

# 1. Bestuur

In het domein Bestuur zijn vijf normen opgenomen. Deze normen geven richting en ondersteuning om de informatiebeveiliging in te richten in lijn met organisatiedoelstellingen, 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.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Adviseur informatiebeveiliging, IBP-verantwoordelijke, it-verantwoordelijke

Geraadpleegd: FG

Geïnformeerd: Medewerkers van de school, Raad van Toezicht

## GO.01 Strategie Informatiebeveiliging

### Norm

Een strategie en visie op informatiebeveiliging zijn leidend voor alle gerelateerde activiteiten en maatregelen binnen de organisatie.

### Waarom is dit nodig?

Een strategie en visie vormen de leidraad voor het nemen van goede beslissingen over de informatiebeveiliging van de organisatie. Ze geven richting en duidelijkheid bij het maken van beveiligingskeuzes en helpen om passende antwoorden te vinden op veranderingen in de schoolomgeving. Op deze manier kan de school een digitaal veilige omgeving creëren voor leerlingen, ouders en medewerkers.

### 1 - Ad hoc

1 – Ad hoc

a) Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging gebeurt ad hoc.

### 2 - Herhaalbaar

2 – Herhaalbaar

a) Een strategie en visie op informatiebeveiliging is geformuleerd, maar niet formeel vastgesteld.

### 3 - Bepaald (streefniveau)

3 – Bepaald

a) Strategie en visie op informatiebeveiliging zijn vastgesteld door het schoolbestuur.

b) Strategie en visie worden actief gecommuniceerd naar medewerkers, leveranciers en contractpartners.

### 4 - Beheerst

4 – Beheerst

a) Strategie en visie zijn leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.

b) Indien van toepassing wordt vastgelegd hoe er in lijn met strategie en visie gewerkt wordt.

c) De geldigheid en uitvoerbaarheid van de strategie en visie wordt periodiek geverifieerd.

### 5 - Continu verbeteren

5 – Continu verbeteren

a) De strategie geeft aan hoe dit de organisatie helpt haar doelstellingen te behalen.

b) Indien nodig worden strategie en visie op informatiebeveiliging bijgesteld om in te spelen op externe ontwikkelingen en veranderende doelstellingen van de organisatie.

## **Aan de slag**

1. Formuleer als schoolbestuur een strategie en visie op informatiebeveiliging.
2. Stel als schoolbestuur de strategie en visie vast.
3. Zorg ervoor dat de strategie en visie (digitaal) beschikbaar zijn, bijvoorbeeld via de website en het intranet.

## **Referentie naar andere normen en kaders**

ISO A5.1

## **Link naar relevante P normen**

## **GO.02 Beleid informatiebeveiliging**

### **Norm**

De organisatie heeft een informatiebeveiligingsbeleid beschreven, vastgesteld en gecommuniceerd naar de medewerkers. Indien van toepassing wordt het beleid actief meegedeeld aan leveranciers. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het schoolbestuur.

### **Waarom is dit nodig?**

Met een beleid zorgt het schoolbestuur voor vastgestelde richtlijnen om te voldoen aan organisatiespecifieke kaders, sectorbrede afspraken en wet- en regelgeving. Door dit actief te communiceren naar medewerkers en leveranciers, weet iedereen binnen welke kaders zij moeten handelen. Hierdoor ontstaat een veilige digitale omgeving voor leerlingen, ouders en medewerkers van je school.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen beleid opgesteld.
- b) Er zijn enkele beleidsstukken in concept.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is informatiebeveiligingsbeleid waarin de meest relevante aspecten van informatiebeveiliging zijn opgenomen.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Informatiebeveiligingsbeleid is vastgesteld door het schoolbestuur.
- b) Beleid wordt actief gecommuniceerd naar medewerkers, leveranciers en contractpartners en is digitaal (op intranet) of in hardcopy beschikbaar.
- c) Het beleid maakt onderdeel uit van het bewustwordingsprogramma.
- d) Er wordt geëvalueerd of en hoe het beleid wordt uitgevoerd.

