Versie april 2023

Bit by Bit

Samen voor digitaal veilig onderwijs

Normenkader informatiebeveiliging en privacy

voor het Funderend Onderwijs

Ministerie van Onderwijs, Cultuur en Wetenschap

Kennisnet

SIVON

PO RAAD

VO RAAD

Inleiding

Als samenleving komen we vandaag de dag veelvuldig in aanraking met gevoelige informatie en gegevens. Het beschermen van met name persoonlijke gegevens is in het onderwijs van cruciaal belang. Deze sector heeft tenslotte te maken met een minderjarige doelgroep. Leerlingen, maar ook ouders en medewerkers vertrouwen hun gegevens toe aan onderwijsinstellingen. Doordachte gegevensverwerking én goede gegevensbeveiliging vallen dan ook onder de verantwoordelijkheid van schoolbesturen en hun medewerkers.

Met het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken. Met dat doel in gedachten ontwikkelen we het Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs (IBP FO). Met dit hulpmiddel kunnen schoolbesturen toewerken naar sterkere informatiebeveiliging en betere bescherming van persoonsgegevens. Onder informatiebeveiliging verstaan we 'het behoud van vertrouwelijkheid, integriteit en beschikbaarheid van informatie'.

Structuur

Het normenkader bevat beschrijvende normen over informatiebeveiliging en privacy. Deze zijn onderverdeeld in vijftien domeinen voor informatiebeveiliging en een domein voor privacy, die met elkaar samenhangende normen bevatten. De normen voor privacy zijn op dit moment nog in ontwikkeling. Elk domein van het normenkader begint met een inleiding. Daarin staat een korte uitleg over het domein, worden relevante begrippen uitgelegd en staat beschreven wie verantwoordelijk zijn voor de uitvoering. Functionarissen zijn hierin met algemene titels omschreven. Zie aanpakibp.kennisnet.nl/rollen-en-verantwoordelijkheden voor toepasselijke titels in je eigen organisatie. Ook benoemen we de hulpmiddelen (zoals handreikingen en formats) die jou hierbij kunnen ondersteunen.

Norm

Per domein staan vervolgens de betreffende normen beschreven. De codering die erbij staat is een verwijzing naar het NBA-model waarop dit kader zich baseert. Over dit model lees je meer op de volgende pagina van deze inleiding. Elke norm is voorzien van een korte toelichting, onder de noemer 'Waarom doen we dit? Zo wordt duidelijker waarop schoolbesturen op het gebied van informatiebeveiliging en privacy moeten letten om continuïteit, kwaliteit en veiligheid van onderwijs te borgen.

Privacynormen
In de onderwijssector bestaat nog geen leidend kader voor privacynormen. Daarom ontwikkelen we die zelf. We baseren ons op het werk dat de Vereniging Nederlandse Gemeenten hiervoor al gedaan heeft. Samen met onderwijsinstellingen en het hoger onderwijs en mbo maken we dit toepasbaar voor onze sectoren. We verwachten deze later dit jaar te publiceren.

Toetsingskader
Bij elke norm hoort een toetsingskader. Het toetsingskader beschrijft het minimumniveau waar we als sector naartoe werken. Dit niveau is de ondergrens; méér doen mag. Het is jouw verantwoordelijkheid om hier op basis van actuele risico's een afweging in te maken.

Voorbeeldmaatregelen
Steeds meer onderwijsinstellingen nemen concrete maatregelen op het gebied van digitale veiligheid. Daarom staan bij elke norm voorbeeldmaatregelen die je kunt nemen om te werken aan digitale veiligheid. Er staan concrete handvatten beschreven om aan het wenselijke minimumniveau te (kunnen gaan) voldoen. De voorbeeldmaatregelen helpen schoolbesturen om invulling te geven aan het normenkader. Zij zijn vrij om te bepalen of ze gebruikmaken van de voorbeeldmaatregelen. Wel geldt: als je álle voorbeeldmaatregelen neemt en goed uitvoert, voldoe je aan het minimumniveau.

Ondersteuning
Kennisnet, SIVON, de PO-Raad en de VO-raad ontwikkelen ondersteunende documentatie (zoals formats en handreikingen), om te voorkomen dat schoolbesturen het wiel opnieuw moet uitvinden. Zie hiervoor: aanpakibp.kennisnet.nl. Daar waar nog geen ondersteuning beschikbaar is, realiseren de vier partijen aanvullende ondersteuning. Denk hierbij aan gemeenschappelijk leveranciersmanagement en technische voorzieningen om de veiligheid te borgen. Hiervoor is de Funderend Onderwijs Referentie Architectuur (FORA) al beschikbaar. Nog niet alle formats en handreikingen zijn gereed of helemaal aangepast aan het normenkader. Deze worden de komende periode in samenwerking met schoolbesturen ontwikkeld.

Groeipad
Waar begin je? Op basis van de risico's die schoolbesturen lopen, wordt er de komende periode vanuit het programma gewerkt aan een realistisch groeipad. Waar lopen scholen het meeste risico en waar staan zij nu? Op basis van een actueel dreigingsbeeld en een sectorale nulmeting wordt er informatie verzameld om dit groeipad voor de sector op te stellen. Op basis van dit groeipad gaan we scholen actief helpen met landelijke ondersteuning. Zolang dit groeipad er niet is, kunnen schoolbesturen beginnen met het nemen van maatregelen voor de 'basis op orde', denk aan de normen uit hoofdstuk 1 (norm 1.1 en 1.2). Heb je deze normen al goed op orde, ga dan verder. Heb je deze normen al goed op orde, kijk dan in deze tabel welke stappen je verder kan zetten.

BIJ DEZE VERSIE (APRIL 2023)

Deze versie van het normenkader is tot stand gekomen onder aansturing van het programma Digitaal Veilig Onderwijs. Zoals aangegeven zijn de normen voor privacy nog in ontwikkeling.

Het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs (IBP FO) is gebaseerd op het NBA Volwassenheidsmodel voor informatiebeveiliging. Dit model is afkomstig van de Nederlandse Beroepsorganisatie van Accountants en is tegenwoordig bekend onder naam NBA-LIO (Ledengroep Intern en Overheidsaccountants). De normen en het toetsingskader zijn vervolgens toepasbaar gemaakt voor de onderwijssector. Ook het hoger onderwijs en middelbaar beroepsonderwijs hanteren het NBA-model als uitgangspunt voor hun IBP-kader. De formulering van de normen en het minimumniveau zijn een zoveel mogelijk letterlijke vertaling van het Engelstalige NBA-kader. Dit maakt het taalgebruik hier en daar erg formeel, maar zo zorgen we ervoor dat iedereen op één lijn zit en dat Kennisnet, SIVON, de PO-Raad en de VO-raad gerichte ondersteuning kunnen bieden.

Samen met IBP'ers van diverse onderwijsinstellingen uit het primair en voortgezet onderwijs is het normenkader bediscussieerd, van toelichting voorzien en toepasbaar gemaakt voor de sector. Het advies van experts om voor alle normen volwassenheidsniveau 3 uit het NBA-model te hanteren is in deze versie overgenomen. De werkgroep heeft bij enkele normen andere adviezen gegeven over het niveau. De werkgroep heeft een belangrijke rol gehad in het opstellen van de voorbeeldmaatregelen die genomen kunnen worden om het minimumniveau te behalen.

Het is voor schoolbesturen een flinke klus om aan het normenkader te voldoen. In het bijzonder voor kleinere schoolbesturen lijken de beschreven niveaus en maatregelen soms ver van de praktijk af te staan. Dit zou in een volgende versie van het normenkader kunnen leiden tot verduidelijkingen en nieuwe voorbeeldmaatregelen.

Een levend document
Het normenkader is een levend document, steeds gebaseerd op de nieuwste kennis en ontwikkelingen. Door er in de sector daadwerkelijk mee te gaan werken, ontdekken we wat er (nog) beter beschreven kan worden. We vragen schoolbesturen om hun suggesties te delen via ibp@kennisnet.nl. Zo verbeteren we samen het normenkader en de informatiebeveiliging in de onderwijssector.

Inhoud

Deel 1

Normenkader informatiebeveiliging

Naar Normenkader informatiebeveiliging

Deel 2

Normenkader privacy

Naar Normenkader privacy

Deel 1

Normenkader informatiebeveiliging

1 Bestuur

Welke onderwerpen staan in dit domein?
In het domein Bestuur zijn vijf normen opgenomen. Deze normen geven richting en ondersteuning om de informatiebeveiliging in te richten in lijn met organisatie-doelstellingen, risicobereidheid en wet- en regelgeving. Ze gaan over de naleving van het normenkader. Met andere woorden: de normen binnen dit domein vormen belangrijke kaders voor de invulling van de normen uit de andere domeinen.

Allereerst is het nodig om je strategie en visie voor informatiebeveiliging te bepalen. Op basis daarvan bepaal je het informatiebeveiligingsbeleid. Als afgeleide van je beleid maak je periodiek informatiebeveiligingsplannen die zorgdragen voor verbetering van je informatiebeveiliging. Vervolgens is er een Enterprise Architectuur die inzicht in en overzicht over de organisatiestructuur en de informatievoorziening geeft en helpt om op verantwoorde wijze veranderingen door te voeren. De laatste norm binnen dit domein gaat over het (laten) toetsen van hoe je er als organisatie voor staat op het gebied van informatiebeveiliging, met als doel inzicht te krijgen in verbetermogelijkheden om risico's te verkleinen.

Wie is verantwoordelijk?

Voor alle onderdelen binnen dit domein geldt dat het bevoegd gezag eindverantwoordelijkheid draagt. Wanneer het gaat over zaken als strategie en beleid, dan zal de voorbereiding meestal gebeuren door een adviseur op het gebied van informatiebeveiliging binnen de organisatie. Deze stemt af met functionarissen als de FG, en de verantwoordelijken voor IBP en IT. Het bevoegd gezag stelt de naleving van informatiebeveiliging vast en is daarvoor ook verantwoordelijk. Medewerkers binnen de organisatie worden geïnformeerd over de zaken die hen aangaan, zoals het informatiebeveiligingsbeleid. In opdracht van het bevoegd gezag voeren interne en/of externe auditors het toezicht op naleving uit. De audit zelf wordt vaak voorbereid door de IBP-coördinator.

Ondersteuningsproducten

Beschikbaar:

- Template *IBP-beleidsplan* (zie Aanpak IBP)
- Toelichting op het template IBP-beleidsplan (zie Aanpak IBP)
- *Funderend Onderwijs Referentie Architectuur* (FORA)

In ontwikkeling/te ontwikkelen:

- Handreiking en format *Strategie en visie*
- Handreiking *Jaarlijkse aandacht voor informatiebeveiliging en privacy*
- Handreiking *Functiebeschrijving informatiemanagement*
- Handreiking *Architectuur*
- Audit-as-a-service

1.1 Strategie

NORM

GO.01
Een strategie en visie op informatie- en cybersecurity is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.

Waarom doen we dit?
Het hebben van een strategie leidt tot gepaste zakelijke en beveiligingsbeslissingen, tot samenhang in beveiligingsbeslissingen en tot een passend antwoord op veranderingen in de bedrijfsomgevingen.

TOETSINGSKADER

- Strategie en visie zijn goedgekeurd door het bevoegd gezag.
- Strategie en missie worden actief gecommuniceerd naar medewerkers, leveranciers en businesspartners.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een strategie en visie geformuleerd op informatie-beveiliging en cybersecurity. De opbouw van deze strategie en visie bevat de elementen die aangereikt worden in de Handreiking *Strategie en Visie* vanuit het ondersteuningsaanbod. Er kan gebruikgemaakt worden van het Format Strategie en Visie.
2. Het bevoegd gezag heeft de strategie en visie vastgesteld.
3. De strategie en visie zijn (digitaal) beschikbaar, bijvoorbeeld via de website en het intranet.

1.2 Beleid

NORM

GO.02

De organisatie heeft een (informatie)beveiligingsbeleid vastgesteld, beschreven en gecommuniceerd met medewerkers. Indien van toepassing wordt het beleid ook actief meegedeeld aan leveranciers en contractpartners. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het senior management.

Waarom doen we dit?

Met een beleid zijn er vastgestelde richtlijnen om te voldoen aan de wet- en regelgeving en/of interne informatiebeveiligingseisen. Door dit te communiceren aan medewerkers en leveranciers, is voor iedereen duidelijk binnen welke kaders zij geacht worden te handelen.

TOETSINGSKADER

- Informatiebeveiligingsbeleid is goedgekeurd door het bevoegd gezag.
- Beleid wordt actief gecommuniceerd naar medewerkers, leveranciers en contractpartners en is digitaal (op intranet) of in hard copy beschikbaar.
- Het beleid maakt onderdeel uit van het security awareness-programma .
- Het voldoen aan beleid wordt geëvalueerd.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een informatiebeveiligingsbeleid opgesteld dat voldoet aan de eisen zoals verwoord in de *Toelichting op het template IBP-beleidsplan*. Het schoolbestuur kan hiervoor gebruikmaken van het *Template IBP-beleid*.
2. Het bevoegd gezag heeft het beleid vastgesteld, blijkend uit een handtekening op het document of notulen van een bestuursvergadering.
3. Tenminste eens per twee jaar vindt een controle plaats of er wijzigingen nodig zijn in het informatiebeveiligingsbeleid. De controle wordt vastgelegd in het document met eventuele wijzigingen die zijn doorgevoerd.
4. Ten minste een keer per jaar wordt er op elke individuele school behorend tot het schoolbestuur in een teamoverleg gesproken over het plan conform Handreiking *Jaarlijkse aandacht voor informatiebeveiliging en privacy*. Doel hiervan is onder meer om te zien of het beleid toereikend is en of het gevolgd wordt binnen de organisatie.
5. Het beleid is goed vindbaar op intranet geplaatst.
6. Elke medewerker wordt tijdens het onboardingsproces geïnformeerd over het informatiebeveiligingsbeleid.
7. Waar nodig en relevant wordt het informatiebeveiligingsbeleid bij uitbesteding van dienstverlening meegenomen in de eisen.

1.3 Planning/Roadmap

NORM

GO.03
Bedrijfsdoelstellingen, risico's en compliance-eisen worden vertaald in een algemeen informatie-beveiligingsplan en/of cybersecurityplan, rekening houdend met de IT-infrastructuur en de veiligheidscultuur.

Waarom doen we dit?
Een informatiebeveiligingsplan en/of cybersecurityplan beschrijft de wijze waarop de organisatie gaat zorgen voor verbetering in overeenstemming tussen informatiebeveiliging en bedrijfsdoelstellingen, risico's en compliance-eisen.

TOETSINGSKADER

- Het plan of de roadmap is goedgekeurd door het bevoegd gezag.
- Het plan is uitgewerkt in (informatie)beveiligingsbeleid en -procedures, tezamen met passende investeringen op het gebied van diensten, personeel, software en hardware.
- Gerelateerde procedures worden gecommuniceerd naar gebruikers en stakeholders.

VOORBEELDMAATREGELEN

1. Elk jaar wordt een jaarplan informatiebeveiliging opgesteld waarin staat welke acties dat jaar uitvoering geven aan het informatiebeveiligingsbeleid, dan wel verbeteringen doorvoeren om te voldoen aan het beleid. Dit jaarplan kan onderdeel uitmaken van het bestuurbrede jaarplan.
2. Het bevoegd gezag stelt het jaarplan vast en zorgt voor de benodigde middelen.
3. Aan het einde van een jaar wordt uitvoering geëvalueerd. De punten uit de evaluatie worden waar nodig meegenomen in het volgende jaarplan.

1.4 Architectuur

NORM

GO.04

Er is een Enterprise Information Architecture Model (EIAM) opgesteld en toegepast om applicatieontwikkeling en beslissingsondersteunende activiteiten mogelijk te maken, conform informatie- of IT-plannen. Dit model moet het mogelijk maken om effectief, veilig en op een robuuste manier informatie te creëren, te gebruiken en te delen zoals wordt vereist door bedrijfsdoelstellingen en wettelijke voorschriften.

Waarom doen we dit?

Het hebben van een architectuur helpt bij het tijdig en goed reageren op zakelijke of juridische veranderingen en/of (externe) dreigingen die een (mogelijke) aanpassing in de informatiehuishouding vragen. Denk hierbij bijvoorbeeld aan de implementatie van de AVG een aantal jaar terug; een EIAM biedt snel inzicht in waar welke gegevens verwerkt worden en hoe deze met elkaar verbonden zijn. Door dit inzicht is het gemakkelijker om de juiste acties te bepalen om hieraan te voldoen.

TOETSINGSKADER

- Er is een baseline voor de huidige (IST) en de beoogde architectuur (SOLL) gedefinieerd.
- De beoogde architectuur is in overeenstemming met de organisatiebrede doelstellingen (inclusief de naleving van wettelijke voorschriften) en de organisatorische verantwoordelijkheden.
- Het EIAM en de relevante processen zijn gedefinieerd en worden toegepast om applicatieontwikkeling en beslissingsondersteunende activiteiten in overeenstemming met de informatie- of IT-plannen mogelijk te maken.
- Het EIAM is goedgekeurd door het bevoegd gezag.

VOORBEELDMAATREGELEN

1. Er is iemand binnen de organisatie die informatiemanagement en daarmee architectuur in het functiepakket heeft zitten (dit zal veelal een rol zijn voor de kleinere organisaties en geen volledige functie). Voor het aanstellen hiervan kan gebruikgemaakt worden van de Functiebeschrijving Informatiemanagement.
2. Het bevoegd gezag stelt FORA vast als referentie-architectuur.
3. Op basis van FORA is een organisatiespecifieke architectuur opgesteld. Ook deze wordt vastgesteld door het bevoegd gezag. Hierbij wordt gebruikgemaakt van de Handreiking *Architectuur*.
4. Bij wijzigingen in het informatielandschap wordt de architectuur gebruikt om te toetsen wat de gewenste oplossingsrichting is.

1.5 Onafhankelijke assurance

NORM

GO.05

Onafhankelijke assurance (intern of extern) wordt verkregen om te bepalen in hoeverre de informatievoorziening (inclusief IT) voldoet aan relevante wet- en regelgeving, het beleid van de organisatie, de normen en procedures van de organisatie, algemeen aanvaarde werkwijzen en effectieve en efficiënte prestaties van IT.

Waarom doen we dit?

Door middel van onafhankelijke assurance komt in beeld waar de realiteit afwijkt van het beleid en voorkom je dat onbekende risico's kunnen blijven bestaan.

TOETSINGSKADER

- Onafhankelijke assurance (intern of extern) wordt verkregen ten aanzien van het voldoen van de informatievoorziening (inclusief. IT) aan relevante wet- en regelgeving, beleid, standaarden, procedures binnen de organisatie en algemeen aanvaarde werkwijzen.
- De activiteiten voor het verkrijgen van assurance zijn beschreven in een auditplan dat is goedgekeurd door het bevoegd gezag en een auditcommissie.
- De resultaten van deze activiteiten worden gerapporteerd aan het bevoegd gezag en de auditcommissie.
- Ingevulde checklists die worden gebruikt bij de controle zijn beschikbaar.

VOORBEELDMAATREGELEN

1. Het bevoegd gezag stelt een auditplan vast waarin beschreven staat welke onderdelen wanneer getoetst worden en of dit door een interne of externe auditor gebeurt. De richtlijn is dat ten minste eens per drie jaar het gehele normenkader getoetst moet worden.
2. Elke audit gaat gepaard met een *prepared-by-client*-lijst, opgesteld door de auditor, die zorgvuldig voorbereid wordt door het betreffende schoolbestuur.
3. De auditresultaten worden besproken door het bevoegd gezag en hierop wordt een actieplan geformuleerd. Het bevoegd gezag stuurt op het actieplan totdat alle bevindingen conform plan zijn opgelost.

2 Organisatie

Welke onderwerpen staan in dit domein?
Het is belangrijk om informatiebeveiliging op de juiste wijze vorm te geven binnen de organisatie. De medewerkers op het hoogste niveau binnen de organisatie dragen een belangrijke verantwoordelijkheid. Zij zijn dan ook degenen die afwegingen dienen te maken voor informatiebeveiliging, zoals risicobereidheid en kosten-batenanalyses.

Ook voor medewerkers in andere lagen van de organisatie is het van belang dat zij weten welke verantwoordelijkheid zij hebben ten aanzien van informatiebeveiliging. Het is dus noodzakelijk om de rollen en verantwoordelijkheden goed te beschrijven en ze in te bedden in de organisatie. Een belangrijk onderdeel hiervan is het zorgen voor functiescheiding. Hiermee voorkom je dat iemand bepaalde acties kan uitvoeren die een potentieel risico voor de organisatie zijn (niet alleen bewuste acties, maar ook menselijke fouten).

