuwe ontwikkelingen is het van belang dat het operationeel beheer en de gebruikers worden betrokken bij alle fasen van het ontwikkelingsproces, om een doeltreffende werking van het voorgestelde systeemontwerp in de praktijk te waarborgen. Laat geschikte testen uitvoeren door het operationeel beheer en de gebruikers om te bevestigen dat ook aan hun acceptatiecriteria is voldaan.

Stem de omvang en diepgang van de testen af op de risico's, bepaald bij het voorbereiden van de wijziging.

Overweeg de volgende punten voordat formele acceptatie wordt verleend:
a. eisen aan prestaties en capaciteit van het computersysteem;
b. procedures voor foutherstel en herstart en continuïteitsplannen;
c. voorbereiding en testen van routinematige bedieningsprocedures volgens welomschreven normen;
d. de overeengekomen beveiligingsmaatregelen zijn geïmplementeerd;
e. doeltreffende handmatige procedures;
f. bedrijfscontinuïteitsplannen;
g. bewijs dat installatie van het nieuwe systeem geen nadelige invloed heeft op bestaande systemen, in het bijzonder tijdens de drukste verwerkingstijden;
h. bewijs dat aandacht is besteed aan de invloed van het nieuwe systeem op de algehele beveiliging van de organisatie;
i. opleiding in bediening of gebruik van nieuwe systemen.
j. gebruiksgemak, met het oog op effectiviteit van het gebruik en vermijden van menselijke fouten.

Een formeel certificatie- en accreditatieproces om te verifiëren dat de beveiligingseisen op de juiste wijze zijn aangepakt, kan deel uitmaken van de acceptatie.
Het is aan te raden om contracten met leverancier en/of de applicatie aanbiedende organisatie sluiten waarin het bovenstaande volledig is afgedekt. Voorbeelden van criteria zijn de termijn voor acceptatie, transparantie, functionele en gebruikerseisen.

9.2.9 Bescherming van testgegevens (ISO27001-A14.3.1)

ISO: Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.
Systeem- en acceptatietesten vereisen doorgaans grote hoeveelheden testgegevens, die een zo getrouw mogelijke weergave moeten zijn van operationele gegevens. Bij een acceptatietest kan het in uitzonderlijke gevallen noodzakelijk zijn de originele klantgegevens te gebruiken. Aanvullende maatregelen zijn dan nodig.

Vermijd gebruik van operationele databases met persoonlijke informatie of enige andere gevoelige informatie voor testdoeleinden. Verwijder, indien persoonlijke of anderszins gevoelige informatie wordt gebruikt voor testdoeleinden, eerst alle gevoelige details en inhoud, of pas deze aan zodat het onherkenbaar is. Overweeg de volgende richtlijnen ter bescherming van operationele gegevens als deze worden gebruikt bij testen:

a. gebruik de toegangsprocedures die voor besturingssystemen worden gebruikt ook voor testsystemen;
b. zorg ervoor dat telkens wanneer besturingsinformatie naar een testsysteem wordt gekopieerd, per keer autorisatie wordt verkregen;
c. wis besturingsgegevens onmiddellijk na beëindiging van de proef van het testsysteem;
d. registreer kopiëren en gebruik van besturingsgegevens om in een 'audit trail' te voorzien.

9.2.10 Herbeoordeling technische naleving (ISO27001-A14.3)

ISO: Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

Controle op naleving van technische normen omvat onderzoek van productiesystemen om te waarborgen dat maatregelen voor apparatuur en programmatuur correct zijn geïmplementeerd. Voor dit soort controles is technische ondersteuning van een deskundige vereist.

Controle op naleving van technische normen omvat verder bijvoorbeeld penetratieproeven en kwetsbaarheidsbeoordelingen die kunnen worden uitgevoerd door onafhankelijke deskundigen die speciaal voor dit doel worden ingehuurd. Een dergelijke controle kan nuttig zijn om zwakke plekken in het systeem te ontdekken en om te controleren hoe doeltreffend de beheersmaatregelen zijn bij het voorkómen van onbevoegde toegang als gevolg van deze zwakke plekken.

a. Voer controle uit op naleving van technische normen, ofwel handmatig door een ervaren systeemtechnicus (zonodig met ondersteuning van geschikte programmatuurhulpmiddelen) ofwel automatisch met behulp van geautomatiseerde hulpmiddelen waarmee een technisch rapport wordt gegenereerd dat vervolgens door een technisch deskundige wordt geïnterpreteerd.
b. Indien penetratieproeven of kwetsbaarheidsbeoordelingen worden toegepast, is voorzichtigheid geboden, daar deze activiteiten kunnen leiden tot compromittering van de beveiliging van het systeem. Plan en documenteer zulke testen en maak ze herhaalbaar.
c. Laat controle op naleving van technische normen uitsluitend uitvoeren door gekwalificeerde, bevoegde personen of onder toezicht van zo een persoon.

Let op:
Penetratieproeven en kwetsbaarheidsbeoordelingen geven een momentopname van een systeem in een bepaalde toestand op een bepaald tijdstip. De momentopname blijft beperkt tot die delen van het systeem die werkelijk zijn getest tijdens de penetratiepoging(en). Penetratieproeven en kwetsbaarheidsbeoordelingen zijn geen vervanging van een risicobeoordeling.