### **4 - Beheerst**

4 – Beheerst

- a) Het informatiebeveiligingsbeleid is ingebed in/overgenomen door de organisatie en is vertaald naar onderliggende procedures, baselines en instructies.
- b) Periodiek wordt het beleid geëvalueerd, geactualiseerd en opnieuw goedgekeurd door het schoolbestuur.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

a) Periodiek wordt aan het schoolbestuur gerapporteerd of aan het informatiebeveiligingsbeleid wordt voldaan.

#### **Aan de slag**

1. Stel een informatiebeveiligingsbeleid op dat voldoet aan de eisen in de Toelichting op het template IBP-beleidsplan. Maak hiervoor gebruik van het template IBP-beleid.
2. Stel het informatiebeveiligingsbeleid vast door een handtekening op het document te zetten of via de notulen van een bestuursvergadering.
3. Controleer ten minste eens per twee jaar of er wijzigingen nodig zijn in het informatiebeveiligingsbeleid. Leg de controle vast in het document met eventuele wijzigingen die zijn doorgevoerd.
4. Bespreek het beleid ten minste een keer per jaar met elke school die onder het schoolbestuur valt.
5. Plaats het beleid op het intranet.
6. Informeer elke medewerker tijdens de inwerkperiode over het informatiebeveiligingsbeleid.
7. Neem het informatiebeveiligingsbeleid waar nodig en relevant mee in de eisen bij aanbesteding van dienstverlening.

#### **Referentie naar andere normen en kaders**

#### **Link naar relevante P normen**

## **GO.03 Planning/roadmap informatiebeveiliging**

### **Norm**

De doelstellingen, risico's en wet- en regelgeving met betrekking tot de informatiebeveiliging van de organisatie worden vertaald in een informatiebeveiligingsplan. Hierbij zijn een planning en roadmap opgesteld om invulling te geven aan de uitvoering van het informatiebeveiligingsbeleid.

### **Waarom is dit nodig?**

Steeds vaker gaat het mis: gegevens komen op straat te liggen of lessen kunnen niet doorgaan. Om de digitale veiligheid op school te verbeteren, heb je een concreet plan nodig. Een informatiebeveiligingsplan beschrijft de manier waarop je informatiebeveiliging in overeenstemming brengt met wet- en regelgeving en de doelstellingen en risico's van de school. In dit plan beschrijf je hoe jouw school de informatiebeveiliging op orde krijgt en daarmee een digitaal veilige schoolomgeving creëert.

### **1 - Ad hoc**

#### **1 – Ad hoc**

- a) Er is geen planning/roadmap informatiebeveiliging opgesteld.
- b) Er lopen enkele projecten op het gebied van it-beveiliging of deze zijn gepland.

### **2 - Herhaalbaar**

#### **2 – Herhaalbaar**

- a) Er is een planning/roadmap informatiebeveiliging opgesteld. Dit plan bestrijkt alle relevante organisatie-doelstellingen, risico's en eisen op het gebied van wet- en regelgeving.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) De planning/roadmap informatiebeveiliging is vastgesteld door het schoolbestuur.
- b) Het plan is uitgewerkt in informatiebeveiligingsbeleid en -procedures, tezamen met passende investeringen op het gebied van diensten, medewerkers, software en hardware.
- c) Gerelateerde procedures worden gecommuniceerd naar gebruikers en stakeholders.

### **4 - Beheerst**

4 – Beheerst

- a) De planning/roadmap informatiebeveiliging is ingevoerd en wordt ondersteund door (informatie)beveiligingsbeleid, procedures, diensten, medewerkers, software en hardware.
- b) De planning/radmap informatiebeveiliging wordt periodiek geëvalueerd, geactualiseerd en goedgekeurd door het schoolbestuur.

### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) De planning/roadmap informatiebeveiliging en daaraan gerelateerde projectportfolio worden periodiek gemonitord op bijvoorbeeld voortgang, bedreigingen, haalbaarheid en mate waarin aan organisatiedoelstellingen wordt voldaan.
- b) Hierover wordt gerapporteerd aan het schoolbestuur.

### **Aan de slag**

1. Stel een plan voor informatiebeveiliging op met acties om het informatiebeveiligings-beleid uit te voeren en/of te verbeteren om te voldoen aan het beleid. Dit plan kan onderdeel zijn van het bestuursbrede jaarplan.
2. Evalueer, herzie en stel als schoolbestuur elk jaar het jaarplan informatiebeveiliging vast en zorg voor de benodigde middelen.