Wie is verantwoordelijk?

Voor alle onderdelen binnen dit domein geldt dat uiteindelijk het bevoegd gezag de eindverantwoordelijkheid draagt. Wanneer het gaat over het beschrijven van de informatiebeveiligingsorganisatie en functiescheiding, dan zal de voorbereiding meestal gebeuren door een adviseur op het gebied van informatiebeveiliging binnen de organisatie. Deze stemt af met functionarissen als de FG en de verantwoordelijken voor IBP en IT. Het bevoegd gezag stelt de inbedding van de organisatie vast en is hiervoor ook verantwoordelijk. Medewerkers binnen de organisatie worden geïnformeerd over de zaken die hen aangaan, in dit geval bijvoorbeeld wanneer ze een specifieke verantwoordelijkheid hebben ten aanzien van informatiebeveiliging.

Ondersteuningsproducten

Beschikbaar:

- Template *IBP-beleidsplan* (zie Aanpak IBP)

In ontwikkeling/te ontwikkelen:

- Format *Intentieverklaring*
- Handreiking *Beleid logische toegangsbeveiliging*

2.1 Eigenaarschap, rollen, verantwoording en verantwoordelijkheid

NORM

OR.01
Informatiebeveiliging wordt beheerst op alle toepasselijke organisatieniveaus en informatiebeveiligings- (of informatierisico)management wordt beheerst in overeenstemming met business requirements/risico's. Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zijn formeel toegewezen en ingebed in de organisatie.

Waarom doen we dit?

Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zorgen voor een effectieve besluitvorming en resulteren in een betrouwbaar management over informatiebeveiliging. Ook staat op deze manier zakelijke belangenafweging centraal in keuzes over informatiebeveiliging.

TOETSINGSKADER

- Alle rollen op het gebied van het managen van informatierisico's zijn vastgesteld en toegewezen.
- De verantwoordelijkheid (en aansprakelijkheid) voor informatierisico- en veiligheidsmanagement is op organisatieniveau vastgesteld en behandelt organisatiebrede kwesties.
- Er is een intentieverklaring van het bevoegd gezag die de doelen en uitgangspunten van informatiebeveiliging en informatierisicobeheer ondersteunen en in overeenstemming zijn met de strategie en organisatiedoelstellingen.
- De governancestructuur is gedocumenteerd met daarin opgenomen de verantwoordelijkheden en rapportagestructuur.

VOORBEELDMAATREGELEN

1. Rollen, verantwoordelijkheden en governancestructuur voor informatiebeveiliging zijn opgenomen in het IBP-beleid.
2. Het schoolbestuur heeft een intentieverklaring opgesteld. Het schoolbestuur kan hiervoor gebruikmaken van het Format *Intentieverklaring*.

2.2 Functiescheiding

NORM

OR.02

Rollen en verantwoordelijkheden zijn gescheiden om de kans te verkleinen dat individuele personen kritieke processen in gevaar brengen. Het personeel voert alleen geautoriseerde taken uit die bij hun respectievelijke functies en rol horen.

Waarom doen we dit?

Functiescheiding is van belang om te voorkomen dat acties van eenlingen (bijvoorbeeld het ongeautoriseerd toegang hebben tot of wijzigen van gegevens) zich kunnen voordoen met een negatief gevolg, bijvoorbeeld door nalatig of opzettelijk misbruik van het systeem.

TOETSINGSKADER

- De scheiding van rollen en verantwoordelijkheden is gedefinieerd en grotendeels geïmplementeerd, wat de kans verkleint dat individuen essentiële processen kunnen compromitteren.
- De scheiding van verantwoordelijkheden is goedgekeurd door het bevoegd gezag.
- Vastgestelde functiescheiding is geïmplementeerd, zodat personeel alleen geautoriseerde handelingen kan verrichten behorend bij hun werkzaamheden.

VOORBEELDMAATREGELEN

1. Er is een matrix van wel en niet toegestane combinaties van taken beschikbaar. Het schoolbestuur kan hiervoor gebruikmaken van de Handreiking *Beleid Logische Toegangsbeveiliging*. Deze matrix bevat een overzicht van wel en niet toegestane combinaties van autorisaties binnen een informatiesysteem, die aan één medewerker mogen worden toegekend. Principes die hierbij gelden:
   a. De beschikkende, bewarende en controlerende taken worden in beginsel nooit in één functionaris tezamen gebracht. Indien dit toch noodzakelijk is dan wordt door de systeemeigenaar apart toezicht georganiseerd op de betreffende functionaris.
   b. (Technische) beheerders mogen geen toegang hebben tot de data van het informatiesysteem waar zij (technisch) beheerder van zijn. Indien dit toch noodzakelijk is dan wordt door de systeemeigenaar apart toezicht georganiseerd op de betreffende functionaris.

3 Risicomanagement

Welke onderwerpen staan in dit domein?
Dit domein bevat de normen die bijdragen aan het op gestructureerde wijze identificeren en beheersen van risico's op het gebied van informatiebeveiliging. Daarvoor is het nodig om in een raamwerk of beleid te beschrijven hoe risicomanagement wordt toegepast binnen de organisatie en wie daar allemaal een rol in hebben. En om vervolgens periodiek te toetsen hoe het ervoor staat op het gebied van risico's.

Nadat risico's geïdentificeerd zijn, dient besloten te worden hoe daarmee wordt omgegaan. Tref je bijvoorbeeld maatregelen en stuur je dan op het nemen van die maatregelen? Of besluit je juist dat het een acceptabel (rest)risico is of dat de kosten van het nemen van maatregelen niet opwegen tegen de baten ervan? Kortom, risicomanagement is niet zozeer gericht op het wegnemen van alle risico's, maar op het identificeren ervan en het formuleren van een juiste aanpak.

Wie is verantwoordelijk?

Voor alle onderdelen binnen dit domein geldt dat uiteindelijk het bevoegd gezag de eindverantwoordelijkheid draagt voor de implementatie van de normen. Ook in het risicomanagementproces zelf dragen zij een belangrijke verantwoordelijkheid. Het bevoegd gezag bepaalt immers welke risicobereidheid er is en of risico's geaccepteerd worden, of dat er juist middelen komen om maatregelen te nemen. Het bevoegd gezag laat de voorbereiding van deze besluitvorming vaak uitvoeren door een verantwoordelijke voor IBP of – bij grotere organisaties – een adviseur risicomanagement. Deze medewerkers bewaken vaak het proces en zorgen voor de uitvoering. Iedereen in een managementpositie draagt zorg voor het uitvoeren van risicomanagement binnen zijn of haar aandachtsgebied.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Handreiking *Risicomanagement*
- Training *Risicomanagement*
- Format *Risicoregister*

3.1 Raamwerk voor informatierisico-management

NORM

RM.01
Er is een raamwerk voor informatierisicomanagement opgesteld en afgestemd op de doelstellingen van de organisatie en het raamwerk voor organisatierisicomanagement.

Waarom doen we dit?

Het raamwerk voor informatierisicomanagement helpt bij het goed uitvoeren van analyses, het juist interpreteren van de risico's en het opstellen van beheersmaatregelen.

TOETSINGSKADER

- Er is organisatiebreed (informatie)risicomanagementbeleid dat is goedgekeurd door het bevoegd gezag.
- Het beleid en de procesbeschrijving geven aan hoe om te gaan met de essentiële elementen van risicomanagement (risicobereidheid/risicoprofiel, eigenaarschap, risico-proces, bepalen, mitigeren en accepteren).
- Het kader voor informatierisico's is in lijn met het kader voor organisatiebreed risico-management en omvat componenten als strategie, programma's, projecten en uitvoering.
- Classificatie van informatierisico's gebeurt op basis van een set van algemeen geldende karakteristieken vanuit het organisatiebrede raamwerk voor risicomanagement en getroffen maatregelen voor informatierisico's zijn gestandaardiseerd en geprioriteerd, waarbij rekening gehouden wordt met kans, impact en restrisico's.
- Training in het kader van dit risicokader is geïmplementeerd.

VOORBEELDMAATREGELEN

1. Risicomanagement maakt onderdeel uit van het informatiebeveiligingsbeleid (zie norm 1.2).
2. In de Handreiking *Risicomanagement* staat beschreven welke zaken procesmatig aandacht behoren te krijgen en op welke wijze hier invulling aan wordt gegeven. Het schoolbestuur volgt deze handreiking voor de verdere invulling van risico-management binnen de kaders van het beleid.
3. Ten minste de IBP-coördinator heeft een training gevolgd om uitvoering te geven aan risicomanagement.

3.2 Risicobeoordeling

NORM

RM.02

Risicobeoordelingen worden uitgevoerd om actuele risicoprofielen met betrekking tot bedrijfsdoelstellingen te bepalen. De waarschijnlijkheid en impact van alle geïdentificeerde risico's worden regelmatig beoordeeld, met behulp van kwalitatieve en kwantitatieve methoden. De waarschijnlijkheid en impact van inherente en restrisico's worden bepaald per categorie, op portfoliobasis.

Waarom doen we dit?

Risicobeoordelingen ondersteunen bij het tijdig en juist opstellen van actieplannen, risico-initiatieven en het invoeren van beheersmaatregelen. Met een risicobeoordeling brengt een organisatie de risico's in kaart ten opzichte van de bedrijfsdoelstellingen. Alleen als de bedrijfsdoelstellingen in het geding zijn, spreken we van een risico, en risico's worden beoordeeld op hun potentiële impact op die bedrijfsdoelstellingen.

TOETSINGSKADER

- Door duidelijke en passende instructies vinden risicoanalyses consistent en herhaaldelijk plaats, als onderdeel van het risicomanagementproces en het raamwerk voor risico-management.
- De risicoanalysemethode is in lijn met bedrijfsbehoeften en identificeert belangrijke bedrijfsrisico's (inclusief kroonjuwelen).
- De geïdentificeerde risico's worden kwalitatief en/of kwantitatief beoordeeld, gebruik-makend van het risicomanagementproces/-raamwerk of *good practice* bronnen..
- Afwijkingen van de risicobereidheid of het risicoprofiel met betrekking tot risicobeperkende maatregelen worden aan het bevoegd gezag gerapporteerd.

VOORBEELDMAATREGELEN

1. De Handreiking *Risicomanagement* beschrijft de wijze waarop risicoanalyses uitgevoerd kunnen worden. Het schoolbestuur gebruikt deze handreiking voor het uitvoeren van de risicoanalyses.
2. De belangrijkste risico's worden periodiek besproken met het bevoegd gezag.

3.3 Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)

NORM

RM.03

Beheersactiviteiten worden op alle niveaus geprioriteerd en gepland om de benodigde mitigerende maatregelen te implementeren, inclusief het bepalen van kosten en baten en de verantwoordelijkheid voor de uitvoering. Goedkeuring wordt verkregen voor aanbevolen acties en acceptatie van restrisico's en er wordt voor gezorgd dat uitgevoerde acties onder verantwoordelijkheid van betrokken proceseigenaar(s) vallen. De uitvoering van plannen wordt bewaakt en eventuele afwijkingen worden gerapporteerd aan het bevoegd gezag.

Waarom doen we dit?

Met beheersactiviteiten worden de waarschijnlijkheid en impact van risico's gereduceerd. Door het prioriteren van risico's en het invoeren van beheersactiviteiten kunnen hoge kosten en andere negatieve gevolgen die gepaard gaan met de manifestatie van risico's worden verminderd.

TOETSINGSKADER

- Er is een proces geïmplementeerd om risico's formeel vast te leggen en op te nemen in een risico-actieplan.
- Overgebleven risico's en maatregelen zijn geïdentificeerd, geanalyseerd en gedocumenteerd (in een risicoregister of -actieplan).
- De geïdentificeerde maatregelen of acceptatie van overgebleven risico's zijn gedocumenteerd, goedgekeurd door het bevoegd gezag en toegewezen aan een (risico) eigenaar.
- De voortgang van implementatie van risicobeperkende maatregelen en eventuele afwijkingen worden gemonitord.
- Het risico-actieplan wordt onderhouden en aangepast indien nodig. Het bevoegd gezag is eigenaar van het risico-actieplan.

VOORBEELDMAATREGELEN

1. De geconstateerde risico's uit de risicoanalyses worden vastgelegd in een register. Hierbij kan gebruikgemaakt worden van het Format *Risicoregister*.
2. Per risico staat beschreven welke maatregelen genomen zullen worden en wat het restrisico is. Het bevoegd gezag geeft goedkeuring voor het al dan niet nemen van de maatregelen.
3. Het doorvoeren van de maatregelen wordt actief gemonitord en en waar nodig bijgestuurd.

4 Personeelsbeheer

Welke onderwerpen staan in dit domein?
In het domein Personeelsbeheer staan de normen die direct betrekking hebben op de medewerkers binnen een organisatie. Dit beslaat de hele cyclus van personeelsbeheer. Bij de werving van medewerkers met een verantwoordelijkheid op het gebied van informatiebeveiliging wordt aandacht besteed aan het binnenhalen van medewerkers die toegerust zijn voor de taak. Medewerkers die in de organisatie zitten krijgen de benodigde opleiding om informatiebeveiligingskennis op peil te houden, en de organisatie bereidt zich voor op het vertrek van medewerkers die op een cruciale plek zitten (sleutelfunctionarissen) bij wie vertrek een risico is voor de continuïteit van de organisatie.

Tot slot is er aandacht voor kennisborging en kennisoverdracht. Behalve in- en uitstroom gaat het binnen dit domein ook over kennisdeling die bijdraagt aan het goed en veilig gebruiken van systemen en het zorgen voor beveiligingsbewustzijn bij alle medewerkers, dus niet alleen die medewerkers die een speciale verantwoordelijkheid hebben op het gebied van informatiebeveiliging.

Wie is verantwoordelijk?

Hoewel ook hier het bevoegd gezag een eindverantwoordelijkheid draagt, komt hier ook de verantwoordelijke voor HR binnen de organisatie nadrukkelijk in beeld. De verantwoordelijke voor HR zorgt dat er aandacht is voor het borgen van deze aspecten. Deze medewerker kan hiervoor hulp krijgen van de verantwoordelijke voor IBP om te bepalen wat er precies nodig is. Ook de verantwoordelijke voor IT heeft een nadrukkelijke verantwoordelijkheid voor de norm die gaat over voldoende kennisdeling aan gebruikers. Tot slot wordt awareness voor alle medewerkers qua uitvoering meestal belegd bij de verantwoordelijke voor IBP.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Bewustwordingsproducten

4.1 Werving

NORM

HR.01

Rekruteringsprocessen voor personeel worden onderhouden in overeenstemming met het algemene personeelsbeleid en de procedures van de organisatie (bijvoorbeeld werving, positieve werkomgeving, oriëntatie, enzovoorts). Processen worden geïmplementeerd om ervoor te zorgen dat de organisatie beschikt over geschikt (IT-)personeel, met de vaardigheden die nodig zijn om de organisatiedoelen te bereiken. Screening maakt deel uit van het rekruteringsproces. De mate en frequentie waarmee deze screening wordt uitgevoerd, worden bepaald door hoe gevoelig en/of cruciaal de functie is. Screening wordt geïmplementeerd voor werknemers, aannemers en leveranciers.

Waarom doen we dit?

Met behulp van goed ingerichte wervingsprocessen wordt geborgd dat er voldoende IT-personeel is en de werknemers juist gekwalificeerd en gescreend zijn.

TOETSINGSKADER

- Wervingsprocessen voor (IT-)personeel zijn vastgelegd en geïmplementeerd, conform het algemene personeelsbeleid en procedures (bijv. aanname, positieve werkomgeving, oriëntatie).
- Er zijn processen geïmplementeerd om te garanderen dat het (IT-)personeel goed is toegerust om bedrijfsdoelen te behalen.
- Screening is onderdeel van het wervingsproces voor (IT-)personeel. Hoe grondig en vaak deze screening wordt geëvalueerd is afhankelijk van de gevoeligheid/het belang van de functie. De screening vindt plaats voor personeel, aannemers en leveranciers.
- De processen zijn goedgekeurd door het bevoegd gezag.

VOORBEELDMAATREGELEN

1. HR zorgt ervoor dat onderdeel van het personeelsbeleid is dat bij het werven van IT-personeel voldoende aandacht is voor de benodigde kwalificaties en zorgt ervoor dat het cv gecheckt wordt bij selectie van een nieuwe medewerker.

4.2 Certificering, training en scholing

NORM

HR.02

Opleiding, training en/of ervaring worden regelmatig getoetst om te zien of het personeel over de benodigde competenties beschikt om taken naar behoren te vervullen. Basis (IT-)competenties zijn vastgesteld en, indien nodig, worden kwalificatie- en certificeringsprogramma's gebruikt om te controleren of ze worden bijgehouden.

Waarom doen we dit?

Door professionele training van (IT-)personeel worden risico's op incidenten en verstoring van de bedrijfsprocessen gereduceerd. Daarnaast helpt het bij het hanteren van operationele procedures en projectbeheer.

TOETSINGSKADER

- Processen voor training en educatie zijn geïmplementeerd en worden uitgevoerd.
- Er zijn individuele persoonlijke ontwikkelplannen beschikbaar.
- Educatie, training en/of ervaring worden gebruikt om regelmatig te verifiëren of personeel over de benodigde vaardigheden beschikt.
- De relevante processen zijn goedgekeurd door het bevoegd gezag.

VOORBEELDMAATREGELEN

1. Scholing rondom informatiebeveiliging en IT is opgenomen in het scholingsplan van de school.
2. Ten minste jaarlijks wordt bekeken of er nog aanvullende opleiding nodig is.

4.3 Afhankelijkheid van individuen

NORM

HR.03
Er is een opvolgingsplanning en een back-upplan voor vitale medewerkers en afdelingen.

Waarom doen we dit?
Om de continuïteit van de functie te waarborgen is het belangrijk dat de taken van sleutelfiguren kunnen worden overgenomen door anderen en dat snel gesignaleerd wordt als er problemen bij het behoud of de werving van vitale afdelingen ontstaan.

TOETSINGSKADER

- Opvolgingsplanning, jobrotatie en back-up van het personeel zijn geïmplementeerd.
- Er zijn trainingsprogramma's om het risico van een te grote afhankelijkheid van sleutelfiguren te verkleinen.
- De meeste sleutelfuncties/-posities zijn geïdentificeerd en formeel gedefinieerd door het bevoegd gezag.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft vastgesteld welke functionarissen op het gebied van IT en informatiebeveiliging op sleutelfuncties zitten.
2. Voor elke sleutelfunctie zijn maatregelen benoemd wat te doen wanneer de medewerker van de één op de andere dag niet meer beschikbaar is. Voorbeelden zijn:
   a. er is een back-up binnen de eigen organisatie die de cruciale kennis heeft om direct ingezet te worden.
   b. er is in een regionale samenwerking afgesproken dat in dergelijke gevallen op basis van loonkosten tijdelijk een functionaris gedeeld kan worden.
   c. er is een lijst voorhanden van organisaties die per direct een inhuurmedewerker met de juiste expertise kunnen invliegen.

4.4 Verandering of beëindiging van functie

NORM

HR.04

Wanneer er functiewijzigingen plaatsvinden, met name beëindiging van het dienstverband, wordt direct effectief actie ondernomen. Kennisoverdracht wordt geregeld, verantwoordelijkheden worden opnieuw toegewezen en toegangsrechten worden verwijderd, zodat risico's worden geminimaliseerd en de continuïteit van de functie wordt gewaarborgd.

Waarom doen we dit?

Door kennisoverdracht wordt de continuïteit van de functie gewaarborgd en de risico's van ongeautoriseerde toegang worden gemitigeerd door het tijdig intrekken van de toegangsrechten.

TOETSINGSKADER

- Goedgekeurde processen zijn geïmplementeerd om kennis over te dragen en toegangsrechten opnieuw toe te wijzen of in te trekken.
- Kennisoverdracht is geregeld, verantwoordelijkheden zijn opnieuw toegewezen en toegangsrechten worden tijdig ingetrokken zodat risico's zijn geminimaliseerd en de continuïteit van de functie wordt gewaarborgd.
- De stappen van functieoverdracht zijn vastgelegd.

VOORBEELDMAATREGELEN

1. Wanneer iemand van functie wijzigt of een dienstverband beëindigd wordt, zorgt de verantwoordelijke manager dat:
   a. kennisoverdracht geregeld wordt,
   b. de verantwoordelijkheden opnieuw worden toegewezen,
   c. toegangsrechten ingetrokken worden.
2. HR heeft een checklist van de benodigde stappen en checkt bij de manager voor vertrek van de medewerker of hieraan uitvoering is gegeven.