### **Referentie naar andere normen en kaders**

ISO A5.2, A5.1, A5.31, A5.32, A5.33, A5.34, A6.3

### **Link naar relevante P normen**

## **GO.04 Informatiearchitectuur**

### **Norm**

Er is een Enterprise Information Architecture Model (EIAM) opgesteld en toegepast om applicatieontwikkeling en beslissingsondersteunende activiteiten mogelijk te maken volgens 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 organisatiedoelstellingen en wettelijke voorschriften.

### **Waarom is dit nodig?**

Een informatiearchitectuur helpt je school om tijdig en goed te reageren op veranderingen en op (externe) dreigingen die een (mogelijke) aanpassing in de informatiehuishouding vragen. Denk aan de invoering van de AVG. Een EIAM laat je snel zien waar in je school welke gegevens verwerkt worden en hoe deze met elkaar verbonden zijn. Met dit inzicht kun je gemakkelijker de juiste acties bepalen en een veilige digitale omgeving creëren voor leerlingen, ouders en medewerkers.

## **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen EIAM gedefinieerd.

## **2 - Herhaalbaar**

2 – Herhaalbaar

- a) De baseline architectuur (IST) is gedefinieerd.
- b) Er zijn EIAM-specifieke processen opgezet om de ontwikkeling van systemen en/of toepassingen mogelijk te maken.

## **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er is een baseline voor de huidige (IST) en de beoogde architectuur (SOLL) gedefinieerd.
- b) De SOLL is in overeenstemming met de organisatiebrede doelstellingen (inclusief de naleving van wettelijke voorschriften) en de organisatorische verantwoordelijkheden.
- c) 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.
- d) Het EIAM is goedgekeurd door het schoolbestuur.

## **4 - Beheerst**

4 – Beheerst

- a) Het model ondersteunt op een veilige manier het creëren, gebruiken en delen van informatie, in lijn met de organisatiedoelstellingen, met inbegrip van innovaties.
- b) De SOLL is gericht op de prioriteiten en performancedoelstellingen van de organisatie.
- c) Het EIAM en de relevante processen worden periodiek geëvalueerd.

## **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Het EIAM vergemakkelijkt het effectief creëren, gebruiken en delen van informatie op een wijze die de integriteit verbetert (of ten minste handhaaft) en die flexibel, functioneel, kosteneffectief en tijdig is.

## **Aan de slag**

1. Zorg dat iemand binnen de organisatie informatiemanagement en daarmee informatiearchitectuur in het functiepakket heeft zitten. Voor kleinere schoolbesturen is dit vaak een rol en geen volledige functie. Gebruik voor het aanstellen van deze functionaris de Functiebeschrijving Informatiemanagement.
2. Stel als schoolbestuur de FORA vast als referentiearchitectuur.
3. Stel op basis van de FORA een organisatiespecifieke informatiearchitectuur op. Stel ook deze vast als schoolbestuur.
4. Zijn er wijzigingen in het informatielandschap? Dan wordt de informatiearchitectuur gebruikt om te toetsen wat de gewenste oplossingsrichting is.

## **Referentie naar andere normen en kaders**

ISO A8.27

## **Link naar relevante P normen**

### **GO.05 Onafhankelijke toetsing**

#### **Norm**

Onafhankelijke toetsing (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 is dit nodig?**

Met een onafhankelijke toetsing krijg je in beeld waar de dagelijkse praktijk op je school afwijkt van het beleid en de procedures. Deze toetsing kan via een interne of externe audit gebeuren. Door een audit uit te voeren, kunnen processen/maatregelen die niet goed lopen, worden geïdentificeerd en kan actie worden ondernomen om de risico's die hierdoor ontstaan te mitigeren.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er vindt geen onafhankelijke toetsing plaats.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) De interne auditfunctie is gedefinieerd en bestaat onder andere uit toetsing op naleving van relevante wet- en regelgeving, it- of informatiebeleid, standaarden en procedures binnen de organisatie.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Onafhankelijke toetsing (intern of extern) wordt ingezet om in beeld te krijgen of de informatievoorziening (inclusief it) voldoet aan relevante wet- en regelgeving, beleid, standaarden, procedures binnen de organisatie en algemeen aanvaarde werkwijzen.
- b) De activiteiten voor het verkrijgen van toetsing zijn beschreven in een auditplan dat is vastgesteld door het schoolbestuur of de schoolleiding en een auditcommissie.
- c) De resultaten van deze activiteiten worden gerapporteerd aan het schoolbestuur of de schoolleiding en de auditcommissie.
- d) Er zijn ingevulde checklists beschikbaar die worden gebruikt bij de controle.

#### **4 - Beheerst**

4 – Beheerst

- a) De uitvoering van de onafhankelijke toetsing wordt periodiek geëvalueerd door de auditcommissie.
- b) Het ontwerp van de onafhankelijke toetsingsfunctie wordt periodiek geëvalueerd door een externe partij.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Onafhankelijke toetsing (intern of extern) omvat ook de effectiviteit en de efficiëntie van de informatieverwerking (inclusief it).

#### **Aan de slag**

1. Stel als schoolbestuur een auditplan vast. Hierin is beschreven 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 wordt.

2. Bespreek de auditresultaten en formuleer een actieplan. Zorg ervoor dat aan de hand van dit actieplan alle bevindingen worden opgelost.

### **Referentie naar andere normen en kaders**

ISO A5.1, A5.35, A5.36

### **Link naar relevante P normen**

## **2. Organisatie**

Effectieve besluitvorming en functiescheiding zijn essentieel voor het bereiken van een digitaal veilige schoolomgeving. Ze dragen bij aan een heldere en concrete uitvoering van alle IBP-maatregelen en beschermen de school op deze manier tegen aanvallen op systemen en processen. De medewerkers in functies op het hoogste niveau dragen een belangrijke verantwoordelijkheid. Zij zijn degenen die afwegingen moeten maken voor informatiebeveiliging, zoals risicobereidheid en kostenbatenanalyses.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Adviseur informatiebeveiliging, IBP-verantwoordelijke

Geraadpleegd: Management, hoofd Bedrijfsvoering, FG, it-verantwoordelijke

Geïnformeerd: Medewerkers van de school (waar relevant)

## **OR.01 Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid**

### **Norm**

Informatiebeveiliging en risicomanagement dragen bij aan het behalen van de organisatiedoelstellingen. Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zijn formeel toegewezen en ingebed in de organisatie.

### **Waarom is dit nodig?**

Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zorgen voor een effectieve besluitvorming en een betrouwbaar management van informatiebeveiliging. Iedereen weet wat er van hem of haar wordt verwacht en wat ieders taak is bij het creëren en in stand houden van een veilige omgeving. Ook kan het schoolbestuur op deze manier belangen goed afwegen bij keuzes over informatiebeveiliging.

### **1 - Ad hoc**

1 – Ad hoc

- a) Eigenaarschap, rollen en verantwoordelijkheden zijn niet toegewezen.
- b) Er zijn enkele rollen te onderscheiden die informeel worden uitgevoerd.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Rollen die cruciaal zijn voor het managen van informatierisico's zijn benoemd en toegewezen, inclusief specifieke verantwoordelijkheid en aansprakelijkheid voor informatiebeveiliging, fysieke veiligheid en het voldoen aan wet- en regelgeving.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a) Alle rollen op het gebied van het managen van informatierisico's zijn vastgesteld en toegewezen.
- b) Op organisatieniveau zijn de verantwoordelijkheid en aansprakelijkheid voor risico- en informatiebeveiligingsmanagement vastgesteld. Hierin worden organisatiebrede kwesties behandeld. Er is een intentieverklaring van het schoolbestuur die stelt dat de schoolleiding de doelen en uitgangspunten van informatiebeveiliging en informatierisicobeheer ondersteunt en dat ze overeenstemming zijn met de strategie en organisatiedoelstellingen.
- c) De governancestructuur is gedocumenteerd met daarin opgenomen de verantwoordelijkheden en rapportagestructuur.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Eigenaarschap, verantwoordelijkheid en aansprakelijkheid voor it-gerelateerde risico's zijn in de organisatie ingebed in het juiste managementniveau.
- b) Bijkomende verantwoordelijkheden voor informatiebeveiligingsmanagement kunnen op een systeemspecifiek niveau worden toegewezen.
- c) Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid worden periodiek geëvalueerd.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a) Het schoolbestuur of de schoolleiding bepaalt formeel de risicobereidheid voor informatierisico's en de acceptatie van restrisico's.