4.5 Kennisdeling

NORM

HR.05

Overdracht van kennis en vaardigheden is geregeld, zodat eindgebruikers het systeem effectief en efficiënt kunnen gebruiken om bedrijfsprocessen te ondersteunen. Kennis en vaardigheden worden overgedragen zodat beheerders en technisch ondersteunend personeel het systeem en de bijbehorende infrastructuur op effectieve en efficiënte wijze kunnen leveren, ondersteunen en onderhouden.

Waarom doen we dit?

De aanwezigheid van procedures en werkinstructies maakt kennisoverdracht mogelijk en leidt tot een doelmatig en efficiënt gebruik van systemen voor het ondersteunen van bedrijfsprocessen.

TOETSINGSKADER

- Er zijn goedgekeurde processen op organisatieniveau geïmplementeerd om kennis over te dragen en gepaste documentatie-, trainings- en implementatiematerialen te onderhouden, zodat systemen op effectieve wijze businessprocessen kunnen ondersteunen. Hier zijn zowel eindgebruikers als operationele en technische support bij betrokken.

VOORBEELDMAATREGELEN

1. IT draagt zorg voor de benodigde gebruikersondersteuning bij IT-applicaties..
2. Beheerdocumentatie wordt actief bijgehouden door IT conform hiervoor opgestelde interne werkprocedures bij IT.

4.6 Veiligheidsbewustzijn

NORM

HR.06

Er is een bewustwordingsprogramma om gebruikers bewust te maken van hun verantwoordelijkheid om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie (middelen) te beschermen.

Waarom doen we dit?

Door medewerkers duidelijk te instrueren over hun verantwoordelijkheden met betrekking tot informatiebeveiliging, kunnen zij effectief bijdragen aan het beperken van informatiebeveiligingsrisico's.

TOETSINGSKADER

- Er is een security awareness-programma opgenomen in het informatiebeveiligingsplan en dit wordt organisatiebreed uitgevoerd.
- Het programma is in lijn met (informatie)beveiligingsbeleid.

VOORBEELDMAATREGELEN

1. Jaarlijks wordt in het informatiebeveiligingsplan (norm 1.3) beschreven welke bewustwordingsactiviteiten dat jaar worden uitgevoerd.
2. Gedurende het jaar komen alle medewerkers in aanraking met bewustwordings-activiteiten.
3. Ook richting leerlingen wordt op gepaste wijze bewustwording onder de aandacht gebracht bij gebruik van digitale middelen.

5 Configuration Management

Welke onderwerpen staan in dit domein?
Configuration management (configuratiemanagement) betreft het bijhouden van alle informatie van en over IT-componenten binnen de organisatie. Je legt vast welke hardware (bijvoorbeeld computers of printers) er zijn, welke software gebruikt wordt (inclusief versienummers), welke updates er zijn uitgevoerd en welke instellingen er gehanteerd worden bij elke component. Ook de onderlinge relaties tussen de componenten worden vastgelegd.

Dit helpt bij het houden van overzicht over alles wat binnen de organisatie gebruikt wordt, maar bijvoorbeeld ook bij het zorgvuldig installeren van software-updates. Alle informatie wordt vastgelegd in een zogeheten configuratiedatabase (CMDB). Het bijhouden van de CMDB moet zorgvuldig gebeuren. Er is een proces nodig om te zorgen dat alle items in het CMDB up-to-date blijven.

Wie is verantwoordelijk?

Het bevoegd gezag draagt de eindverantwoordelijkheid. De verantwoordelijke voor IT is binnen de organisatie verantwoordelijk voor het proces rondom configuratiemanagement en een medewerker IT is gewoonlijk belast met de uitvoering ervan.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Handreiking *Beheerprocessen*
- Format *Configuratiemanagement*

5.1 Identificatie en onderhoud van configuratie-items

NORM

CO.01

Er zijn configuratieprocedures vastgesteld om het beheer en loggen van alle wijzigingen in de configuratiedatabase te ondersteunen. Deze procedures zijn in overeenstemming met (en een voorwaarde voor) procedures voor change, incident en problem management.

Waarom doen we dit?

Inzicht hebben in de wijzigingen van de configuratie van systemen en diensten is noodzakelijk wanneer er verstoringen ontstaan. Deze configuraties staan vastgelegd in de configuratie-database. Het is nodig dat wijzigingen in configuraties ook vastgelegd worden in de configuratiedatabase. Zo kan de database bijdragen aan het vinden van de oorzaak van de verstoringen en is er inzicht in hoe een gedane wijziging effect heeft op andere processen.

TOETSINGSKADER

- Er bestaan geformaliseerde configuratieprocedures en werkmethoden om alle configuratie-items en hun attributen te identificeren en te onderhouden.
- De procedure is afgestemd met procedures voor change, incident en problem management. Management.
- De procedure is gedocumenteerd, gestandaardiseerd en gecommuniceerd.
- Er is beleid voor het labelen van fysieke bedrijfsmiddelen en nieuwe bedrijfsmiddelen worden geregistreerd in het inkoopproces.
- Er zijn processen geïmplementeerd voor het beheer van aangeschafte, toegewezen, gearchiveerde en verlopen licenties, die ervoor zorgen dat aan de licentievoorwaarden/-afspraken voldaan wordt.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een procedure voor configuratiemanagement. De opbouw van de procedure bevat de elementen die aangereikt worden in de Handreiking *Beheerprocessen*. Dit zijn elementen zoals het labelen van bedrijfsmiddelen en hoe bij de aanschaf van soft- of hardware op een centrale plek kenbaar wordt gemaakt dat er iets aangeschaft is. Er kan gebruik worden gemaakt van het Format Configuratiemanagement, waarin de processtappen zijn benoemd, evenals de rollen en verantwoordelijkheden en de communicatielijnen.
2. Het bevoegd gezag heeft de procedure configuratiemanagement vastgesteld.

5.2 Configuratiedatabase en baseline

NORM

CO.02

Een supporttool en een centrale opslag zijn ingericht voor alle relevante informatie over configuratie-items. Alle middelen en wijzigingen aan deze middelen worden gemonitord en vastgelegd. Na wijzigingen wordt voor ieder systeem en elke dienst als benchmark een baseline van configuratie-items geïmplementeerd.

Waarom doen we dit?

Monitoring van de middelen en wijzigingen draagt bij aan het betrouwbaar houden van de systemen van de organisatie. Door gebruik te maken van configuratie-baselines wordt voor elk type systeem en elke dienst een basisconfiguratie vastgelegd, zodat na een nieuwe wijziging indien noodzakelijk altijd teruggegaan kan worden naar die baseline.

TOETSINGSKADER

- Alle middelen en wijzigingen in middelen worden gemonitord en vastgelegd in een centrale opslagplaats.
- De relaties tussen configuratie-items worden geïdentificeerd en bijgehouden.
- Een tool voor configuratiemanagement (of gelijksoortige tools) wordt (worden) geïmplementeerd voor alle platforms.
- Er wordt enige automatisering ter ondersteuning gebruikt bij het volgen van wijzigingen in apparatuur en software.
- Configuratiebaselines baselines voor componenten worden vastgesteld en gedocumenteerd als benchmark na wijzigingen.
- Wijzigingen in de configuratiedatabase (CMDB) worden geregistreerd.

VOORBEELDMAATREGELEN

1. De organisatie heeft een CMDB ingericht met daarin alle hardware, software, onderlinge relaties, versienummers, licenties en configuratie-baselines.
2. De CMDB wordt up-to-date gehouden. Dat betekent dat bij processen die leiden tot een wijziging in de CMDB, ook een stap is opgenomen voor het bijwerken van de CMDB.

6 Incident-/Problem Management

Welke onderwerpen staan in dit domein?
Binnen de IT zijn er diverse beheerprocessen die eigenlijk in elke organisatie aandacht horen te krijgen. Incident- en problem management zijn hier onderdeel van. Bij incident-management gaat het erom zo snel mogelijk verstoringen van de continuïteit te verhelpen. Door hierbij een eenduidig proces te volgen met duidelijke verantwoordelijkheden voor betrokken functionarissen, worden incidenten gestructureerd behandeld. Nadat een incident geconstateerd of gemeld wordt, wordt geanalyseerd wat er aan de hand is. Op basis daarvan wordt bekeken welke actie eventueel moet worden genomen.

Dat kan zijn het verhelpen van het incident, escaleren naar het management, of het verkleinen van de gevolgen van het incident. Als het voldoende behandeld is, wordt het incident gesloten. Periodiek wordt een rapportage gemaakt, zodat het management op de hoogte is van wat er speelt op dit gebied. Als incidenten meermaals voorkomen, dan kan dat in een rapportage naar voren komen en aanleiding geven tot meer actie dan in een individueel incident. Is het een veelvuldig voorkomend incident in een systeem, dan gaat het over naar problem management, waar door grondige analyse gekeken wordt naar de onderliggende oorzaak met als doel de kwestie structureel te verhelpen.

Wie is verantwoordelijk?

Beheerprocessen vallen gebruikelijk onder de verantwoordelijke voor IT. Uitvoering van de processen vindt dan ook plaats binnen IT.

Ondersteuningsproducten

Beschikbaar:

- Format *Register beveiligingsincidenten en datalekken*

In ontwikkeling/te ontwikkelen:

- Handreiking *Beheerprocessen*
- Format *Incidentmanagementbeleid*
- Format *Problem managementbeleid*

6.1 Incident management

NORM

IM.01

Een formeel incidentmanagementproces wordt gecommuniceerd en geïmplementeerd. Er zijn procedures ingesteld om ervoor te zorgen dat alle incidenten en storingen worden geregistreerd, geanalyseerd, gecategoriseerd en geprioriteerd naar impact. Alle incidenten worden bijgehouden en periodiek beoordeeld om ervoor te zorgen dat ze tijdig worden verholpen.

Waarom doen we dit?

Een goed incidentmanagementproces draagt niet alleen bij aan een goede afhandeling van incidenten, maar ook aan het leren ervan om incidenten in de toekomst te voorkomen.

TOETSINGSKADER

- Het incidentmanagementbeleid is formeel gedocumenteerd en gecommuniceerd.
- Rollen en verantwoordelijkheden van de organisatie en de leveranciers zijn duidelijk gedefinieerd.
- Aspecten rondom juridisch en forensisch onderzoek zijn vastgesteld en toegewezen.
- Het registreren van, de communicatie over, de toewijzing van en de analyse van incidenten zijn formeel belegd in de organisatie.
- Incidenten worden gecategoriseerd en geprioriteerd op basis van impact.
- (Cyber)beveiligingsincidenten worden voorkomen of gedetecteerd en er is een proces om deze tijdig en effectief aan te pakken.
- Informatie wordt op een proactieve en formele manier gedeeld door personeel.
- Er wordt gemonitord of incidenten tijdig worden opgelost.
- Er wordt beperkt gerapporteerd aan het management over incident- en oplossings-analyses.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een incidentmanagementbeleid. De opbouw van dit beleid bevat elementen die aangereikt worden in de Handreiking *Beheerprocessen*. Er kan gebruik worden gemaakt van het Format *Incidentmanagementbeleid*, waarin de processtappen zijn benoemd, evenals de rollen en verantwoordelijkheden en de communicatielijnen.
2. Het bevoegd gezag heeft het incidentmanagementbeleid vastgesteld.
3. Het incidentmanagementbeleid is (digitaal) beschikbaar voor alle medewerkers, bijvoorbeeld via intranet.
4. Incidenten worden geregistreerd in een register van beveiligingsincidenten en datalekken. Er kan gebruik worden gemaakt van het Format *Register van beveiligingsincidenten en datalekken.*
5. Periodiek, bijvoorbeeld elk kwartaal, wordt gerapporteerd aan het management over de belangrijkste incidenten, met hierbij informatie over de wijze waarop het is opgelost.

6.2 Incident-escalatie

NORM

IM.02

Er worden procedures voor incidentmanagement (of voor de servicedesk) vastgesteld, zodat wanneer incidenten niet binnen de afgesproken termijn kunnen worden opgelost, service-niveaus adequaat worden geëscaleerd en, indien nodig, wordt voorzien in een tijdelijke oplossing. Eigenaarschap van incidenten en levenscyclusmonitoring blijven de verantwoordelijkheid van de servicedesk voor gebruikersincidenten, ongeacht welke IT-groep aan de oplossing werkt.

Waarom doen we dit?

De procedures voor incidentmanagement zorgen voor sturing op het proces en duidelijkheid over verantwoordelijkheden.

TOETSINGSKADER

- Het formeel vastgelegde beleid voor incidentmanagement bevat een escalatieprocedure.
- Er zijn escalatiecriteria bepaald.
- De escalatieprocedure is gebaseerd op serviceniveaus voor incidenten die niet meteen opgelost kunnen worden.
- Categoriseren en prioriteren vindt plaats op basis van impactanalyse, de bepaalde criteria en serviceniveaus.
- De responsteams krijgen de benodigde training.
- De verantwoordelijkheid voor het oplossen van een incident is toegewezen.

VOORBEELDMAATREGELEN

1. Indien de Handreiking *Incidentmanagementbeleid* onder 6.1 wordt gevolgd, is al invulling gegeven aan de escalatieprocedure en bijbehorende aspecten.
2. Degenen die betrokken zijn bij afhandeling van incidenten krijgen de benodigde instructies en deze worden periodiek herhaald.

6.3 Incidentrespons op (cyber)beveiligingsincidenten

NORM

IM.03

De organisatie beschikt over mogelijkheden voor incidentrespons om (cyber) beveiligingsincidenten snel te detecteren, te isoleren en de impact te beperken en om diensten op een betrouwbare manier te herstellen en weer in de lucht te brengen.

Waarom doen we dit?

Door een goede incidentrespons wordt schade door grote verstoringen van de infrastructuur, datalekken of informatiediefstal met financiële en/of imagoschade beperkt.

TOETSINGSKADER

- Naast de gebruikelijke incident- en problem managementprocedures zijn er ook plannen om preventie, risicobeperking, voorbereiding, tijdige reactie en herstel van (cyber) beveiligingsincidenten aan te pakken.
- Er zijn rollen en verantwoordelijkheden vastgelegd en toegewezen.
- De organisatie kan snel reageren op een verstoring, op gepaste schaal/escalatieniveau afhankelijk van mogelijke impact.

VOORBEELDMAATREGELEN

1. Indien het Format *Incidentmanagementbeleid* onder 6.1 wordt gevolgd, is al invulling gegeven aan de preventie, risicobeperking, voorbereiding, tijdige reactie en herstel van (cyber)beveiligingsincidenten evenals de rollen en verantwoordelijkheden.

6.4 Problem Management

NORM

IM.04

Een formeel problem managementproces is gedefinieerd en geïmplementeerd. Er zijn procedures ingesteld om oorzaken van (potentiële) incidenten en problemen (proactief en reactief) te identificeren en bekende fouten te beheersen totdat ze zijn opgelost. Structurele fouten in IT-services worden geminimaliseerd, zodat aantal en impact van mogelijke problemen wordt verminderd.

Waarom doen we dit?

Problem management draagt bij aan het verminderen van structurele fouten in IT-services, zowel in aantal als in impact ervan.

TOETSINGSKADER

- Er is formeel beleid voor problem management en dit is gecommuniceerd.
- Er zijn procedures om de oorzaak van problemen te identificeren.
- De rollen en verantwoordelijkheden van de organisatie en leveranciers zijn duidelijk vastgesteld.
- Er is een formele plek in de organisatie waar problems geregistreerd, gecommuniceerd, geanalyseerd en toegewezen worden aan verantwoordelijken.
- Problems worden geprioriteerd en toegewezen aan responsteams conform beleid.
- Informatie wordt proactief en op formele wijze gedeeld binnen responsteams.
- De managementanalyse van probleemidentificatie en -oplossing is beperkt en informeel.
- Bekende fouten worden geregistreerd en beheerst tot ze zijn opgelost.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een problem managementbeleid. De opbouw van dit beleid bevat elementen die aangereikt worden in de Handreiking *Beheerprocessen*. Er kan gebruik worden gemaakt van het Format *Problem managementbeleid*, waarin de processtappen zijn benoemd, evenals de rollen en verantwoordelijkheden en de communicatielijnen.
2. Het bevoegd gezag heeft het problem managementbeleid vastgesteld.
3. Problems worden meegenomen in de incidentenregistratie (zie 6.1.4)
4. Problems worden meegenomen in de periodieke rapportage aan het management voor de belangrijkste incidenten (zie 6.1.5)

7 Change Management

Welke onderwerpen staan in dit domein?
Change management, ook wel wijzigingenbeheer, gaat over het beheerst doorvoeren van wijzigingen in IT. Net als incident- en problem management is het een IT-beheer-proces. Ook hier werk je vanuit een vastgestelde procedure. Belangrijk is dat je daarin ook aandacht hebt voor het beoordelen van impact, het stellen van prioriteiten en wie er goedkeuring geeft voor een door te voeren wijziging.

En dat je een noodprocedure paraat hebt wanneer er met spoed een wijziging moet worden doorgevoerd in verband met de continuïteit van de bedrijfsvoering, waardoor de normale procedure te veel doorlooptijd vereist. Je moet wijzigingen eerst testen voor je ze doorvoert. Het is daarbij belangrijk dat er een representatieve testomgeving is en dat testen volgens een vooraf opgesteld testplan worden uitgevoerd. Na het zorgvuldig testen worden wijzigingen naar de productieomgeving gebracht. Hierbij is het van belang dat de juiste functionarissen goed-keuring verlenen en er waarborgen zijn voor een goede overdracht naar de productieomgeving.

Wie is verantwoordelijk?

Voor alle onderdelen binnen dit domein geldt dat uiteindelijk het bevoegd gezag de eind-verantwoordelijkheid draagt. Wanneer het gaat om wijzigingenbeheer ligt echter de dominante verantwoordelijkheid bij de verantwoordelijke voor IT. De IT-medewerkers geven hieraan uitvoering. Tot slot geldt dat de lijnmanager of de proceseigenaar van een specifiek product wijzigingen moet accorderen en daarom ook toetst of het wijzigingenproces goed gevolgd wordt.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Handreiking *Beheerprocessen*
- Format *Change managementprocedure*

7.1 Change Management

NORM

CH.01

Procedures voor formeel change management zijn opgezet om alle aanvragen (inclusief onderhoud en patches) voor wijzigingen in applicaties, procedures, processen, systeem- en serviceparameters en de onderliggende platforms op een gestandaardiseerde manier te behandelen.

Waarom doen we dit?

Goede procedures rondom wijzigingen helpen bij het borgen van de continuïteit van de bedrijfsvoering, doordat het beoordelen, autoriseren, testen, implementeren, documenteren en vrijgeven van voorgestelde wijzigingen gestructureerd gebeurt.

TOETSINGSKADER

- Het beleid voor wijzigingsbeheer en de werkwijzen zijn gedocumenteerd, gestandaardiseerd en gecommuniceerd.
- Er is een formeel wijzigingsbeheerproces voor het wijzigen van applicaties, procedures, processen, systemen en diensten, en de onderliggende platformen en infrastructuren.
- Het proces omvat alle componenten van overzetten naar productie, inclusief autorisatie, impactanalyse, release van het management, bijhouden van wijzigingen en rollback-procedures.
- Rollen en verantwoordelijkheden zijn vastgesteld en toegewezen. (Verzoeken voor) wijzigingen worden op een gestandaardiseerde manier behandeld.
- Wijzigingen worden gedocumenteerd. Documentatie is correct en actueel.
- Er is/wordt een systeem voor versiebeheer geïmplementeerd.
- Er is documentatie waaruit blijkt dat de organisatie wijzigingen conform de procedure heeft uitgevoerd, bijvoorbeeld een:
  - kopie van het gehanteerde RFC formulier (lijncontrole);
  - kopie van de impactanalyse van de wijziging (lijncontrole);
  - kopie van het acceptatieformulier, inclusief testuitkomsten (lijncontrole);
  - schermprint van de change die van ontwikkelomgeving naar productieomgeving wordt geïmplementeerd (lijncontrole).

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een procedure voor change management. De opbouw van de procedure bevat de elementen die aangereikt worden in de Handreiking *Beheerprocessen*. Er kan gebruik worden gemaakt van het Format *Change managementprocedure*, waarin de processtappen zijn benoemd, evenals de rollen en verantwoordelijkheden, impactbeoordelingen, noodprocedures en testplannen.
2. Het bevoegd gezag heeft de change managementprocedure vastgesteld.
3. De documentatie rondom wijzigingen wordt bewaard, zodat herleidbaar is welk proces gevolgd is.

7.2 Impact assessment, prioriteren en autoriseren

NORM

CH.02

Alle wijzigingsverzoeken worden op een gestructureerde manier beoordeeld om de impact te bepalen voor operationele systemen en functionaliteit. Alle wijzigingen zijn gecategoriseerd, geprioriteerd en geautoriseerd.

Waarom doen we dit?

Door het gestructureerd beoordelen van wijzigingsverzoeken wordt het risico op verstoring, verminking of verlies van (vertrouwelijke) data gereduceerd.

TOETSINGSKADER

- Er is een formele procedure voor categoriseren, prioriteren en autoriseren van wijzigingen en deze is gecommuniceerd.
- Voorafgaand aan de wijziging wordt een impact assessment uitgevoerd. Implicaties op het gebied van (cyber)veiligheid, juridische zaken, contracten en wet- en regelgeving worden in dit proces meegenomen.
- Er is een formele procedure voor het autoriseren van wijzigingen (Change Advisory Board).
- Elk wijzigingsverzoek wordt formeel (via de Change Advisory Board) goedgekeurd door de business-proceseigenaar en de stakeholders.
- Prioritering en categorisering zijn gebaseerd op vooraf vastgestelde criteria.
- Verslagen van resultaten van wijzigingen (wel/niet succesvol, reden van succes/falen, vervolgactie, aard van de impact) zijn beschikbaar.

VOORBEELDMAATREGELEN

1. Indien de Handreiking *Beheerprocessen* met het Format *Change management-procedure* onder 7.1 wordt gevolgd, is al invulling gegeven aan het beoordelen, prioriteren en categoriseren van wijzigingen en het bewaren van de wijzigings-resultaten.

7.3 Noodwijzigingen

NORM

CH.03

Wijzigingen tijdens een noodsituatie die onmiddellijke implementatie vereisen, worden op de juiste manier afgehandeld om minimale impact op systemen en IT-toepassingen te garanderen. De noodsituatiewijziging wordt na implementatie geregistreerd, geëvalueerd, getest en goedgekeurd door het senior management.

Waarom doen we dit?

Om een noodsituatie op te lossen kan een wijziging nodig zijn. Het doorlopen van het normale change managementproces duurt dan te lang. Daarom is er voor noodsituaties een route om tijdig te handelen en achteraf alsnog benodigde stappen uit het standaardwijzigingsproces uit te voeren, zodat de wijziging goed beheerd wordt.

TOETSINGSKADER

- De noodwijzigingsprocedure is formeel vastgelegd, gedocumenteerd en gecommuniceerd.
- (Verzoeken tot) noodwijzigingen worden op een gestandaardiseerde manier uitgevoerd.
- Rollen en verantwoordelijkheden zijn helder gedefinieerd en toegewezen.
- Noodwijzigingen zijn geautoriseerd en gedocumenteerd.
- Controlestappen, inclusief goedkeuring, worden conform procedure uitgevoerd na de noodwijziging.
- Kritieke afwijkingen van het proces worden geëvalueerd.

VOORBEELDMAATREGELEN

1. Indien de Handreiking *Beheerprocessen* met het Format *Change management-procedure* onder 7.1 wordt gevolgd, is al invulling gegeven aan de noodwijzigingsprocedure.

7.4 Testomgeving

NORM

CH.04
Er is een beveiligde testomgeving gedefinieerd en ingericht, die representatief is voor de geplande productieomgeving met betrekking tot beveiliging, interne controles, operationele procedures, gegevenskwaliteit, privacyvereisten en systeembelasting.

Waarom doen we dit?
Door middel van een representatieve testomgeving kunnen wijzigingen worden getest zonder dat het gevolgen heeft voor de productieomgeving én is duidelijk wat het effect van de wijziging in de productieomgeving is.

TOETSINGSKADER

- Formeel beleid is vastgesteld en geïmplementeerd voor de testomgeving.
- Er is een veilige testomgeving gedefinieerd en ingericht.
- De testomgeving representeert de productieomgeving en komt overeen in aspecten zoals workload/stress, besturingssystemen, applicatiesoftware, database, het management, netwerken en infrastructuur.
- De testomgeving staat volledig los van de productieomgeving.
- De testomgeving is beschermd tegen ongeautoriseerde toegang en gebruik.
- Het eigenaarschap van de test- en productieomgeving is duidelijk toegewezen.
- Er zijn richtlijnen voor het gebruik van data in de testomgeving, zodat aan privacywetgeving wordt voldaan.

VOORBEELDMAATREGELEN

1. Indien de Handreiking *Beheerprocessen* met het Format *Change management-procedure* onder 7.1 wordt gevolgd, is al invulling gegeven aan het beleid voor de testomgeving.
2. Voor elk systeem/elke applicatie in eigen beheer is een testomgeving beschikbaar. De testomgeving is zoveel als mogelijk gelijk aan de productieomgeving.
3. Er wordt niet gebruikgemaakt van productiedata, zeker niet wanneer deze persoonsgegevens bevat. Testen gebeurt met testdata die representatief is.

7.5 Testen van wijzigingen

NORM

CH.05

Voorafgaand aan migratie naar de operationele omgeving worden wijzigingen op onafhankelijke wijze getest in overeenstemming met het gedefinieerde testplan. Er wordt voor gezorgd dat het plan rekening houdt met beveiliging en prestaties.

Waarom doen we dit?

Met zorgvuldig testen kunnen fouten worden gevonden voordat de wijzigingen in de productieomgeving zijn doorgevoerd. Dit draagt bij aan het borgen van de continuïteit van de bedrijfsvoering en de betrouwbaarheid van de gegevensverwerking.

TOETSINGSKADER

- Formeel beleid voor het testen van wijzigingen is gedocumenteerd en gecommuniceerd.
- Rollen en verantwoordelijkheden zijn vastgesteld en toegewezen.
- Er worden testplannen gemaakt voordat de tests worden uitgevoerd.
- Er zijn criteria vastgesteld om te zorgen dat belangrijke elementen, zoals beveiliging en prestatie, opgenomen zijn in het testplan.
- Wijzigingen worden onafhankelijk volgens de tesplannen getest.
- Er is een beheerprocedure geïmplementeerd voor het bewaren en verwijderen van testresultaten.
- Fallback- of back-outplannen worden voorbereid en getest voordat wijzigingen in productie worden genomen.

VOORBEELDMAATREGELEN

1. Indien de Handreiking *Beheerprocessen* met het Format *Change management-procedure* onder 7.1 wordt gevolgd, is al invulling gegeven aan de wijze waarop omgegaan wordt met het testen.
2. Per wijziging wordt een testplan gemaakt en dit wordt gebruikt bij het testen van de wijziging.
3. De tester is niet betrokken geweest bij de ontwikkeling van de softwarewijziging.

7.6 Promotie naar productie

NORM

CH.06

Na testen wordt het gewijzigde systeem op gecontroleerde wijze en volgens het implementatieplan overgezet naar productie. Goedkeuring wordt verkregen van belangrijke stakeholders, zoals gebruikers, systeemeigenaar en operationeel management. Waar nodig wordt het gewijzigde systeem enige tijd naast het oude systeem gebruikt en worden gedrag en resultaten vergeleken.

Waarom doen we dit?

Door een toepassing volgens het implementatieplan op gecontroleerde wijze te promoveren naar de productieomgeving worden verstoringen van de bedrijfsvoering en ongeautoriseerde wijzigingen verminderd dan wel voorkomen.

TOETSINGSKADER

- Formeel beleid voor de overdracht van gewijzigde systemen is gedocumenteerd en gecommuniceerd.
- Er zijn procedures voor het gebruik van OTAP-omgevingen. Er zijn ook goedkeuringsprocessen.
- Het goedkeuringsproces bevat een formeel vastgelegde sign-off door belangrijke stakeholders.
- Rollen en verantwoordelijkheden zijn gedefinieerd en toegewezen.
- Toegangsregels voor de verschillende (OTAP-)omgevingen zijn gedefinieerd om functiescheiding te bewerkstellen.
- Voor overdracht worden implementatieplannen gemaakt, en overdracht vindt plaats volgens deze plannen.
- Waar nodig (op basis van impactanalyse) wordt het veranderde systeem enige tijd parallel aan het oude systeem gedraaid, waarbij gedrag en resultaat worden vergeleken.
- Acceptatiecriteria worden bepaald en acceptatietests worden uitgevoerd en gelogd.
- Er zijn beheersmaatregelen om te garanderen dat geaccepteerde wijzigingen daadwerkelijk onderdeel zijn van de overdracht naar productie (volledig).

VOORBEELDMAATREGELEN

1. Indien de Handreiking *Beheerprocessen* met het Format *Change management-procedure* onder 7.1 wordt gevolgd, is al invulling gegeven aan de wijze waarop overdracht aan productie plaatsvindt.
2. Er worden voorafgaand aan het overbrengen van de wijziging acceptatiecriteria bepaald en deze worden getoetst.

8 Systeemontwikkeling

Welke onderwerpen staan in dit domein?
Dit domein is vooral relevant voor schoolbesturen die (enige) softwareontwikkeling in eigen huis doen. In andere gevallen kunnen de meeste normen binnen het domein als 'niet van toepassing' verklaard worden. Uitzondering hierop zijn de normen die ook de aanschaf van software omvatten.

In de basis gaat het binnen dit domein om veilige ontwikkeling van software, bijvoorbeeld door de principes van *security by design en privacy by design* toe te passen, functiescheiding toe te passen en te zorgen voor zorgvuldige dataconversie.

Wie is verantwoordelijk?

De verantwoordelijkheid voor veilige ontwikkeling ligt over het algemeen bij de verantwoordelijke voor IT. De uitvoering van de normen zal door IT-medewerkers gebeuren. In meer algemene zin kunnen we constateren dat binnen het funderend onderwijs veelal geen (kritische) software-ontwikkeling plaatsvindt en deze normen veelal als 'niet van toepassing' verklaard kunnen worden.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Handreiking *Secure Software Development*

8.1 Methodiek voor veilige softwareontwikkeling en -implementatie

NORM

SD.01

Er is een gestructureerde aanpak (levenscyclus voor veilige softwareontwikkeling) voor interne ontwikkeling en aanschaf van software geïmplementeerd, die ervoor zorgt dat potentiële risico's voor bedrijfsvoering adequaat worden beoordeeld en beperkt, en dat de aspecten vertrouwelijkheid, integriteit en beschikbaarheid worden meegenomen. Voor elke nieuwe ontwikkeling of acquisitie is goedkeuring vereist door het juiste niveau van bedrijfs- en IT-management.

Waarom doen we dit?

Door een gestructureerde aanpak vinden softwareontwikkeling en -aanschaf plaats in lijn met de strategie van de organisatie en komen deze overeen met de functionele, technische en beveiligingseisen, goedkeuringsnormen en de informatiearchitectuur.

TOETSINGSKADER

- De organisatie heeft een gestructureerde aanpak voor interne ontwikkeling en aanschaf van software geïmplementeerd.
- Er zijn verplichte standaarden voor veilig coderen bepaald. Security by design, privacy by design en privacy by default worden door richtlijnen en standaarden afgedwongen.
- Voor elke nieuwe ontwikkeling of aanschaf is goedkeuring nodig van het juiste niveau van het business- of IT-management.
- De methodiek voor assurance van softwarekwaliteit bevat verplichte "mijlpalen voor informatiebeveiliging" (met inbegrip van risicobeoordeling, broncodebeoordeling en tests) die niet kunnen worden omzeild en deze worden gedocumenteerd.
- Awarenesstraining voor beveiliging wordt op vrijwillige basis gevolgd.

VOORBEELDMAATREGELEN

1. De Handreiking S*ecure Software Development* wordt toegepast bij de ontwikkeling van software.
2. Periodiek wordt binnen het ontwikkelteam aandacht besteed aan/getraind op veilige softwareontwikkeling.

8.2 Toegang tot de productieomgeving door ontwikkelaars

NORM

SD.02

Medewerkers (ontwikkelaars) die betrokken zijn bij de ontwikkeling en implementatie van wijzigingen in applicaties en ondersteunende besturingssystemen en databases, hebben geen schrijftoegang tot de productieomgeving. Medewerkers (ontwikkelaars) die verantwoordelijk zijn voor het vrijgeven van de broncode voor productie hebben geen schrijftoegang tot de test- of ontwikkelomgeving.

Waarom doen we dit?

Scheiding van taken tussen ontwikkelaars helpt bij het voorkomen van ongeoorloofde toegang tot of wijzigingen in programma's en gegevens.

TOETSINGSKADER

- Een samenhangend beleid is bepaald, geïmplementeerd en goedgekeurd door het bevoegd gezag.
- Ontwikkelaars hebben geen schrijftoegang tot productie, en systeembeheerders die software overzetten naar productie hebben geen schrijftoegang tot de ontwikkel-, test- en acceptatieomgeving.
- Uitzonderingen op het beleid worden vooraf goedgekeurd door de systeem-/proces-eigenaar en tijdens de tijdelijke schrijftoegang wordt gebruikgemaakt van logging en/of het vier-ogen-principe.
- Er is beleid of een procesbeschrijving voor het beheer van speciale bevoegdheden.
- Er zijn functie- of rolbeschrijvingen van de beheerders van speciale bevoegdheden.
- Er is informatie uit systemen waaruit blijkt dat de technische of functioneel beheerders die speciale bevoegdheden hebben, ook een gewone gebruikers-ID hebben voor hun reguliere werkzaamheden.

VOORBEELDMAATREGELEN

1. Conform de Handreiking *Secure Software Development* wordt functiescheiding toegepast en zijn er afspraken rondom speciale bevoegdheden binnen systemen.

8.3 Dataconversie en/of migratie

NORM

SD.03

Het management beschikt over beheersmaatregelen om te zorgen dat de dataconversie accuraat en volledig is. Deze dataconversie-controles zijn opgesteld om de data-integriteit gedurende het conversieproces te behouden.

Waarom doen we dit?

Door deze beheersmaatregelen wordt de integriteit (bijvoorbeeld nauwkeurigheid en volledigheid) van de gegevens/het systeem gewaarborgd, aangezien afwijkingen tijdig worden gedetecteerd.

TOETSINGSKADER

- Er wordt een risico- en bedrijfsimpactanalyse uitgevoerd ter rechtvaardiging van de gedefinieerde beheersmaatregelen.
- Het ontwerp van de beheersmaatregelen is gedocumenteerd en formeel aanvaard door de eigenaar van het systeem of het proces.
- De beheersmaatregelen waarborgen de juistheid en volledigheid van de dataconversie/ migratie en bewaken ook de integriteit van de data.
- De resultaten van de (handmatige en/of geautomatiseerde) uitgevoerde integriteits-controles worden gedocumenteerd en beoordeeld door de eigenaar van het systeem of het proces om de dataconversie formeel te accepteren.

VOORBEELDMAATREGELEN

1. Conform de Handreiking *Secure Software Development* wordt bij dataconversie aandacht besteed aan zaken als impactanalyse en beheersmaatregelen voor integriteit van de data.

9 Datamanagement

Welke onderwerpen staan in dit domein?
In het domein Datamanagement gaat het over het onderhouden van de volledigheid, beschikbaarheid, juistheid en de bescherming van gegevens. Bij data-management is het van belang dat er binnen de organisatie eigenaarschap is toegewezen voor alle informatie en informatiesystemen. De informatie en de systemen dienen geclassificeerd te worden, zodat het juiste beschermingsniveau kan worden toegepast.

Daarnaast moet de organisatie hebben nagedacht over wat er nodig is op het gebied van het opslaan, bewaren en archiveren van data. Bij uitwisseling van data en software moet een passend beschermingsniveau worden gebruikt en bij verwijdering van data, apparatuur en media moeten verwijderingsprocedures worden gebruikt.

Wie is verantwoordelijk?

Het bevoegd gezag is eindverantwoordelijk voor datamanagement. Wanneer iets fout gaat op dit vlak, kan het grote gevolgen hebben (bijvoorbeeld datalekken). Elke proces- of systeemeigenaar heeft vervolgens binnen het eigen proces of systeem een verantwoordelijkheid voor correct datamanagement. IT geeft uitvoering aan de beveiligingsmaatregelen die voortvloeien uit de classificatie.

Ondersteuningsproducten

Beschikbaar:

- Certificeringsschema ROSA

In ontwikkeling/te ontwikkelen:

- Bewaartermijnen binnen het verwerkingsregister FORA

9.1 Data- en systeemeigenaarschap

NORM

DM.01

De organisatie beschikt over procedures en hulpmiddelen waarmee zij de verantwoordelijkheid voor het eigenaarschap van informatie en informatiesystemen kan adresseren. Eigenaren nemen beslissingen over het classificeren van informatie en (informatie)systemen en beschermen ze in overeenstemming met deze classificatie.

Waarom doen we dit?

Eigenaarschap bevordert de effectieve besluitvorming, de bescherming van gegevens en informatiesystemen en de controle over gegevensbeheer.

TOETSINGSKADER

- Het goedgekeurde beleid geeft een duidelijke omschrijving van rollen, verantwoordelijkheden en eigenaarschap.
- Beleid en procedures ondersteunen de bescherming van informatiemiddelen, maken efficiënte levering en gebruik van businessapplicaties mogelijk en zorgen voor effectieve besluitvorming over (informatie)beveiliging.
- Beleid en procedures worden naar de hele organisatie gecommuniceerd en toegepast op bedrijfskritische data en informatiesystemen.

VOORBEELDMAATREGELEN

1. Data-eigenaarschap en -classificatie maken onderdeel uit van het informatie-beveiligingsbeleid (zie norm 1.2). Indien gebruik wordt gemaakt van het format IBP-beleid uit die norm, wordt invulling gegeven aan de eisen die gesteld worden aan het beleid in het toetsingskader. Invulling aan dataclassificatie gebeurt op basis van het standaard-certificeringsschema ROSA.

9.2 Classificatie

NORM

DM.02

Stel een classificatieschema op dat in de hele organisatie van toepassing is, op basis van de kriticiteit en gevoeligheid (bijvoorbeeld openbaar, vertrouwelijk, topgeheim) van organisatie-gegevens. Dit schema bevat details over het eigenaarschap van gegevens; gedefinieerde passende (informatie)beveiligingsniveaus en beschermingsmaatregelen; en een korte beschrijving van eisen voor het bewaren en vernietigen van gegevens, en gevoeligheid. Het wordt gebruikt als basis voor het toepassen van maatregelen zoals toegangscontrole, archivering en versleuteling.

Waarom doen we dit?

Een classificatieschema helpt bij het ervoor zorgdragen dat de beveiligingsmaatregelen in lijn zijn met de eisen die de organisatie stelt voor informatie van die betreffende classificatie.

TOETSINGSKADER

- Er zijn een dataclassificatieschema en richtlijnen voor het gebruik daarvan geïmplementeerd en toegepast binnen de hele organisatie.
- Eigendom van data, definities en eisen voor verschillende niveaus van dataclassificatie worden allemaal nadrukkelijk beschreven in de richtlijnen.
- De richtlijnen worden gebruikt als een basis voor het toepassen van de benodigde (cyber) beheersmaatregelen voor kritische businessprocessen en/of applicaties.
- Het classificatieschema is goedgekeurd door het bevoegd gezag.

VOORBEELDMAATREGELEN

1. Het schoolbestuur stelt vast dat dat het certificeringsschema ROSA (Edustandaard) toegepast wordt binnen de organisatie.
2. Door consequente toepassing van ROSA wordt invulling gegeven aan alle aspecten van het toetsingskader.

9.3 Beveiligingseisen voor datamanagement

NORM

DM.03

Beleid en procedures zijn vastgesteld en geïmplementeerd om (informatie)beveiligingseisen te identificeren en toe te passen op de ontvangst, verwerking, opslag en doorgifte van relevante gegevens in lijn met bedrijfsdoelstellingen, het (informatie)beveiligingsbeleid van de organisatie en wettelijke vereisten (bijvoorbeeld privacy van bepaalde gegevens).

Waarom doen we dit?

Door middel van beleid en procedures rondom de ontvangstverwerking, opslag en doorgifte van gegevens wordt het risico op overtreding van wet- en regelgeving verkleind.

TOETSINGSKADER

- Er is een beleid bepaald, geïmplementeerd en gecommuniceerd om gevoelige data te beschermen tegen ongeautoriseerde toegang en incorrecte uitwisseling.
- Het beleid is goedgekeurd door het bevoegd gezag.
- Er is een formeel proces dat gevoelige data identificeert en uitspraken doet over vertrouwelijkheid en het voldoen aan relevante wet- en regelgeving (zoals data privacy).
- Er is overeenstemming met proceseigenaren over dataclassificatie.
- De eisen voor essentiële (informatie)systemen zijn in overeenstemming met organisatie-doelen. De eisen zijn opgesteld voor fysieke en logische toegang tot data-output, waarvan de vertrouwelijkheid duidelijk gedefinieerd en afgewogen is.