### **Aan de slag**

1. Neem rollen, verantwoordelijkheden, eigenaarschap en een governancestructuur voor informatiebeveiliging op in het IBP-beleid.
2. Maak een intentieverklaring voor in het IBP-beleid. Beschrijf hierin hoe het IBP-beleid bijdraagt aan de organisatiedoelen en op welke manier het in lijn is met de strategie. Het template IBP-beleid bevat een voorbeeld van een intentieverklaring.

### **Referentie naar andere normen en kaders**

ISO 5.3, A5.2, A5.4

### **Link naar relevante P normen**

BL.02

## **OR.02 Functiescheiding**

### **Norm**

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

### **Waarom is dit nodig?**

Functiescheiding is van belang om te voorkomen dat iemand schadelijke acties kan uitvoeren, bijvoorbeeld door nalatig gebruik of opzettelijk misbruik van het systeem. Denk hierbij aan ongeautoriseerde toegang tot gegevens of het al dan niet per ongeluk wijzigen van gegevens.



## **1 - Ad hoc**

1 – Ad hoc

- a) Er vindt geen of nagenoeg geen functiescheiding plaats.

## **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Rollen en verantwoordelijkheden zijn gescheiden.
- b) Hoe deze rollen en verantwoordelijkheden worden gescheiden is niet formeel vastgelegd en/of afgestemd met het schoolbestuur of de schoolleiding.

## **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) De scheiding van rollen en verantwoordelijkheden is gedefinieerd en grotendeels ingevoerd. Dit verkleint de kans dat individuele medewerkers essentiële processen kunnen schaden.
- b) De scheiding van verantwoordelijkheden is vastgesteld door het schoolbestuur of de schoolleiding.
- c) Vastgestelde functiescheiding is ingevoerd, zodat medewerkers alleen geautoriseerde handelingen kunnen verrichten die passen bij hun werkzaamheden.

## **4 - Beheerst**

4 – Beheerst

- a) Een functiescheidingconflictmatrix is gedefinieerd en wordt periodiek getoetst aan de werkelijke implementatie van systemen en processen.
- b) Deze functiescheidingconflictmatrix wordt in ieder geval geëvalueerd na grote wijzigingen in processen of systemen.
- c) De implementatie en uitvoering van relevante procedures worden periodiek geëvalueerd.

## **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Periodiek worden er databasechecks uitgevoerd om de huidige processen te toetsen in relatie tot de functiescheidingsmatrix. Hierbij wordt gekeken naar ongebruikelijk transacties en gebieden voor verbetering (bijvoorbeeld met processminingtechnieken).

## **Aan de slag**

1. Maak een matrix van wel en niet toegestane combinaties van taken. Deze matrix moet een overzicht bevatten van wel en niet toegestane combinaties van autorisaties binnen een informatiesysteem, die aan één medewerker mogen worden toegekend.
2. Ga bij het maken van de matrix uit van het principe dat beschikkende, bewarende en controlerende taken nooit in één functionaris worden samengebracht. Is dit toch noodzakelijk? Organiseer dan dat de systeemeigenaar apart toezicht houdt op de betreffende functionaris.
3. (Technische) beheerders mogen geen toegang hebben tot de data van het informatiesysteem waarvan zij (technisch) beheerder zijn. Is dit toch noodzakelijk? Organiseer dan ook in dit geval dat de systeemeigenaar apart toezicht houdt op de betreffende functionaris.

## **Referentie naar andere normen en kaders**

ISO A5.3, A5.4

**Link naar relevante P normen**

### **3. Risicomanagement**

Risicomanagement gaat over het gestructureerd identificeren en beheersen van risico's op het gebied van informatiebeveiliging. Het gaat hierbij niet zo zeer om het wegnemen van alle risico's, maar om het identificeren van deze risico's en het formuleren van een juiste aanpak om ermee om te gaan. Tref je maatregelen en stuur je op de uitvoering van deze maatregelen? Of besluit je juist dat het een acceptabel (rest)risico is, omdat bijvoorbeeld de kosten van de maatregelen niet opwegen tegen de baten?