VOORBEELDMAATREGELEN

1. De beveiligingseisen van het certificeringsschema ROSA worden toegepast.

9.4 Inrichting van opslag en retentie

NORM

DM.04

Er zijn procedures gedefinieerd en geïmplementeerd voor het effectief en efficiënt opslaan, bewaren en archiveren van gegevens, zodat wordt voldaan aan organisatiedoelstellingen, het (informatie)beveiligingsbeleid van de organisatie en wettelijke vereisten.

Waarom doen we dit?

Procedures worden gedefinieerd en geïmplementeerd om te voldoen aan de organisatiedoelstellingen, het (informatie)beveiligingsbeleid van de organisatie en de wettelijke vereisten.

TOETSINGSKADER

- Er zijn formele procedures en richtlijnen voor het opslaan, bewaren en archiveren van data.
- In lijn met bedrijfsvoering zijn er eisen gesteld aan het opslaan, bewaren en archiveren van data (technieken) en deze zijn geïmplementeerd.
- Er is voor gezorgd dat deze eisen in overeenstemming zijn met (informatie)beveiligings-beleid, contractuele afspraken en wet- en regelgeving.

VOORBEELDMAATREGELEN

1. Zorg dat er een eenduidige wijze is voor het opslaan, bewaren en archiveren van data. Het is verstandig dit onderwerp op te nemen in het Beleid IBP.
2. Stel de termijnen voor archivering en verwijderen vast voor alle data- en document-typen. Hiervoor kan gebruikgemaakt worden van de bewaartermijnen zoals opgenomen in het verwerkingsregister van FORA.

9.5 Uitwisseling van (gevoelige) gegevens

NORM

DM.05

(Cyber)beleid en procedures zijn vastgesteld en geïmplementeerd, zodat aan bedrijfseisen voor de bescherming van gegevens en software wordt voldaan wanneer gegevens en software worden uitgewisseld binnen de organisatie of met een externe partij. Gevoelige transactiegegevens worden alleen uitgewisseld via een vertrouwd pad of medium waarbij (cyber)maatregelen zijn genomen om de authenticiteit van de inhoud, bewijs van versturen, bewijs van ontvangst en onweerlegbaarheid van de oorsprong aan te tonen.

Waarom doen we dit?

Het implementeren en vaststellen van (cyber)beleid en procedures is van belang voor de bescherming van gegevens tijdens uitwisseling om zo de kans op ongeautoriseerde toegang of openbaarmaking van gevoelige informatie te verkleinen.

TOETSINGSKADER

- Het (cyber)beleid en de procedures zijn gedefinieerd en geïmplementeerd om data en software te beschermen en uitwisseling mogelijk te maken.
- Het (cyber)beleid is goedgekeurd door het bevoegd gezag en wordt algemeen toegepast.
- Bedrijfsdata wordt geclassificeerd naar de mate van vertrouwelijkheid.
- Data die uitgewisseld worden buiten de organisatie moet voor versturen versleuteld worden.
- Logs van essentiële applicaties worden geëvalueerd en incorrecte of incomplete data-uitwisselingen worden tegengehouden.

VOORBEELDMAATREGELEN

1. In het IBP-beleid (norm 1.2) is vastgelegd op welke wijze data en software beschermd zijn. Hieruit blijkt ook welke middelen de organisatie inzet om gevoelige data uit te wisselen.
2. Bij uitwisselingen van data middels applicaties, houdt IT toezicht op de logdata, zodat incorrecte en incomplete data-uitwisselingen gestopt worden.

9.6 Verwijdering van data

NORM

DM.06

Er zijn (cyber)procedures vastgesteld en geïmplementeerd om ervoor te zorgen dat aan business requirements voor het beschermen van (gevoelige) gegevens en software wordt voldaan bij het verwijderen of overdragen van gegevens of hardware.

Waarom doen we dit?

Door procedures omtrent het verwijderen van data wordt aan wet- en regelgeving voldaan en wordt de kans verkleind dat data in verkeerde handen komen.

TOETSINGSKADER

- Er zijn (cyber)procedures formeel vastgelegd en geïmplementeerd om erop toe te zien dat er aan business requirements en wet- en regelgeving voor het beschermen van (gevoelige) data en software wordt voldaan wanneer data en hardware worden verwijderd of overgedragen.
- Apparatuur en media met gevoelige informatie worden zoveel mogelijk opgeschoond voor gebruik of verwijdering.
- De verantwoordelijkheden voor verwijderingsprocedures zijn duidelijk gedefinieerd.

VOORBEELDMAATREGELEN

1. Een gecertificeerde dienstverlener verwijdert de data voorafgaand aan de afvoer van apparatuur en media.
2. Bij doorgifte van apparatuur draagt IT zorg voor zorgvuldige verwijdering van alle data van de vorige gebruiker.
3. Specifiek is er aandacht voor verwijdering van beeldmateriaal door leerlingen die gebruikmaken van devices van de school. Hier wordt bij inlevering van een device elke keer expliciet op gewezen.

10 Identity & Access Management

Welke onderwerpen staan in dit domein?
Identity & Access Management, afgekort IAM, draagt zorg voor het beheren van de logische toegang tot informatie, informatiediensten en externe koppelingen. Met logische toegang wordt de toegang tot systemen bedoeld. Dit begint met het bepalen welke gebruikers en rollen toegang mogen hebben en het doorvoeren van toegangsrechten.

Voor het doorvoeren van wijzigingen in toegangsrechten geldt functiescheiding, zodat iemand niet zichzelf alle rechten kan toekennen. Er is speciale aandacht voor zogeheten superuser-rechten, onder andere door logging, om te voorkomen dat iemand ongeoorloofd toegang heeft. Ook is er een procedure voor noodtoegang die bijvoorbeeld bij een verstoring noodzakelijk kan zijn. Tot slot worden alle toegangsrechten periodiek beoordeeld.

Wie is verantwoordelijk?

Het bevoegd gezag is eindverantwoordelijk. Verantwoordelijkheid van het inrichten van IAM ligt vaak bij de verantwoordelijke voor IT. De IBP-medewerker adviseert over de kaders voor IAM. De systeemeigenaar stelt toegangsrechten voor een specifiek systeem vast en voert periodiek controle uit.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Voorbeeld *Autorisatiematrix*
- Voorbeeld *Proces toegangsrechten*
- Voorbeeld *Audit- en controleplan*

10.1 Toegangsrechten

NORM

ID.01

De organisatie heeft toegangsgroepen (of rollen) gedefinieerd op basis van vastgestelde bedrijfsregels, waaronder functiescheiding, in een Autorisatiematrix. Er zijn procedures die tijdige initiatie en update in de autorisatiematrices voor alle toepassingen regelen. Het management keurt wijzigingen in vastgestelde rechten voor toegangsgroepen (of rollen) goed. Alle gebruikersactiviteiten zijn traceerbaar tot op het individu (bijvoorbeeld gebaseerd op een combinatie van gebruikersnaam en wachtwoord of token of biometrische informatie).

Waarom doen we dit?

Door toegangsrechten toe te wijzen aan groepen of rollen wordt functiescheiding mogelijk gemaakt en is de grondslag voor de toekenning van rechten aan individuen altijd duidelijk. Als alle activiteiten te herleiden zijn tot een individu, kan men bij incidenten nagaan wie wat wanneer gedaan heeft. Dit komt de betrouwbaarheid van gegevens en continuïteit ten goede.

TOETSINGSKADER

- Het beleid en de SOLL-matrix voor toegangsrechten van gebruikers en rollen zijn gedefinieerd, formeel vastgesteld en gecommuniceerd en worden nauwgezet onderhouden.
- De identificatie, authenticatie en autorisatie van gebruikers zijn geïmplementeerd en worden afgedwongen.
- Toegangsrechten toegekend op basis van de SOLL-matrix worden periodiek vergeleken met de IST-situatie.
- Activiteiten van gebruikers kunnen worden getraceerd naar uniek identificeerbare gebruikers.
- Gebruikers-ID's en toegangsrechten worden bijgehouden in een centrale opslag.

VOORBEELDMAATREGELEN

1. Logische toegangsbeveiliging is onderdeel van het IBP-beleid (norm 1.2).
2. Voor alle bedrijfskritische applicaties - denk hierbij aan zaken als financiële administratie, personeelsadministratie, leerlingenadministratie, LAS, elektronische leeromgevingen - is een Autorisatiematrix vastgesteld door de systeem- of proceseigenaar. Hiertoe kan gebruikgemaakt worden van het Voorbeeld *Autorisatiematrix*. De Autorisatiematrix is op niveau van rollen ingericht; welke rol heeft welke toegangsrechten nodig? Hiermee wordt voorkomen dat op individueel niveau telkens opnieuw bepaald hoeft te worden en het maakt uitzonderingen goed te beargumenteren. Toegang is op basis van need-to-know.
3. Minimaal elk kwartaal wordt gekeken of de toegekende toegangsrechten overeenkomen met de vastgestelde Autorisatiematrix. Afwijkingen worden voorgelegd aan de systeemeigenaar.
4. Elke applicatie werkt met identificatie, authenticatie en autorisatie van gebruikers.
5. Toegang wordt toegekend aan individuele gebruikers, niet aan groepen.
6. Er vindt centrale opslag plaats van gebruikers-ID's en toegangsrechten.

10.2 Administratie van toegangsrechten

NORM

ID.02

Toegangsrechten voor werknemers worden toegewezen in overeenstemming met toegewezen taakverantwoordelijkheden (bijvoorbeeld via op rollen gebaseerde toegang). Beheerprocedures zijn beschikbaar om activiteiten vast te stellen voor het aanvragen, uitgeven of sluiten van een account en de bijbehorende toegangsrechten voor gebruikers. De procedure omvat tevens de methode die door het bevoegd gezag wordt gebruikt om deze activiteiten op de juiste wijze te autoriseren. Toegang wordt verschaft op basis van het need-to-know/need-to--have-principe.

Waarom doen we dit?

Een goede administratie van toegangsrechten maakt het mogelijk om de continuïteit van de processen bij bijvoorbeeld vertrek van een werknemer te waarborgen en maakt de rechten van de individuele gebruiker zichtbaar.

TOETSINGSKADER

- Het beleid voor alle accounts en toegangsrechten is gedefinieerd, gedocumenteerd, formeel vastgesteld en gecommuniceerd.
- Hieronder valt ook de toestemmingsprocedure voor de data-/of systeemeigenaar die toegangsrechten toekent.
- Er is een geschikte functiescheiding voor het aanvragen, toekennen, implementeren en intrekken van toegangsrechten van gebruikers.
- De toegangsrechten van werknemers zijn geïmplementeerd op basis van hun rollen.

VOORBEELDMAATREGELEN

1. Zie norm 10.1 voor beleid en rolgebaseerde toegang.
2. Er is een proces voor het toekennen/wijzigen van toegangsrechten gedefinieerd. Hiertoe kan gebruikgemaakt worden van het Voorbeeld *Proces toegangsrechten.*
3. Er is een koppeling met het in- en uitdiensttredingsproces gemaakt voor autorisaties.

10.3 Superusers

NORM

ID.03

Het management heeft maatregelen ingevoerd die ervoor zorgen dat superusertoegang beperkt is tot de juiste (beperkte) groep individuen en dat activiteiten die worden uitgevoerd met superuseraccounts worden gemonitord. Superuseraccounts moeten worden goedgekeurd door het verantwoordelijk management.

Waarom doen we dit?

Het beperken en monitoren van het gebruik van superuserrechten is noodzakelijk om ongeoorloofde toegang en verstoringen te beperken.

TOETSINGSKADER

- Er is een formele procedure voor superuserrechten gedefinieerd, gedocumenteerd en gecommuniceerd.
- Individuen met superuserrechten zijn vastgelegd en toekenning is goedgekeurd door het verantwoordelijke management.
- Gebruik van de superuserrechten wordt gelogd en geëvalueerd.

VOORBEELDMAATREGELEN

1. De kaders voor superuserrechten maken onderdeel uit van het beleid (zie norm 10.1). Het proces voor de toekenning maakt onderdeel uit van het proces voor toegangsrechten. (zie norm 10.2).
2. Er is een goede, up-to-date administratie van superuserrechten.
3. Elk gebruik van superuserrechten wordt gelogd.
4. Periodiek wordt geëvalueerd of de superuserrechten conform de kaders gebruikt zijn en of de toekenning nog altijd nodig is.

10.4 Noodtoegang (envelopprocedure/ breek-het-glasprocedure)

NORM

ID.04

Er is een noodprocedure vastgesteld om in geval van noodtoegang tot accounts met superuserrechten te beheren, die door de organisatie wordt gevolgd.

Waarom doen we dit?

Om tijdens een noodgeval adequaat te kunnen handelen is een noodprocedure nodig.

TOETSINGSKADER

- De formele noodprocedure is gedefinieerd, gedocumenteerd en gecommuniceerd.
- Het gebruik van de noodprocedure wordt bijgehouden.
- Het gebruik van de noodprocedure wordt geëvalueerd, samen met de uitgevoerde ingrepen met superuserrechten en wijzigingen van de noodwachtwoorden.

VOORBEELDMAATREGELEN

1. Het hebben van een noodprocedure maakt onderdeel uit van het proces toegangs-rechten.
2. Het gebruik van de noodprocedure wordt altijd vastgelegd.
3. Na afloop van de noodsituatie wordt de noodprocedure geëvalueerd en wordt nagegaan of gebruik ervan conform alle afspraken heeft plaatsgevonden.

10.5 Periodieke beoordeling van toegangsrechten

NORM

ID.05

Het management beoordeelt periodiek de gebruikerstoegang die geïmplementeerd is voor de relevante applicaties (IST-situatie) om de juistheid van geïmplementeerde accounts en rollen (de toegangsrechten) te bevestigen, en valideert dat toegangsrechten passend zijn voor toegewezen taken, zoals bepaald door de toegangsregels (SOLL-situatie). Elke onjuiste toegang die tijdens het beoordelingsproces wordt opgemerkt, wordt direct ingetrokken. Deze controle houdt in dat SOLL- en IST-matrices worden vergeleken door het verantwoordelijke management.

Waarom doen we dit?

Om ongeautoriseerde toegang tot het besturingssysteem, gegevens en applicaties te reduceren worden de toegangsrechten periodiek gecontroleerd door het management.

TOETSINGSKADER

- De procedures voor Identity & Access Management en SOLL-IST-evaluaties zijn gedefinieerd, gedocumenteerd en formeel vastgelegd.
- De SOLL- en IST-matrices worden voor alle gebruikers periodiek vergeleken, geëvalueerd en goedgekeurd door het management.
- Ongepaste toegangsrechten worden ingetrokken.
- De procedures voor Identity & Access Management en de SOLL-IST-evaluaties worden periodiek geëvalueerd en zijn effectief.

VOORBEELDMAATREGELEN

1. Er is vastgelegd en vastgesteld door het bevoegd gezag hoe vaak en op welke wijze getest wordt of de informatiebeveiliging op orde is. Dit gebeurt in een audit- en controleplan. Hiervoor kan gebruikgemaakt worden van het Voorbeeld *Audit- en controleplan*. Daarin staat ook vastgelegd wanneer welke autorisaties gecheckt worden.
2. Wanneer uit de controle blijkt dat er ongepaste toegangsrechten zijn, geeft de verantwoordelijk manager opdracht aan IT om deze rechten in te trekken.

11 Security Management

Welke onderwerpen staan in dit domein?
Security management gaat over de meer technische kant van informatiebeveiliging. Het zorgdragen dat risico's op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid voor een informatievoorziening zo veel mogelijk geadresseerd en gemitigeerd worden. Hiervoor zijn richtlijnen noodzakelijk die het kader beschrijven waarbinnen dit gebeurt.

Belangrijk is dat de juiste authenticatiemechanismen ingericht worden, dat mobiele apparaten op correcte wijze zorgen voor informatiebeveiliging en dat alle handelingen binnen een systeem gelogd worden. Daarnaast dient de beveiliging regelmatig getest te worden met bijvoorbeeld penetratietesten, moeten beschikbare beveiligingsfixes (patches) van software tijdig worden doorgevoerd en moet er aandacht zijn voor dreigingen en kwetsbaarheden. De IT-infrastructuur moet beschermd en onderhouden worden. Wanneer versleuteling plaatsvindt, moet er beheer plaatsvinden op de cryptografische sleutels. Het netwerk dient voorzien te zijn van de benodigde beveiliging (bijvoorbeeld een firewall), malware moet worden tegengegaan en de beveiligingstechnologie moet beschermd worden.

Wie is verantwoordelijk?

De eindverantwoordelijkheid ligt bij het bevoegd gezag. Verantwoordelijkheid voor het inrichten van security management wordt over het algemeen belegd bij de verantwoordelijke voor IT. De uitvoering van de normen zal door IT-medewerkers plaatsvinden. In meer of mindere mate kan een aantal van deze zaken uitbesteed zijn aan een leverancier. In dat geval vindt beheersing plaats door middel van ketenbeheer of leveranciersmanagement.

Ondersteuningsproducten

Beschikbaar:

- Voorbeeldsgedragcode *Veilig gebruik ICT-middelen en persoonsgegevens*

In ontwikkeling/te ontwikkelen:

- Handreiking *Hardening*
- Voorbeeld *Audit- en controleplan*
- Handreiking *Beheerprocessen*
- Format *Beleid patchmanagement*
- Handreiking *Beleid cryptografie*
- Overzicht *Best practices netwerkbeveiliging*

11.1 Security baselines

NORM

SM.01

IT security baselines en richtlijnen voor IT-infrastructuur zijn vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. Beveiligingsbaselines worden formeel vastgelegd, periodiek geactualiseerd en goedgekeurd door het bevoegd gezag. Verantwoordelijk IT-personeel wordt hiervan op de hoogte gesteld. Geïmplementeerde beveiligingsinstellingen voor IT-middelen worden periodiek beoordeeld op naleving van beveiligingsbaselines. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

Waarom doen we dit?

Beveiligingsbaselines zorgen voor een consistente implementatie van beveiligingsinstellingen. Dit resulteert in een consistent en hoog niveau van beveiliging, en bevordert de continuïteit van de IT-services.

TOETSINGSKADER

- Beveiligingsbaselines zijn gedefinieerd, goedgekeurd door het bevoegd gezag en gecommuniceerd naar verantwoordelijk IT-personeel.
- De geïmplementeerde beveiligingsinstellingen voor IT-middelen worden periodiek gecontroleerd op overeenstemming met de beveiligingsbaselines.
- Resultaten worden gedocumenteerd, afwijkingen worden gedocumenteerd en goedgekeurd (of gecorrigeerd).
- Voor nieuwe IT-infrastructuurcomponenten en projectmanagementprocessen wordt implementatie van beveiligingsbaselines afgedwongen.
- In hoeverre aan de baseline wordt voldaan wordt periodiek gerapporteerd aan het bevoegd gezag.

VOORBEELDMAATREGELEN

1. De IT-medewerkers hebben bepaald welke minimale security-instellingen nodig zijn voor veilig gebruik van bedrijfskritische applicaties en dit vastgelegd in een security baseline die is vastgesteld door het bevoegd gezag. Hiervoor kan gebruikgemaakt worden van de Handreiking *Hardening*.
2. De instellingen van applicaties worden minimaal jaarlijks gecontroleerd op de security baselines. Na elke wijziging vindt ook standaard een controle plaats.
3. Afwijkingen worden gedocumenteerd in het incidentenregister en gecorrigeerd. Indien de afwijking niet gecorrigeerd wordt, wordt acceptatie ervan gedocumenteerd.
4. Bij ontwikkeling van IT-middelen wordt aan de voorkant meegenomen dat de security baselines worden geïmplementeerd.
5. Afwijkingen op de baseline gaan mee in de periodieke incidentenrapportage aan het bestuur.

11.2 Authenticatiemechanismes

NORM

SM.02

Alle gebruikers (intern, extern en tijdelijk) en hun activiteiten op IT-systemen moeten uniek identificeerbaar zijn. Het management is verantwoordelijk voor de periodieke controle van de lijst met actieve ID's in relevante applicaties om te bepalen of unieke user ID's zijn geïmplementeerd om traceerbaarheid te garanderen en ervoor te zorgen dat algemene en systeemaccounts geblokkeerd of op andere wijze beschermd zijn. Alle onjuiste of inactieve user ID's die tijdens het controleproces worden opgemerkt, worden tijdig gedeactiveerd.

Waarom doen we dit?

Authenticatiemechanismen zorgen voor geoorloofde toegang tot programma's/gegevens door herleidbaarheid van activiteiten tot gebruikers en ongeoorloofde toegang wordt tegengegaan door de identiteit van gebruikers vast te stellen.