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Management, IBP-verantwoordelijke, adviseur informatiebeveiliging

Geraadpleegd: FG, it-verantwoordelijke

Geïnformeerd: Medewerkers van de school (waar relevant)

#### **RM.01 Raamwerk voor informatierisicomanagement**

##### **Norm**

1. Zorg ervoor dat risicomanagement onderdeel uitmaakt van het informatiebeveiligingsbeleid. Zie hiervoor ook norm GO.02 Beleid informatiebeveiliging.
2. Volg de handreiking Risicomanagement voor de verdere invulling van risicomanagement binnen de kaders van het informatiebeveiligingsbeleid. Hierin staat beschreven welke zaken procesmatig aandacht behoren te krijgen en op welke wijze hier invulling aan wordt gegeven.  
Stel een Risicomanagement proces op voor de verdere invulling van risicomanagement binnen de kaders van het informatiebeveiligingsbeleid
3. Draag als IBP-verantwoordelijke bij aan het kennisniveau over risicomanagement van medewerkers en leidinggevendenden, bijvoorbeeld door het geven van voorlichting of training.

##### **Waarom is dit nodig?**

Het raamwerk als basis voor het risicomanagementproces voor informatierisicomanagement helpt je om analyses goed uit te voeren, risico's te interpreteren en beheersmaatregelen op te stellen. Een gedegen risicomanagementproces zorgt ervoor dat risico's geen onverwachte verstoring veroorzaken. Door de verantwoordelijkheden voor de verschillende stappen in het proces helder vast te leggen en de aanpak scherp te hebben, krijgt de organisatie grip op eventuele verstoringen.

##### **1 - Ad hoc**

1 – Ad hoc

- a) Informatierisico's zijn niet of worden ad hoc bepaald.
- b) Er is geen raamwerk voor informatierisicomanagement en geen informatierisicomanagementproces.

##### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) (Informatie)risicomanagementbeleid en een informatierisicomanagementproces zijn opgesteld; meestal op een hoog abstractieniveau en worden alleen toegepast bij grote projecten of als reactie op problemen.
- b) Er is een beknopt raamwerk voor informatierisicomanagement en de risicobereidheid is op een hoog niveau bepaald. Raamwerk en risicobereidheid zijn in beperkte mate in lijn met de organisatiedoelstellingen en bedrijfsrisico's.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a) Er is organisatiebreed (informatie)risicomanagementbeleid dat is vastgesteld door het schoolbestuur of de schoolleiding.
- b) Het beleid en de procesbeschrijving geven aan hoe om te gaan met de essentiële elementen van risicomanagement (risicobereidheid/risicoprofiel, eigenaarschap, risicoproces, bepalen, mitigeren en accepteren).
- c) Het kader voor informatierisico's is in lijn met het kader voor organisatiebreed risicomanagement en omvat componenten als strategie, programma's, projecten en uitvoering.
- d) 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.
- e) Training in het kader van dit risicokader is ingevoerd.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Het raamwerk voor informatierisicomanagement en hoe de daaraan verbonden processen in de praktijk functioneren, worden periodiek geëvalueerd.
- b) Periodiek wordt gerapporteerd over (het raamwerk voor) informatierisicomanagement, waardoor het schoolbestuur risico's kan monitoren en op basis daarvan overwogen besluiten kan nemen over welke risico's het accepteert.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a) Het raamwerk voor informatierisicomanagement focust ook op efficiëntieaspecten van primaire bedrijfsvoering.
- b) Informatierisicomanagement is volledig geïntegreerd in alle it- en bedrijfsvoering, wordt volledig geaccepteerd en betreft hierin medewerkers en leveranciers.
- c) Het raamwerk voor informatierisicomanagement en de daaraan verbonden processen worden voortdurend verbeterd.

### **Aan de slag**

1. Zorg ervoor dat risicomanagement onderdeel uitmaakt van het informatiebeveiligingsbeleid. Zie hiervoor ook norm GO.02 Beleid informatiebeveiliging.
2. Stel een Risicomanagement proces op voor de verdere invulling van risicomanagement binnen de kaders van het informatiebeveiligingsbeleid
3. Draag als IBP-verantwoordelijke bij aan het kennisniveau over risicomanagement van medewerkers en leidinggevenden, bijvoorbeeld door het geven van voorlichting of training.