TOETSINGSKADER

- Formeel beleid en procedures voor gebruikersauthenticatie en Identity & Access Management zijn gedefinieerd, gedocumenteerd, geformaliseerd en gecommuniceerd. Hieronder valt ook de toestemmingsprocedure voor de data- of systeemeigenaar die toegangsrechten toekent.
- Voor logische toegang tot alle systemen en bronnen wordt gebruikgemaakt van toegangsbepaling en authenticatiebeheer voor alle gebruikers.
- Er is een strikte functiescheiding voor het aanvragen, toekennen, implementeren en intrekken van toegangsrechten van gebruikers.
- User ID's en toegangsrechten worden bijgehouden in een centrale opslag.
- Ongepaste of inactieve gebruikersrechten worden tijdig uitgeschakeld.
- Het gebruik van tweefactorauthenticatie wordt afgedwongen voor niet vertrouwde omgevingen en kritieke systemen.

VOORBEELDMAATREGELEN

1. In het IBP-beleid (norm 1.2) zijn de kaders voor authenticatie gedefinieerd.
2. Er is een proces voor het aanvragen, toekennen, toewijzen en intrekken van toegang.
3. Op een centrale plek worden de user ID's en toegangsrechten bijgehouden.
4. Bij ongepaste gebruikersrechten vindt directe intrekking plaats.
5. Periodiek wordt gecontroleerd op inactieve gebruikers en worden inactieve gebruikers uitgeschakeld.
6. Bij niet vertrouwde omgevingen (bijvoorbeeld inloggen via intranet) of bij kritieke systemen wordt tweefactorauthenticatie toegepast. Uitzondering hierop kan zijn een bedrijfskritische applicatie waar (jonge) leerlingen op inloggen, omdat dit simpelweg te veel vraagt van de gebruiker. In dat geval verdient het de aanbeveling om een risicoanalyse uit te voeren voor benodigde mitigerende maatregelen.

11.3 Mobiele apparaten en telewerken

NORM

SM.03

Informatiebeveiliging wordt geborgd bij het gebruik van mobiele apparaten en telewerk-faciliteiten. Mobile device management, versleuteling en bescherming tegen malware zijn aanwezig om de risico's te beperken.

Waarom doen we dit?

Het gebruik van mobile device management, versleuteling en bescherming tegen malware helpen bij de bescherming van gegevens van de organisatie.

TOETSINGSKADER

- Formeel beleid en procedures voor het beveiligen van mobiele apparaten en/of telewerk-faciliteiten worden gedocumenteerd en gecommuniceerd (mobile device management).
- Anti-malware-software op mobiele apparaten wordt up-to-date gehouden.
- In geval van verlies of diefstal wordt de communicatie met gecentraliseerde applicaties afgesloten.
- Er worden geen bedrijfsgegevens opgeslagen op telewerkfaciliteiten thuis of elders (zero footprint).
- De vertrouwde (logische) werkplek is beschermd tegen malware.
- Bedrijfsgegevens in niet vertrouwde omgevingen worden alleen afgedrukt na een risicobeoordeling.

VOORBEELDMAATREGELEN

1. Mobile device management of mobile application management (MDM/MAM) wordt gebruikt voor het beveiligen van mobiele apparaten of telewerkfaciliteiten. Dit wordt opgenomen in het IBP-beleid (norm 1.2). Het MDM of MAM moet dusdanig zijn ingesteld dat invulling wordt gegeven aan de elementen van het toetsingskader.
2. Er is een Gedragscode *Veilig gebruik ICT-middelen en persoonsgegevens* voor zowel leerlingen als medewerkers opgesteld. Hierbij worden de elementen uit de voorbeeldgedragscode toegepast.

11.4 Logging

NORM

SM.04

Eisen voor logging zijn gedefinieerd op basis van monitoring- en rapportagebehoeften en geïmplementeerd in systemen, databases en netwerkcomponenten. Logs worden periodiek beoordeeld op indicaties van ongepaste of ongebruikelijke activiteiten en er worden adequate follow-up-acties gedefinieerd. Bewaartermijnen van logs en toegangsrechten zijn in lijn met de business requirements.

Waarom doen we dit?

Logging helpt bij het op tijd opmerken van ongepaste of ongebruikelijke activiteiten en het uitvoeren van vervolgacties. Bewaartermijn worden vastgesteld om te borgen dat voldaan wordt aan wet- en regelgeving.

TOETSINGSKADER

- Eisen voor logging zijn formeel vastgelegd; de procedures en toegepaste technieken voor het onderhouden, opslaan en evalueren van logging zijn gedocumenteerd, formeel vastgelegd, en gebaseerd op risico-analyse.
- De procedure is conform business requirements.
- Het loggen van ongebruikelijke activiteiten en incorrecte of gebrekkige logging wordt gedocumenteerd, geanalyseerd en opgevolgd met gepaste maatregelen.

VOORBEELDMAATREGELEN

1. Op basis van een expliciete risicoafweging wordt per applicatie bepaald hoelang de logging bewaard dient te worden en of er aanvullende eisen voor de logging zijn.
2. Een logregel bevat minimaal informatie over de gebeurtenis of handeling, welke gebruiker deze uitvoert, vanaf welk apparaat dit gebeurt, het resultaat van de actie en een datum en tijdstip van de handeling.
3. Ook activiteiten van systeembeheerders worden vastgelegd in de logging.
4. Er zijn waarborgen dat de logging niet gewijzigd kan worden. Eventuele wijzigingen in logging of pogingen tot het verwijderen van logging dienen vastgelegd te worden in de logging zelf.
5. Er vindt periodieke controle van de logging plaats om ongebruikelijke activiteiten te ontdekken. Grotere organisaties kunnen hiervoor bijvoorbeeld een SIEM (Security Incident en Event Managementsysteem) voor inzetten zodat automatische controle plaatsvindt en ook om na te gaan of de logging correct plaatsvindt.
6. IT heeft een overzicht van alle logbestanden binnen de organisatie.

11.5 Testen van, inspectie van en toezicht op beveiliging

NORM

SM.05

Implementatie van IT-beveiliging wordt proactief getest en bewaakt. IT-beveiliging moet regelmatig worden getoetst om ervoor te zorgen dat de door de organisatie goedgekeurde baseline voor informatiebeveiliging wordt gehandhaafd. Een log- en bewakingsfunctie maakt vroegtijdige preventie en/of detectie en daaropvolgende tijdige rapportage van ongebruikelijke en/of abnormale activiteiten die moeten worden aangepakt, mogelijk.

Waarom doen we dit?

Testen, inspectie en monitoring hebben tot doel om tijdig ongebruikelijke en abnormale activiteiten te detecteren en aan te pakken.

TOETSINGSKADER

- Er zijn procedures en beleid voor het scannen, testen en beheren van IT-beveiliging gedefinieerd en geïmplementeerd. Deze zijn goedgekeurd door het bevoegd gezag.
- Er is een beveiligingsbaseline geïmplementeerd voor alle IT-componenten die essentieel zijn voor bedrijfsvoering.
- Penetratietesten en social engineering-testen worden gepland en periodiek uitgevoerd.
- Er is een log- en controlefunctie ingericht voor vroegtijdige preventie en/of detectie en vervolgens tijdige melding van ongewone en/of abnormale activiteiten. Er wordt extra aandacht besteed aan cybersecurity-dreigingen.

VOORBEELDMAATREGELEN

1. Voor de beveiligingsbaselines, zie norm 11.1.
2. Er is vastgelegd en vastgesteld door het bevoegd gezag hoe vaak en op welke wijze getest wordt of de informatiebeveiliging op orde is. Dit gebeurt in een audit- en controleplan. Hiervoor kan gebruikgemaakt worden van het Voorbeeld *Audit- en controleplan*. Daarin staat vastgelegd welke systemen dat jaar op welke wijze worden getoetst.
3. Ten minste eens per twee jaar vindt een penetratietest plaats binnen (een kritiek systeem van) de organisatie en jaarlijks worden (geautomatiseerde) kwetsbaarheidsanalyses uitgevoerd.

11.6 Patchmanagement

NORM

SM.06

Beschikbare patches en/of beveiligingsfixes worden geïnstalleerd in overeenstemming met vooraf vastgesteld en goedgekeurd beleid (inclusief dat voor besturingssystemen, databases en geïnstalleerde applicaties) en aanbevelingen van CSIRT en/of leveranciers.

Waarom doen we dit?

Afwezigheid van patches of beveiligingsoplossingen kan ertoe leiden dat bekende kwetsbaarheden worden misbruikt om ongeautoriseerde toegang tot de IT-infrastructuur te verkrijgen.

TOETSINGSKADER

- Er is een formeel vastgelegd beleid voor patchmanagement.
- Patchmanagement is op organisatieniveau geïmplementeerd en gedocumenteerd, in lijn met change management.
- Patches worden in de basis overgenomen in samenwerking met CSIRT.
- IT-personeel checkt handmatig de patchlevels van besturingssystemen, databases en applicaties.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een beleid voor patchmanagement. De opbouw van de procedure bevat de elementen die aangereikt worden in de Handreiking *Beheerprocessen*. Er kan gebruik worden gemaakt van het Format *Beleid patchmanagement*.
2. Het bevoegd gezag heeft de change managementprocedure vastgesteld.
3. Controle op patchlevels vindt met regelmaat plaats en wordt vastgelegd.

11.7 Threat en Vulnerability Management

NORM

SM.07

Er is een proces voor Threat en Vulnerability Management geïmplementeerd om bedreigingen te identificeren en kwetsbaarheden, die kunnen leiden tot een verslechtering van de prestaties van of een aanval op bedrijfsmiddelen, tijdig te detecteren en te verhelpen. Het aantal aanvalsvectoren wordt ook beschouwd, waardoor de algehele blootstelling wordt verminderd.

Waarom doen we dit?

Threat en Vulnerability Management helpt in het verkrijgen van inzicht in de manieren waarop en door wie de organisatie zou kunnen worden aangevallen.

TOETSINGSKADER

- Er is een formeel vastgelegd proces voor Threat en Vulnerability Management (inclusief samenwerking met CSIRT) geïmplementeerd, gedreven vanuit compliance en bekende risico's.
- Er is een tool voor het beoordelen van kwetsbaarheden die waarschijnlijk met scans vanuit verschillende bronnen gevoed wordt.

VOORBEELDMAATREGELEN

1. IT heeft een vastgestelde procedure voor Threat en Vulnerability Management geïmplementeerd. Hiervoor kan gebruikgemaakt worden van de Handreiking *Beheerprocessen*.
2. Er is een tool beschikbaar voor vulnerability scanning binnen de organisatie en deze wordt met regelmaat ingezet. Resultaten worden vastgelegd.

11.8 Beschikbaarheid en bescherming van infrastructuur

NORM

SM.08

Interne beheers-, beveiligings- en auditmaatregelen worden geïmplementeerd tijdens configuratie, integratie en onderhoud van hardware en infrastructuursoftware om middelen te beschermen en beschikbaarheid en integriteit te waarborgen. Verantwoordelijkheden voor het gebruik van gevoelige infrastructuurcomponenten zijn duidelijk gedefinieerd en bekend bij degenen die infrastructuurcomponenten ontwikkelen en integreren. Het gebruik ervan wordt gecontroleerd en geëvalueerd.

Waarom doen we dit?

Door de IT-infrastructuur te beveiligen wordt de beschikbaarheid en integriteit gewaarborgd.

TOETSINGSKADER

- Er is een helder gedefinieerd en door iedereen begrepen proces voor de bescherming en beschikbaarheid van de IT-infrastructuur.
- De procesbeschrijving is in lijn met de business requirements en goedgekeurd door het bevoegd gezag.
- De verantwoordelijkheden voor het gebruik van gevoelige componenten van de infrastructuur zijn gedefinieerd en begrepen door de ontwikkelaars van infrastructuur-componenten en degenen die ze implementeren.
- Het testen betreft o.a. de functionaliteit, beveiliging, beschikbaarheid en integriteit, en eventueel andere aanbevelingen van de leverancier.
- Test- en productieomgevingen van de IT-infrastructuur zijn van elkaar gescheiden.
- Alle applicatiesoftware wordt voor installatie getest in een gescheiden maar vergelijkbare omgeving van productie. De installatie van gelicenseerde software is conform richtlijnen van de leverancier.

VOORBEELDMAATREGELEN

1. IT heeft beschreven op welke wijze bescherming en beschikbaarheid van de IT-infrastructuur plaatsvindt. Dit is vastgesteld door het bevoegd gezag.
2. Er is voor elk onderdeel van de IT-infrastructuur vastgelegd wie wijzigingen in de component mag en kan aanbrengen. Deze persoon zorgt ervoor dat kennis over de component up-to-date is. Bijvoorbeeld door het volgen van trainingen, of het lezen van alle door de leverancier gepubliceerde informatie.
3. Test- en productieomgevingen zijn altijd gescheiden van elkaar. Software wordt altijd eerst getest in de testomgeving alvorens deze geïnstalleerd wordt op productie.
4. Bij installatie van gelicenseerde software worden de richtlijnen van de leverancier toegepast.

11.9 Onderhoud van de infrastructuur

NORM

SM.09

Interne beheers-, beveiligings- en auditmaatregelen worden geïmplementeerd tijdens configuratie, integratie en onderhoud van hardware en infrastructuursoftware om middelen te beschermen en beschikbaarheid en integriteit te waarborgen. Verantwoordelijkheden voor het gebruik van gevoelige infrastructuurcomponenten zijn duidelijk gedefinieerd en bekend bij degenen die infrastructuurcomponenten ontwikkelen en integreren. Het gebruik ervan wordt gecontroleerd en geëvalueerd.

Waarom doen we dit?

Door de IT-infrastructuur te beveiligen wordt de beschikbaarheid en integriteit gewaarborgd.

TOETSINGSKADER

- Er is een duidelijk, gedefinieerd en begrepen proces voor het onderhoud van de IT-infrastructuur.
- De procesomschrijving is in lijn met change management en goedgekeurd door het bevoegd gezag.
- Het proces ondersteunt de behoeften van essentiële businessapplicaties, is in lijn met IT- en businessstrategieën en wordt consequent toegepast.
- Onderhoud wordt gepland, ingeroosterd en gecoördineerd.
- De documentatie voor systeemsoftware wordt onderhouden en periodiek geactualiseerd met leveranciersdocumentatie voor alle systemen.

VOORBEELDMAATREGELEN

1. Onderhoud van de IT-infrastructuur is opgenomen in het proces voor change management (norm 7.1).
2. De organisatie heeft een maintenance window opgesteld, zodat onderhoud alleen op vooraf vastgestelde momenten plaatsvindt.
3. IT houdt een overzicht bij van al het onderhoud en plant dit in binnen het maintenance window.
4. Na wijzigingen wordt systeemdocumentatie geüpdatet.

11.10 Cryptographic Key Management

NORM

SM.10
Er zijn beleid en procedures voor het genereren, veranderen, intrekken, vernietigen, verspreiden, certificeren, opslag, invoer, gebruik en archivering van cryptografische sleutels om sleutels te beschermen tegen aanpassing en ongeautoriseerde toegang.

Waarom doen we dit?
Cryptographic Key Management is belangrijk voor de bescherming betreffende vertrouwelijkheid, authenticiteit of integriteit van informatie. Dit beperkt het risico op diefstal, corruptie en onjuist of ongeautoriseerd gebruik van informatiemiddelen.

TOETSINGSKADER

- Er zijn formeel vastgelegd beleid en procedures voor Key Lifecycle Management.
- Beschermende maatregelen zijn geïmplementeerd om informatie veilig met elkaar te kunnen delen (bijvoorbeeld door toepassing van encryptie).
- De vertrouwelijkheid en integriteit van private keys wordt afgedwongen.

VOORBEELDMAATREGELEN

1. Indien een schoolbestuur cryptografische sleutels gebruikt bij encryptie, is er beleid vastgesteld en toegepast voor sleutelmanagement. Hiertoe kan het schoolbestuur gebruikmaken van de Handreiking *Beleid cryptografie.*

11.11 Network security

NORM

SM.11

Beveiligingstechnieken en bijbehorende beheerprocedures (zoals firewalls, beveiligingsapparatuur, netwerksegmentatie en inbraakdetectie) worden gebruikt voor het autoriseren van toegangs- en besturingsinformatiestromen van en naar netwerken. Er wordt gebruikgemaakt van *best practices* op dit gebied (bijvoorbeeld NCSC, ISO/IEC, ITSec).

Waarom doen we dit?

Network security helpt bij het tegengaan van bedreigingen van buitenaf. Door beveiligingstechnieken toe te passen, en hierbij gebruik te maken van best practices, worden diefstal, corruptie en onjuist of ongeautoriseerd gebruik van informatiemiddelen gereduceerd.

TOETSINGSKADER

- Er is een netwerkbeveiligingsbeleid vastgesteld en geïmplementeerd: procedures, richtlijnen en documentatie voor het beheer van essentiële netwerkcomponenten zijn ingericht en worden onderhouden.
- Beveiligingstechnieken worden gebruikt voor toegangsautorisatie, beheer van informatiestromen en verschillende beveiligingszones.
- Er wordt gebruikgemaakt van geschikte encryptie bij het transport van gevoelige data over niet vertrouwde netwerken.

VOORBEELDMAATREGELEN

1. Met behulp van het Overzicht *Best practices netwerkbeveiliging* stelt de organisatie vast welk beleid, procedures en richtlijnen voor de organisatie van toepassing zijn. Dit wordt vastgelegd in de security baselines (norm 11.1).
2. Bij transport van gevoelige data (bijvoorbeeld grote hoeveelheden persoonsgegevens) over een niet vertrouwd netwerk, vindt versleuteling plaats.

11.12 Beheersing van malware-aanvallen

NORM

SM.12

Preventie-, detectie- en correctiemaatregelen zijn aanwezig (met name actuele beveiligingspatches en virusscanning) in de hele organisatie om informatiesystemen en technologie te beschermen tegen malware (bijvoorbeeld virussen, wormen, spyware, spam).

Waarom doen we dit?

De gevolgen van malware kunnen enorm zijn. Door de juiste maatregelen te treffen wordt het risico hierop beperkt en wanneer er toch een inbreuk plaatsvindt de gevolgschade verminderd.

TOETSINGSKADER

- Er is anti-malwarebeleid gedefinieerd, gedocumenteerd en gecommuniceerd.
- Medewerkers zijn zich bewust van hun verantwoordelijkheid om zich aan het beleid te houden.
- Geautomatiseerde antivirussoftware is in gebruik en formeel vastgelegd.
- Beveiligingssoftware (versies en patches) wordt centraal gedistribueerd en bevat up-to-date virusdefinities.
- Alle (inkomende en uitgaande) e-mail wordt gefilterd op spam en malware.
- Er zijn maatregelen genomen om het verspreiden van malware te beperken.

VOORBEELDMAATREGELEN

1. In de security baselines is opgenomen welke anti-malwaremaatregelen technisch genomen worden (norm 11.1).
2. In de activiteiten voor beveiligingsbewustwording van medewerkers én leerlingen wordt malware expliciet opgenomen.
3. E-mail, zowel inkomend als uitgaand, wordt gescand en gefilterd op spam en malware.
4. Netwerksegmentatie wordt toegepast om verspreiding te kunnen beperken.
   Zie hiervoor informatie van de IBD.

11.13 Bescherming van beveiligingstechnologie

NORM

SM.13
Technologie gerelateerd aan beveiliging is bestand gemaakt tegen manipulatie en beveiligingsdocumentatie wordt niet onnodig openbaar gemaakt.

Waarom doen we dit?
Door technologie bestand te maken tegen manipulatie en documenten hierover niet openbaar te maken wordt het kwaadwillenden moeilijker gemaakt om systemen te compromitteren.

TOETSINGSKADER

- Er zijn beleid en procedures opgesteld om de gevolgen van een inbreuk in de beveiliging te beperken (deze bevatten specifiek beheersmaatregelen voor configuration management, applicatietoegang, databeveiliging en fysieke beveiligingseisen).
- Beveiligingsfuncties zijn ontworpen om wachtwoordregels (zoals minimumlengte, soort karakters, geldigheidsduur en voorkomen van hergebruik) te ondersteunen.
- Toegang is geautoriseerd en op de juiste wijze goedgekeurd.

VOORBEELDMAATREGELEN

1. Alle beveiligingsmaatregelen die er zijn voor andere applicaties worden expliciet ook toegepast op technologie die beveiliging moet borgen. Zodat inbreuk op beveiligingstechnologie zo moeilijk mogelijk wordt gemaakt.
2. Documentatie over beveiliging wordt niet openbaar gemaakt. Bij opslag en verzenden van deze documentatie worden de maatregelen toegepast die gelden bij een hoog vertrouwelijke classificatie.

12 Fysieke beveiliging

Welke onderwerpen staan in dit domein?
Bij fysieke beveiliging gaat het om de maatregelen die genomen worden om een pand of specifieke ruimten binnen een pand te beschermen. Een school heeft een vrij open karakter. Dat kenmerk maakt dat fysieke beveiliging bij de meeste scholen niet zal gaan om de beveiliging van het gehele pand, al is bijvoorbeeld een alarm voor de nacht in veel gebouwen prima denkbaar.