### **Referentie naar andere normen en kaders**

ISO 4.4, 6.1.1, 6.1.2

Certificeringsschema ROSA:

Vertrouwelijkheid/Omggaan met kwetsbaarheden

### **Link naar relevante P normen**

BL.03

## **RM.02 Risicobeoordeling**

### **Norm**

Risicobeoordelingen worden uitgevoerd om actuele risico's die betrekking hebben op de doelstellingen van het schoolbestuur of de school te bepalen. De waarschijnlijkheid en impact van alle geïdentificeerde risico's worden regelmatig beoordeeld, met behulp van kwalitatieve en kwantitatieve methoden.

### **Waarom is dit nodig?**

Risicobeoordelingen ondersteunen de school om tijdig en juist actieplannen op te stellen en beheersmaatregelen in te voeren. Met een risicobeoordeling breng je de risico's voor de school in kaart en kijk je in hoeverre deze risico's impact hebben op de doelstellingen van de school. Alleen als de doelstellingen in het geding zijn, spreken we van een risico. Risico's worden beoordeeld op hun potentiële impact op die doelstellingen.

### **1 - Ad hoc**

#### 1 – Ad hoc

- a) Risicoanalyses worden zelden gedaan en zijn afhankelijk van individuen.
- b) Soms worden risicoanalyses uitgevoerd als onderdeel van een projectplan.

### **2 - Herhaalbaar**

#### 2 – Herhaalbaar

- a) Risicoanalyses worden uitgevoerd als onderdeel van het risicomanagementproces en risico's worden kwalitatief of kwantitatief geïdentificeerd.
- b) De kans en/of impact wordt vooral bepaald op basis van algemene criteria, niet volledig in lijn met de organisatiedoelen.
- c) Risicoanalyses worden (als onderdeel van een project) beknopt gedocumenteerd.

### **3 - Bepaald (streefniveau)**

#### 3 – Bepaald

- a) Dankzij duidelijke en passende instructies vinden risicoanalyses consistent en herhaaldelijk plaats, als onderdeel van het risicomanagementproces.
- b) De risicoanalysemethode is in lijn met behoeften van de organisatie en identificeert belangrijke risico's (inclusief kroonjuwelen).
- c) De geïdentificeerde risico's worden kwalitatief en kwantitatief beoordeeld, gebruikmakend van het risicomanagementproces of good practice-bronnen.
- d) Afwijkingen ten opzichte van het risicoprofiel worden gerapporteerd aan het schoolbestuur.

### **4 - Beheerst**

#### 4 – Beheerst

- a) De correlatie tussen de geïdentificeerde risico's wordt geanalyseerd en gedocumenteerd. Zo kunnen de resultaten van de risico of dreigingsanalyse worden opgenomen in de overkoepelende risk heat map.
- b) De risicoanalysemethodiek wordt periodiek geëvalueerd.

### **5 - Continu verbeteren**

#### 5 – Continu verbeteren

- a) De risicoanalysemethodiek wordt ondersteund door geautomatiseerde tools, workflowprocessing en geïntegreerde dashboards.

## **Aan de slag**

1. Stel een standaard risicoanalyseproces vast waarin het gebruik van een risicoanalyse template is opgenomen.
2. Bespreek de belangrijkste risico's periodiek met het schoolbestuur of de schoolleiding.

## **Referentie naar andere normen en kaders**

ISO 4.4, 6.1.2, 6.1.3

## **Link naar relevante P normen**

BL.03

## **RM.03 Plan voor behandeling en beperking van risico's**

### **Norm**

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 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 schoolbestuur of de schoolleiding.

### **Waarom is dit nodig?**

Met beheersactiviteiten verklein je de kans en impact van risico's. Als je risico's prioriteert en maatregelen doorvoert die risico's beperken, verminder je hoge kosten en andere negatieve gevolgen.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen plan voor het aanpakken of mitigeren van risico's.
- b) Als een risico wordt geïdentificeerd, worden de risicobeperkende maatregelen inconsistent toegepast, afhankelijk van individuele competenties.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Plannen voor het aanpakken en mitigeren van risico's zijn gemaakt, maar niet formeel vastgelegd.
- b) Risicobeperkende maatregelen zijn onvolledig en niet geformaliseerd/goedgekeurd, en eigenaarschap is slechts gedeeltelijk toegewezen aan risicomaatregelen of geaccepteerde risico's.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

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

#### **4 - Beheerst**

##### **4 – Beheerst**

- a) Indien van toepassing wordt de prioritering van risicobeperkende maatregelen en argumenten voor risicoacceptatie heroverwogen.
- b) Geïdentificeerde risicoreacties geven ook inzicht in de kosten en baten daarvan, inclusief bewaking van het budget.
- c) De operationele effectiviteit van het risicomanagementproces wordt regelmatig geëvalueerd.