Maar ongeacht het open karakter van een school, wil je bepaalde ruimten wel extra beveiligen. Wellicht is er een ruimte waarin nog fysieke dossiers staan met hierin personeelsgegevens of oude leerlingendossiers. Of heb je eigen servers binnen het pand die belangrijk zijn voor de continuïteit. Of heb je slimme leerlingen die, wanneer ze toegang hebben tot computers zonder toezicht, zich misdragen op het internet (script kiddies). Dit zijn redenen om beheersmaat-regelen te nemen. Een simpel slot op de deur kan al zo'n beheersmaatregel zijn.

Wie is verantwoordelijk?

Eindverantwoordelijkheid ligt bij het bevoegd gezag. Fysieke beveiliging is qua uitvoering lang niet altijd bij een eenduidige rol belegd. In elk geval zal een verantwoordelijk manager het in de portefeuille moeten hebben en zorgen dat uitvoering hiervan plaatsvindt. Het kan gekoppeld zijn aan bijvoorbeeld facilitaire zaken. De IBP-medewerker kan op basis van een risicoanalyse adviseren welke maatregelen wenselijk zijn.

Ondersteuningsproducten

Beschikbaar:

- Handreiking *Cameratoezicht* (zie Aanpak IBP)
- Modelreglement *Cameratoezicht* (zie Aanpak IBP)

In ontwikkeling/te ontwikkelen:

- *Format Autorisatiematrix fysieke beveiliging*

12.1 Fysieke beveiligingsmaatregelen

NORM

PH.01

Voor specifieke (kantoor)ruimten waarin gevoelige informatie aanwezig is, of IT-componenten staan, heeft de organisatie fysieke beveiligingsmaatregelen vastgesteld en geïmplementeerd in overeenstemming met de organisatie-eisen, zodat de toegang tot informatiesystemen op passende wijze wordt beperkt en die er tevens voor zorgen dat risico's met betrekking tot diefstal, temperatuur, brand, rook, water, trillingen, terreur, vandalisme, stroomuitval, chemicaliën of explosieven effectief worden voorkomen, gedetecteerd en beperkt. Toegang tot deze ruimten wordt gemotiveerd, geautoriseerd, geregistreerd en gemonitord. Dit geldt voor alle personen die de ruimten betreden, inclusief personeel, tijdelijk personeel, klanten, leveranciers, bezoekers of welke andere derde partij dan ook.

Waarom doen we dit?

Door toegang tot specifieke ruimten (met gevoelige informatie dan wel IT-gerelateerde componenten) binnen de scholen te motiveren, te autoriseren, te registreren en te monitoren wordt de integriteit en beschikbaarheid van IT-componenten niet in gevaar gebracht.

TOETSINGSKADER

- Er is een alomvattend, op risico's gebaseerd beleid inzake fysieke beveiliging, dat is gedocumenteerd, gecommuniceerd en wordt ondersteund door (toegangs)systemen ten behoeve van de bescherming en ondersteuning van medewerkers (tijdelijke werknemers, klanten, leveranciers, bezoekers, et cetera) en voor incidentrespons en -rapportage.
- Het beleid is goedgekeurd door het bevoegd gezag.
- Er zijn effectieve maatregelen genomen om bedreigingen en ongeautoriseerde toegang tot terrein en gebouwen of het meenemen van apparatuur te voorkomen, te detecteren en tegen te houden.
- Fysieke beveiligingsmaatregelen zijn passend voor de organisatie en worden actief meegewogen vanaf de eerste fase van een eventuele verhuizing of verbouwing; er wordt rekening gehouden met ontwerp- en certificeringseisen voor zonering en controle.
- Verantwoordelijkheden en eigenaarschap zijn duidelijk vastgesteld.

VOORBEELDMAATREGELEN

1. Fysieke beveiliging maakt onderdeel uit van het IBP-beleid (norm 1.2).
2. Op basis van een risicoanalyse is bepaald welke maatregelen genomen moeten worden. Deze risicoanalyse wordt ten minste elke drie jaar herhaald.
3. Indien cameratoezicht wordt ingezet, wordt de Handreiking *Cameratoezicht* en het Modelreglement *Cameratoezicht* toegepast door het schoolbestuur.
4. Over de status van maatregelen die nog niet geïmplementeerd zijn wordt periodiek gerapporteerd aan het schoolbestuur.
5. Bij verhuizing of verbouwing wordt fysieke beveiliging meegenomen in het ontwerp op basis van een risicoanalyse.

12.2 Beheer van fysieke toegangsrechten

NORM

PH.02

Procedures worden vastgesteld en gevolgd om toegang tot IT-kritieke ruimtes of datacenters (zoals locaties, gebouwen en ruimten) toe te staan, te beperken en in te trekken, afhankelijk van organisatiebehoeften, inclusief noodtoegang. Adequate beveiligingsmaatregelen (zoals slot op deur, toegangssysteem met kaartsleutel, cijferslot, et cetera) worden gebruikt om fysieke toegang tot computerfaciliteiten waarin zich belangrijke applicaties bevinden te beperken.

Waarom doen we dit?

Door de fysieke toegangsrechten uit te geven aan personen die ter vervulling van hun functie daartoe gerechtigd zijn en in te trekken indien zij een andere functie gaan bekleden of de organisatie verlaten en hiervan een goede administratie bij te houden is inzichtelijk wie welke bevoegdheid heeft en deze wel al dan niet hoort te hebben.

TOETSINGSKADER

- Er worden formeel vastgelegde procedures voor de administratie van fysieke toegang toegepast.
- Er worden beveiligingsmaatregelen en toegangsbeperkingen toegepast zodat alleen geautoriseerd personeel fysieke toegang heeft tot gebouwen, IT-kritieke omgevingen of datacenters.
- Toegang tot fysieke IT-omgevingen (serverruimtes) wordt verleend op basis van functie en verantwoordelijkheden.
- Er zijn procedures om de toegangsprofielen up-to-date te houden.
- Er is een proces geïmplementeerd om alle toegangen tot fysieke IT-omgevingen te controleren en te bewaken, waarbij alle bezoekers, inclusief leveranciers en onderhoudspersoneel, worden geregistreerd.
- Verantwoordelijkheden en eigenaarschap zijn duidelijk toegewezen en gecommuniceerd.

VOORBEELDMAATREGELEN

1. IT-kritieke ruimtes hebben toegangsbeperkende maatregelen. Bij voorkeur wordt hier gebruikgemaakt van een toegangssysteem (met pas) en niet alleen een sleutel.
2. Met een risicoanalyse wordt bepaald welke andere fysieke maatregelen noodzakelijk zijn (bijvoorbeeld een alarmsysteem in de nacht).
3. Het schoolbestuur heeft een overzicht waarin is vastgelegd welke rol/functie toegang krijgt tot IT-kritieke ruimtes of datacenters en waarom. Het schoolbestuur kan hiervoor gebruikmaken van het Format *Autorisatiematrix fysieke beveiliging*.
4. Er is schriftelijke vastlegging van de toekenning van nieuwe toegangsrechten.
5. Er vindt vastlegging plaats van toegang tot IT-kritieke ruimtes (kan ook door middel van toegangssysteem).

13 IT-operatie

Welke onderwerpen staan in dit domein?
De onderwerpen binnen dit domein zijn vrij technisch van aard en betreffen feitelijk een drietal standaard IT-beheeractiviteiten die geborgd dienen te worden. In welke mate dit noodzakelijk is, of beter gezegd: of dit überhaupt voor een school allemaal van toepassing is, is afhankelijk van welke IT-taken zelf uitgevoerd worden en wat er uitbesteed is.

Het gaat binnen dit domein namelijk over het geautomatiseerd uitvoeren van standaard-processen, het maken van back-ups en hebben van herstelprocedures, en capacity and performance management (heb je bijvoorbeeld voldoende servercapaciteit staan wanneer de organisatie groeit en er meer gebruik wordt gemaakt van een specifieke applicatie).

Wie is verantwoordelijk?

De eindverantwoordelijkheid ligt bij het bevoegd gezag. De uitvoering van de normen binnen dit domein vallen onder verantwoordelijkheid van de IT-verantwoordelijke. Uitvoering geven aan de normen gebeurt door IT'ers binnen de afdeling. Bij veel scholen zullen niet al deze normen van toepassing zijn vanwege de hoge mate van uitbestede IT-dienstverlening binnen het funderend onderwijs.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Handreiking *Back-up en herstel*

13.1 Job processing

NORM

OP.01

De organisatie heeft procedures voor geautomatiseerde job scheduling. Taakactiviteiten worden gecontroleerd en omvatten:

- het gebruik van interfaces tussen relevante systemen om te bevestigen dat de datatransmissies volledig, nauwkeurig en geldig zijn.
- de resultaten van de back-ups om de succesvolle uitvoering te bevestigen.

Storingen worden geregistreerd en opgelost via de procedure voor incidentmanagement.
De mogelijkheid om taakschema's, batchtaken en geautomatiseerde interfaces te wijzigen is beperkt tot geautoriseerde personen.

Waarom doen we dit?

De procedures zorgen ervoor dat controle van de automatische activiteiten (zoals back-ups of dagelijkse gegevensuitwisselingen) plaatsvindt en storingen tijdig geïdentificeerd en opgelost kunnen worden.

TOETSINGSKADER

- Een runbook voor job scheduling is beschikbaar en is afgestemd op de bedrijfsdoelstellingen (overeengekomen door systeem- of proceseigenaar).
- Het runbook bevat gedetailleerde informatie en instructies.
- Job processing en interfacebewaking worden centraal geïmplementeerd en worden centraal beheerd, inclusief de correlatie tussen verschillende systemen.
- Uitzonderingen of afwijkingen in de job processing worden geregistreerd via het incident-managementproces.

VOORBEELDMAATREGELEN

1. Wanneer het schoolbestuur applicaties heeft die data uitwisselen en zelf back-ups maakt van systemen (dus niet bij een leverancier heeft belegd), zorgt het voor een overzicht van job scheduling (een runbook). Hierin staat beschreven welke taak op welke wijze wordt uitgevoerd en wat er gebeurt bij afwijkingen.

13.2 Procedures voor back-up en herstel

NORM

OP.02

De organisatie heeft een strategie geïmplementeerd voor het maken van back-ups van relevante data en programma's. Back-up en herstelprocedures zijn formeel gedefinieerd en geïmplementeerd voor alle daarvoor aangewezen systemen. Het back-upschema en de retentieperiode zijn in lijn met de door de organisatie geaccepteerde risico's voor dataverlies gebaseerd op de gevoeligheid van het systeem en de kosten voor handmatig herstel. Herstelprocedures worden periodiek getest en gedocumenteerd.

Waarom doen we dit?

Door de strategie voor back-up en herstel vast te stellen en daar procedures op in te richten en deze regelmatig te testen, vermindert het risico om meer data te verliezen dan acceptabel is voor de organisatie bij een incident en verminderen de kosten van herstel.

TOETSINGSKADER

- Er zijn passende procedures en beleid voor de back-up van systemen, applicaties, data en documentatie, en deze nemen zowel organisatie- als beveiligingseisen in overweging.
- Beleid en procedures zijn in lijn met organisatiebehoeften en goedgekeurd door het bevoegd gezag.
- De verantwoordelijkheden voor het maken, herstellen en bewaken van back-ups zijn duidelijk toegewezen.
- De prioriteit voor dataherstel is gebaseerd op eisen die de organisatie heeft bepaald en procedures voor de continuïteit van IT-diensten.

VOORBEELDMAATREGELEN

1. Voor alle systemen, applicaties en dataverwerkingen is bepaald welke eisen er zijn ten aanzien van back-up en herstelprocedures. Dit is vastgelegd in een beleidsdocument en in procedures die voldoen aan de eisen zoals verwoord in de Handreiking *Back-up en herstel*.
2. Het bevoegd gezag heeft het beleid en de bijbehorende procedures vastgesteld.
3. Dataherstel is opgenomen in het bedrijfscontinuïteitsplan (zie norm 14.1).

13.3 Capacity and Performance Management

NORM

OP.03

De organisatie heeft procedures geïmplementeerd om ervoor te zorgen dat de prestaties en capaciteit van IT-services en de IT-infrastructuur de overeengekomen servicedoelstellingen op een kosteneffectieve en tijdige manier kunnen realiseren. Capacity and performance management houdt rekening met alle middelen die nodig zijn om de IT-service te leveren en met plannen voor korte, middellange en lange termijn business requirements, inclusief het voorspellen van toekomstige behoeften op basis van eisen voor werkbelasting, opslag en onvoorziene gebeurtenissen.

Waarom doen we dit?

Om aan gebruikersbehoeften te kunnen blijven voldoen, is het belangrijk om deze behoeften te anticiperen, en de capaciteit van IT-services daarop af te stemmen, bijvoorbeeld op het gebied van bandbreedte of opslagruimte. Capacity and performance management is van belang om de capaciteit en prestaties van de IT-services te monitoren en te beoordelen, zodat tijdig kan worden ingegrepen als uitbreiding of verbetering van de systemen noodzakelijk blijkt.

TOETSINGSKADER

- Er is een proces (en technologie) gedefinieerd en geïmplementeerd om samenhangende tracking en geautomatiseerde rapportage van "raw performance metrics" op server- of partition-niveau te bewerkstelligen.
- De geautomatiseerde periodieke rapportage op basis van metrics wordt voor het grootste deel van de infrastructuur gedaan. Deze rapportages maken het signaleren van trends en problemen mogelijk en geven beperkt inzicht in toekomstige behoeften.

VOORBEELDMAATREGELEN

1. Wanneer men eigen IT in huis heeft, wordt actief gemonitord of er voldoende capaciteit beschikbaar is (bijvoorbeeld servercapaciteit en opslagcapaciteit) en of de performance voldoet.
2. Bij afwijkingen wordt de benodigde actie ondernomen.

14 Bedrijfscontinuïteitsmanagement

Welke onderwerpen staan in dit domein?
In dit domein gaan de normen over het voorbereid zijn op grote verstoringen. Dit begint bij het weten welke processen kritiek zijn en snel opgestart dienen te worden bij een verstoring. Bij het onderwijs hebben we het dan al snel over het primaire proces van het verzorgen van onderwijs en het bekijken welke zaken randvoorwaardelijk zijn om hier doorgang aan te kunnen geven. Denk bijvoorbeeld aan het hebben van een fysiek gebouw om leerlingen te ontvangen, of een ondersteunende applicatie met internet om onderwijs op afstand te kunnen verzorgen. Daarnaast moet in kaart gebracht worden welke grote calamiteiten denkbaar zijn.

Zo geldt voor iedereen dat er een risico is op een ransomware-aanval, maar is het afhankelijk van de locatie of overstroming of ontsporing van een chloortrein meegenomen moet worden. Op basis van deze informatie kan bepaald worden hoe continuïteitsplannen en herstelplannen van een school eruit moeten zien. Deze plannen moeten vervolgens met regelmaat getest worden. Ook is er specifiek aandacht voor de wijze waarop met back-ups wordt omgegaan, aangezien deze essentieel zijn voor herstel van data. Tot slot is crisismanagement van belang, zodat bij grote verstoringen er een team is dat weet wat er moet gebeuren en duidelijk is wie welke rol heeft bij een crisis. Het crisismanagement moet ook regelmatig geoefend worden.

Wie is verantwoordelijk?

Eindverantwoordelijkheid ligt bij het bevoegd gezag. Afhankelijk van de grootte van de organisatie, wordt de verantwoordelijkheid voor de uitvoering vaak belegd bij een risicomanager, de verantwoordelijke voor IBP, IT of bedrijfsvoering.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Handreiking *Aanpak BCM*
- Template *Bedrijfscontinuïteitsplan (BCP)*
- Scenariokaarten
- Crisismanagementoefeningen

14.1 Bedrijfscontinuïteitsplanning

NORM

BC.01

Business- en IT-continuïteitsplannen worden ontwikkeld op basis van het framework en zijn ontworpen om de impact van een grote verstoring op de belangrijkste bedrijfsfuncties en bedrijfsprocessen te verminderen. De plannen zijn gebaseerd op risicogericht inzicht in potentiële bedrijfsimpact en houden rekening met vereisten betreffende veerkracht, alternatieve verwerkings- en herstelmogelijkheden in alle kritieke IT-services. De plannen omvatten ook gebruiksrichtlijnen, rollen en verantwoordelijkheden, procedures, communicatieprocessen en de testmethode.

Waarom doen we dit?

Door bedrijfs- en IT-continuïteitsplannen te ontwikkelen kan tijdens een grote storing adequaat worden gehandeld, zodat de gevolgen worden gereduceerd.

TOETSINGSKADER

- Bedrijfs- en IT-continuïteitsplannen zijn gedefinieerd, geïntegreerd en goedgekeurd door het senior management.
- De organisatie heeft een bedrijfsimpactanalyse uitgevoerd, op basis waarvan recoverytime-doelen zijn bepaald en volledig gedocumenteerde IT-herstelplannen en bedrijfs-continuïteitsplannen zijn opgesteld om deze doelen te bereiken.
- De plannen betreffen gebruikershandleidingen, rollen, verantwoordelijkheden, crisismanagement, communicatieprocessen en de testmethode.
- Dankzij deze plannen kan de organisatie waarschijnlijk belangrijke operationele processen voortzetten in het geval van een grote onderbreking.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een bedrijfscontinuïteitsplan opgesteld en vastgesteld. Er kan gebruikgemaakt worden van de Handreiking *Aanpak BCM*, waarin een praktische aanpak voor BCM staat beschreven. Van het uitvoeren van een bedrijfs-impactanalyse (BIA) tot het bepalen van herstelstrategie en -aanpak. Wanneer gebruik wordt gemaakt van het Template *Bedrijfscontinuïteitsplan*, geeft het schoolbestuur invulling aan alle aspecten bij de norm.

14.2 Testen van Disaster Recovery

NORM

BC.02

Bedrijfs- en IT-continuïteitsplannen worden regelmatig getest om ervoor te zorgen dat essentiële systemen en diensten effectief kunnen worden hersteld, dat tekortkomingen worden aangepakt en dat het plan relevant blijft. Dit vereist een zorgvuldige voorbereiding, documentatie, rapportage de resultaten, de implementatie van een actieplan. De mate van testherstel in afzonderlijke applicaties varieert van geïntegreerde testscenario's tot end-to-end-tests en geïntegreerde leverancierstests.

Waarom doen we dit?

Door het testen van bedrijfs- en IT-continuïteitsplannen komen tekortkomingen aan het licht en kunnen vervolgens de plannen worden verbeterd.

TOETSINGSKADER

- Bedrijfs- en IT-continuïteitsplannen worden getest via goedgekeurde, geïntegreerde test-/herstelscenario's.
- Bedrijfs- en IT-continuïteitsplannen worden op regelmatige basis getest (ten minste eenmaal per jaar) om ervoor te zorgen dat essentiële systemen effectief kunnen worden hersteld, dat tekortkomingen worden aangepakt en dat het plan up-to-date blijft.
- Er is voorzien in een gedegen voorbereiding, documentatie, rapportage van de testresultaten en, afhankelijk van de resultaten, uitvoering van een actieplan.

VOORBEELDMAATREGELEN

1. Voor kritische applicaties wordt jaarlijks getest of de continuïteitsplannen werken.
2. De tests worden zorgvuldig gedocumenteerd, zodat de resultaten waar nodig leiden tot verbeteracties.

14.3 Offsite back-upopslag

NORM

BC.03

Alle kritieke back-upmedia, documentatie en andere IT-resources die nodig zijn in het kader van IT-herstel- en bedrijfscontinuïteitsplannen worden offsite opgeslagen. De inhoud van back-upopslag wordt bepaald in samenspraak met de eigenaren van bedrijfsprocessen en IT-personeel. Het beheer op de externe opslagfaciliteit werkt op basis van het beleid voor dataclassificatie en de gebruikelijk manier van mediaopslag van de organisatie. IT-management zorgt ervoor dat offsite-arrangementen periodiek, ten minste jaarlijks, worden beoordeeld op inhoud, bescherming tegen omgevingsfactoren en beveiliging. De compatibiliteit van hardware en software voor het herstellen van gearchiveerde gegevens is gewaarborgd en gearchiveerde gegevens worden periodiek getest en ververst.

Waarom doen we dit?

Back-ups en andere IT-resources die extern zijn opgeslagen, worden niet aan dezelfde fysieke dreigingen blootgesteld als de IT-infrastructuur (zie 12.1). Deze blijven dus inzetbaar op het moment dat fysieke schade optreedt op de locatie van de IT-infrastructuur.

TOETSINGSKADER

- Er is een gedetailleerd overzicht van alle kritieke back-upmedia die off-site opgeslagen dient te worden. Het overzicht is goedgekeurd door bevoegd gezag.
- Aan het management worden duidelijke beschrijvingen van de noodzakelijke dataopslag-beheersmaatregelen gegeven over de off-site opslagfaciliteit, inclusief transport, herstelinstructies, labelen en voorraadlijsten van back-upmedia.
- De off-site regeling is in lijn met de vereisten voor bedrijfscontinuïteit en wordt periodiek geëvalueerd.

VOORBEELDMAATREGELEN

1. Op basis van de continuïteitseisen is vastgesteld welke back-ups hoe vaak gemaakt moeten worden en welke daarvan op een andere locatie opgeslagen dienen te worden. Dit overzicht is voorgelegd aan het bevoegd gezag en vastgesteld.
2. Over de wijze waarop de data worden opgeslagen, zijn duidelijke afspraken gemaakt.
3. Jaarlijks wordt bekeken of de off-site opslag nog passend is bij de eisen van de organisatie.

14.4 Gegevensreplicatie

NORM

BC.04

Gegevensreplicatie is opgezet tussen de productiefaciliteit van de organisatie en de disaster-recoveryfaciliteit, zodat kritieke financiële en operationele gegevens op korte termijn beschikbaar zijn. Replicatiestatus wordt bewaakt als onderdeel van het bewakingsproces voor systeemtaken.

Waarom doen we dit?

Als datareplicatie goed is geconfigureerd zullen tijdens een incident gegevens tijdig beschikbaar zijn.

TOETSINGSKADER

- Er is een datareplicatieproces geïmplementeerd in de faciliteiten voor productie- en disaster recovery van de organisatie.
- De organisatie heeft inzicht in welke financiële en operationele data essentieel zijn en dus gerepliceerd moeten worden. Dit is goedgekeurd door het senior management.
- In het geval van een incident zijn data op korte termijn beschikbaar.

VOORBEELDMAATREGELEN

1. Indien de businessimpactanalyse daartoe aanleiding geeft, worden gegevens realtime gerepliceerd naar een herstelfaciliteit. De inschatting is dat dit voor scholen niet aan de orde is. De kritieke systemen van scholen (bijvoorbeeld leerlingenadministratie of financiële boekhouding) zijn eigenlijk altijd uitbesteed. Dit betreft dus een eis die feitelijk altijd aan een leverancier gesteld dient te worden.

14.5 Crisismanagement

NORM

BC.05

De organisatie heeft crisismanagement ingericht om snel, grondig en gecoördineerd op incidenten te reageren, de gevolgen te verminderen en de dienstverlening binnen een redelijke tijd te herstellen.

Waarom doen we dit?

Crisismanagement heeft als doel om als organisatie adequaat te reageren tijdens calamiteiten en zo de gevolgen te verminderen.

TOETSINGSKADER

- Er is een crisismanagementplan dat onderdeel is van het bedrijfscontinuïteitsplan (BCP), waardoor de organisatie de essentiële bedrijfsvoering weer kan oppakken, terwijl het crisismanagementteam zich op de crisis richt.
- Alle betrokkenen zijn op de hoogte van de verantwoordelijkheden tijdens een crisis.
- Er zijn periodiek crisisoefeningen voor crisismanagementteams.

VOORBEELDMAATREGELEN

1. In het BCP (norm 14.1) staat het crisismanagementplan gedefinieerd.
2. Jaarlijks wordt een crisisoefening gehouden voor het crisismanagementteam.

15 Ketenbeheer

Welke onderwerpen staan in dit domein?
Het domein Ketenbeheer gaat over controle hebben op de uitbestede IT-diensten. Zeker binnen de onderwijssector worden veel Software-as-a-Service-oplossingen gebruikt (SAAS-oplossingen). Dit biedt voordelen, want de grotere organisaties die hierin gespecialiseerd zijn hebben veelal een hoger securityniveau dan een individuele school zelf zou kunnen bereiken.

Tegelijkertijd betekent het ook dat er minder directe controle over is. Daarom is het van groot belang dat men goede afspraken maakt met leveranciers over de minimale beveiligingsvereisten. Belangrijke componenten van de dienstverlening worden vastgelegd in een Service Level Agreement (SLA). Het beheren van die dienstverleningsafspraken is vervolgens van belang. Ook moet er gekeken worden naar belangrijke risico's en moeten hierop beheersmaatregelen ter mitigatie worden vastgesteld. Denk bijvoorbeeld aan geheimhoudingsverklaringen of afspraken over overdracht wanneer een nieuwe leverancier wordt gecontracteerd, maar ook boetes bij het niet voldoen aan de SLA horen hierbij. Tot slot dient men periodiek te bekijken of de leverancier voldoet aan de gestelde eisen.

Wie is verantwoordelijk?

Het bevoegd gezag is eindverantwoordelijk. De verantwoordelijkheid voor het geven van uitvoering aan de normen wordt veelal belegd bij een leveranciersmanager in geval van grotere organisaties, of de verantwoordelijke voor IT bij kleinere organisaties. Bij het aanbesteden van diensten is het van belang dat de IBP-medewerker wordt betrokken voor het vaststellen van de beveiligingseisen voor de te contracteren leverancier.

Ondersteuningsproducten

In ontwikkeling/te ontwikkelen:

- Checklist *Eisen aan leveranciers*
- Checklist *SLA*
- Handreiking *Leveranciersmanagement*
- Collectief strategisch leveranciersmanagement opzetten

15.1 Service Level Agreement

NORM

SC.01
IT-services die aan de organisatie worden geleverd, worden gedefinieerd in het contract en bijhorende SLA. Er zijn maatregelen genomen om ervoor te zorgen dat diensten voldoen aan de huidige en toekomstige behoeften van de organisatie.

Waarom doen we dit?
Een Service Level Agreement, ook wel dienstverleningsovereenkomst genoemd, zorgt voor duidelijke afspraken over onder andere het onderhoud en ondersteuning van een IT-component tussen de organisatie en de leverancier van het product.

TOETSINGSKADER

- Service levels van IT-diensten zijn gebaseerd op business requirements.
- SLA bevat afspraken over periodieke rapportage van geleverde diensten en performance.
- De gedefinieerde serviceniveaus zijn gedocumenteerd in een SLA en formeel goedgekeurd door het (senior) management en de IT-service provider.

VOORBEELDMAATREGELEN

1. Voorafgaand aan offerte-aanvraag of aanbesteding bepaalt de organisatie wat de eisen zijn die gesteld worden aan de dienst en de leverancier. Hiervoor kan gebruikgemaakt worden van de Checklist *Eisen aan leveranciers* en de IT-eisen uit *ROSA*. Denk hierbij bijvoorbeeld aan waar de opslag van data moet plaatsvinden, back-up-eisen, beschikbaarheidsniveaus en certificering voor kwaliteit en informatiebeveiliging.
2. Bij het contracteren van de dienstverlener wordt een SLA opgesteld. De SLA bevat ten minste de punten die genoemd staan in de Checklist *SLA*.
3. De SLA wordt goedgekeurd door het bevoegd gezag.

15.2 Service Level Management

NORM

SC.02

Business requirements en de manier waarop IT-services en serviceniveaus bedrijfsprocessen ondersteunen, worden periodiek geanalyseerd. Services en serviceniveaus worden besproken en overeengekomen met de organisatie en vergeleken met het huidige serviceportfolio om nieuwe of gewijzigde services of serviceniveau-opties te identificeren.

Waarom doen we dit?

Door een goed beheer van de SLA's worden afwijkingen in de prestaties van leveranciers op tijd gedetecteerd. Dit komt ten goede aan de organisatieprestaties, aangezien de leveranciers worden gebonden aan de afgesproken voorwaarden.

TOETSINGSKADER

- Er is een proces voor service level management gedefinieerd, geïmplementeerd en goedgekeurd door het bevoegd gezag.
- De performance van de services worden periodiek gerapporteerd in een service level rapport (SLR), en indien nodig besproken met de leverancier.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een proces leveranciersmanagement beschreven en vastgesteld waar service level management onderdeel van uitmaakt. De elementen die hierin opgenomen dienen te worden staan uitgewerkt in de Handreiking *Leveranciersmanagement*, evenals een voorbeelduitwerking.
2. In de SLA staat afgesproken dat er periodiek een rapportage wordt ontvangen (afhankelijk van de kriticiteit van de dienstverlening kun je hier kiezen voor maandelijks of elk kwartaal bijvoorbeeld). Deze rapportages worden beoordeeld en afwijkingen worden conform het proces van punt 1 besproken met de proceseige-naar en indien nodig met de leverancier.

15.3 Leveranciersrisicomanagement

NORM

SC.03

Risico's met betrekking tot het vermogen van leveranciers om effectieve dienstverlening op een veilige en efficiënte manier voort te zetten worden voortdurend geïdentificeerd en beperkt. Contracten voldoen aan universele zakelijke standaarden in overeenstemming met wet- en regelgeving. Risicomanagement neemt aspecten als niet-openbaarmakingsovereenkomsten (non-disclosure agreements/NDA's), escrow-contracten, voortdurende levensvatbaarheid van de leverancier, conformiteit met beveiligingseisen, alternatieve leveranciers, boetes en beloningen enzovoorts in overweging.

Waarom doen we dit?

Leveranciersrisicomanagement is van belang om een leverancier te vinden die voldoet aan de business requirements en om risico's tijdens de duur van het contract te inventariseren. Voorbeelden hiervan zijn levensvatbaarheid van de leverancier, naleving van beveiligingseisen, conventionele vergoedingen en bonussen.

TOETSINGSKADER

- Er is een proces voor leveranciersrisicomanagement gedefinieerd, geïmplementeerd en goedgekeurd door het bevoegd gezag.
- Risico's betreffende het vermogen van de leverancier om effectief en veilig (cloud)diensten te leveren worden voortdurend geanalyseerd en beperkt.
- In het proces voor leveranciersrisicomanagement wordt rekening gehouden met non-disclosure agreements (NDA's), escrow-contracten, levensvatbaarheid van leveranciers, compliance met beveiligingseisen, alternatieve leveranciers, boetes en beloningen, et cetera.
- Over niet-gemitigeerde of geaccepteerde risico's wordt periodiek aan het (senior) management gerapporteerd.
- Contracten zijn conform algemene bedrijfsstandaarden en voldoen aan wet- en regelgeving (e.g. data privacy).
- Voordat de contracten worden ondertekend wordt een assurance verkregen, die aantoont dat de levering van diensten voldoet aan wet- en regelgeving en ook aan het eigen (beveiligings)beleid.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een proces leveranciersmanagement beschreven en vastgesteld waar leveranciersrisicomanagement onderdeel van uitmaakt. De elementen die hierin opgenomen dienen te worden staan uitgewerkt in de Handreiking *Leveranciersmanagement*, evenals een voorbeelduitwerking.
2. Risico's die niet gemitigeerd worden, of geaccepteerd worden, worden besproken door het bevoegd gezag.

15.4 Interne beheersing bij derden

NORM

SC.04
De status van de interne beheersmaatregelen van externe dienstverleners wordt beoordeeld. Er zijn procedures om te zorgen dat externe dienstverleners voldoen aan wet- en regelgeving en contractuele verplichtingen.

Waarom doen we dit?
De beheersmaatregelen van externe dienstverleners en het voldoen aan de wet- en regelgeving door deze derde partij, is van belang voor de eigen organisatie, aangezien de continuïteit van de derde partij en integriteit van de geleverde IT-componenten moet worden geborgd.

TOETSINGSKADER

- Er is een formeel vastgelegd proces om te zorgen dat interne beheersing effectief toegepast wordt.
- De status van de interne beheersmaatregelen van de externe dienstverleners wordt periodiek geëvalueerd.
- Er zijn procedures om te garanderen dat externe dienstverleners zich aan de contractuele verplichtingen houden.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een proces leveranciersmanagement beschreven en vastgesteld waar toetsing van interne beheersmaatregelen van leveranciers onderdeel van uitmaakt. De elementen die hierin opgenomen dienen te worden staan uitgewerkt in de Handreiking *Leveranciersmanagement*, evenals een voorbeelduitwerking.

Deel 2

Normenkader Privacy

Privacynormen toelichting:

Voor privacy is nog geen leidend kader beschikbaar voor het onderwijs. Gedurende de ontwikkeling van dit normenkader hebben het programma Digitaal Veilig Onderwijs en SURF het initiatief genomen om gezamenlijk de privacynormen te ontwikkelen voor de gehele onderwijssector. Dit zal in de tweede helft van 2023 tot een nieuw privacy-kader leiden.

Begrippenlijst

Assurance: het verschaffen van zekerheid over informatieverwerking door een neutrale partij, om het vertrouwen bij de gebruikers van die informatie te versterken.

Autorisatiematrix: een overzicht van welke rol waar toegang toe krijgt. Bij voorkeur is dit gebaseerd op een rol of functie, zodat het need-to-know-principe wordt toegepast.

Back-up: een reservekopie van gegevens, zodat bij beschadiging of verlies van gegevensherstel kan plaatsvinden.

Capacity and performance management: het IT-beheerproces dat ervoor zorgt dat de beschikbare capaciteit overeenkomt met dat wat nodig is om te voldoen aan de eisen van de organisatie en dat hierbij ook kijkt naar toekomstige benodigdheden.

Certificeringsschema ROSA: in deze standaard worden afspraken gemaakt over het (basis) niveau van informatiebeveiliging en privacy voor toepassingen die worden gebruikt in het onderwijs (PO, VO, mbo en ho). Het certificeringsschema ROSA bepaalt het niveau voor betrouwbaarheid, integriteit en vertrouwelijkheid van een toepassing en schrijft op basis daarvan de benodigde maatregelen voor.

Change management: het beheerst doorvoeren van wijzigingen in IT.

Configuratiedatabase (CMDB): de plek waar alle configuratie-items van een organisatie zijn opgeslagen.

Cryptografie/versleuteling: de technologie van het omzetten van informatie naar een vorm die alleen door de beoogde ontvangers te lezen is. Een voorbeeld hiervan is geheimschrift: alleen als je de codering weet, kun je het bericht ontcijferen. Wanneer je cryptografische sleutels gebruikt, zul je hierop een vorm van beheer moeten voeren: Cryptographic Key Management, ook wel Key Lifecycle Management.

CSIRT: een Computer Security Incident Response Team, ook wel CERT genaamd, is een gespecialiseerd team voor het reageren op beveiligingsincidenten, met als doel schade te beperken en herstel van dienstverlening te bevorderen. In Nederland is het NCSC de nationale CSIRT en zijn er diverse sectorale CERTs. SURFcert is de bekendste binnen de onderwijssector.

Dataclassificatie: het labelen van informatie op basis van kenmerken van de informatie naar een standaardindeling, zodat bepaald kan worden welk beschermingsniveau van toepassing is en welke beheersmaatregelen toegepast dienen te worden.

Dataconversie: het verplaatsen van data van het ene systeem naar het andere, al dan niet gepaard met een omzetting van formaat. Vaak is dit noodzakelijk wanneer er een nieuw systeem wordt geïmplementeerd. Denk bijvoorbeeld aan het inzetten van een nieuw financieel systeem: de historische financiële gegevens wil je hoogstwaarschijnlijk ook in het nieuwe systeem kunnen inzien.

Enterprise Information Architecture Model: de informatiearchitectuur beschrijft de inhoudelijke samenhang en relaties tussen applicaties en gegevensverzamelingen, ook wel de informatiehuishouding genoemd, en helpt bij het verbeteren van de vindbaarheid van informatie en de wijze waarop informatie hergebruikt kan worden. Hierdoor wordt de grip op informatie vergroot.

Incidentmanagement: het proces om elke ongeplande onderbreking zo snel en goed mogelijk te herstellen.

Informatierisicomanagement: het beheersen van risico's voor informatie, systemen, applicaties en processen langs de lijnen van de betrouwbaarheidskenmerken voor informatiebeveiliging (beschikbaarheid, vertrouwelijkheid en integriteit). Met andere woorden: het gaat hier om risicomanagement binnen het informatiebeveiligingsdomein.

IST en SOLL: de IST betreft de huidige situatie, de SOLL betreft de gewenste situatie.

Job processing runbook: een gedetailleerde beschrijving van alle geautomatiseerde en herhaalbare taken en processen die binnen de IT-operatie plaatsvinden.

OTAP: een OTAP-straat is een begrip uit de IT dat de fases van software-ontwikkeling aangeeft: Ontwikkeling, Test, Acceptatie en Productie. De fases zijn feitelijk de verschillende omgevingen waarbinnen de ontwikkeling plaatsvindt. Gestart wordt met de ontwikkeling van iets nieuws, dit wordt vervolgens getest, dan wordt het opgeleverd aan acceptatie (een omgeving die zoveel mogelijk gelijk is aan productie). Als de gebruikers en verantwoordelijke akkoord zijn, kan het over naar productie (de "normale" omgeving waar gebruikers gebruikmaken van de software).

Patchmanagement: het verwerven, testen en installeren van wijzigingen die beveiligingsproblemen in software herstellen.

Penetratietesten: het toetsen van een systeem op kwetsbaarheden door daadwerkelijk te pogen in te breken op een systeem, zodat duidelijk wordt op welke punten de beveiliging aangescherpt moet worden.

Privacy by default: volgens dit principe staan voor gebruikers standaard de meest privacyvriendelijke instellingen aan.

Privacy by design: al vanaf de start van het ontwerp wordt privacy meegenomen in de ontwikkeling. Standaardproducten of -diensten staan zo ingesteld dat privacy wordt gewaarborgd. Alle opties om persoonsgegevens te delen staan standaard 'uit'.

Problem management: het beheren van een reeks incidenten met onbekende hoofdoorzaak.

Response: de wijze waarop op een incident gereageerd wordt.

RFC-formulier: een formulier waarin een Request For Change, ook wel een wijzigingsverzoek, wordt vastgelegd.

Rollback-procedure: door een rollback-procedure kun je teruggaan naar de situatie vóór de wijziging werd doorgevoerd, zodat een onvoorzien en ongewenst gevolg kan worden terug-gedraaid.

Security by design: al vanaf de start van het ontwerp wordt informatiebeveiliging meegenomen in de ontwikkeling. Hierdoor worden geen losse maatregelen genomen, maar ontstaat er een geheel aan ontwerpprincipes die gezamenlijk de veiligheid verhogen.

Service Level Agreement: SLA, ook wel dienstverleningsovereenkomst (DVO). Bijlage bij een contract waarin de kwaliteit van de dienstverlening beschreven staat. Zo weet de afnemer bijvoorbeeld welke ondersteuning hij kan verwachten, is bepaald wat de beschikbaarheidseisen van de dienst zijn en hoe snel incidenten opgelost worden.

Sleutelfunctionaris: een functionaris die cruciaal is voor de continuïteit van de organisatie. Als voorbeeld: een zeer specifieke applicatiebeheerder die niet gemakkelijk te vervangen is en waar er maar één van is binnen de organisatie, of de schoolbestuurder vanwege de kritieke informatiepositie.

Superuser: het hoogste beheeraccount in een systeem. Met andere woorden: met dit account kan vrijwel alles gewijzigd worden en daarom dient extra zorgvuldig te worden omgegaan met deze rechten

Hoe ga ik met het Normenkader IBP FO aan de slag?

Je kunt niet alles tegelijk doen, dus hoe stel je als schoolbestuur prioriteiten in de normen die je op orde wil gaan brengen. Onderstaande tabel helpt je met het aanbrengen van prioriteiten. In plaats van jouw organisatie direct op alle onderdelen te gaan scoren kun je beginnen met 'de basis op orde'. Als je dat goed in kaart hebt en de juiste acties in gang hebt gezet, kun je aan de slag met het mitigeren van de hoge en later de medium risico's. In de laatste fase is het dan tijd om de puntjes op die i te zetten. Op deze manier is de grote hoeveelheid aan normen een stuk beter hanteerbaar.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
De basis op orde	1.1 1.2	2.1				6.1 6.2 6.4	7.1 7.2 7.3		9.1 9.2 9.3			12.1		14.1 14.5	
Mitigeren *hoge* risico's			3.1 3.2 3.3	4.6			7.4 7.5 7.6	8.1 8.2	9.5	10.1 10.2 10.3 10.5	11.2 11.4 11.6 11.12 11.13	12.2	13.2	14.2 14.3	15.3
Mitigeren *medium* risico's	1.4 1.5	2.2		4.1 4.4	5.1 5.2	6.3			9.4 9.6		11.1 11.3 11.5 11.7		13.3	14.4	15.1 15.2 15.4
Verdere verfijning	1.3			4.2 4.3 4.5				8.3		10.4	11.8 11.9 11.10 11.11		13.1		