#### **5 - Continu verbeteren**

##### **5 – Continu verbeteren**

- a) Het documenteren, analyseren, bewaken en rapporteren van risicomanagementdata gebeurt (grotendeels) geautomatiseerd.
- b) Strategieën voor het mitigeren van risico's worden voortdurend door het schoolbestuur of de schoolleiding geëvalueerd.

#### **Aan de slag**

1. Leg de geconstateerde risico's uit de risicoanalyses vast in een register en benoem hierbij de risico-eigenaar.
2. Beschrijf per risico welke maatregelen worden genomen en wat het restrisico is. Het schoolbestuur of de schoolleiding geeft goedkeuring voor het al dan niet nemen van de maatregelen. Koppel aan elke maatregel een actiehouders die verantwoordelijk is voor de implementatie ervan.
3. Monitor het doorvoeren van de maatregelen en stuur waar nodig bij.

#### **Referentie naar andere normen en kaders**

ISO 6.1.3

#### **Link naar relevante P normen**

BL.03

## **4. Personeelsbeheer**

Personeelsbeheer bevat de normen die direct betrekking hebben op alle medewerkers van de school. Dit beslaat de hele cyclus van personeelsbeheer: van werving, doorstroming en uit dienst gaan tot het delen en op peil houden van de kennis en bewustwording van het belang van informatiebeveiliging. Door de kennis te borgen en over te dragen zorgt de organisatie ervoor dat de continuïteit van het onderwijs niet in gevaar komt als medewerkers op een cruciale plek uit dienst gaan.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Hoofd HR, IBP-verantwoordelijke, it-verantwoordelijke

Geraadpleegd: Adviseur informatiebeveiliging, management

Geïnformeerd: Medewerkers van de school (waar relevant)

### **HR.01 Werving van medewerkers**

#### **Norm**

Wervingsprocessen voor medewerkers worden onderhouden in overeenstemming met het algemene personeelsbeleid en de procedures van de organisatie (bijvoorbeeld werving, positieve werkomgeving, oriëntatie, enzovoorts).

Processen worden ingevoerd om ervoor te zorgen dat de organisatie beschikt over geschikte (it-)medewerkers, met de vaardigheden die nodig zijn om de organisatiedoelen te bereiken. Screening maakt deel uit van het wervingsproces. De mate en frequentie waarmee deze screening wordt uitgevoerd, worden bepaald door hoe gevoelig en/of cruciaal de functie is. Screening wordt ingevoerd voor medewerkers, ingehuurde medewerkers en leveranciers.

### **Waarom is dit nodig?**

Heb je de werving en selectie van nieuwe medewerkers goed ingericht? Dan is de kans groter dat jouw school voldoende it-medewerkers kan aantrekken die juist gekwalificeerd en gescreend zijn.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Activiteiten of maatregelen voor het werven van (it-)medewerkers zijn ad hoc ingevoerd en/of uitgevoerd.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Wervingsprocessen voor (it-)medewerkers zijn gedefinieerd en ingevoerd.
- b) Er zijn processen ingevoerd om te garanderen dat (it-)medewerkers van de organisatie goed zijn toegerust.
- c) Af en toe wordt screening toegepast in het wervingsproces, maar dit is niet formeel vastgelegd.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Wervingsprocessen voor (it-)medewerkers zijn vastgelegd en ingevoerd volgens het algemene personeelsbeleid en procedures (bijv. aanname, positieve werkomgeving, oriëntatie).
- b) Er zijn processen ingevoerd om te garanderen dat (it-)medewerkers goed zijn toegerust om bedrijfsdoelen te behalen.
- c) Screening is onderdeel van het wervingsproces voor (it-)medewerkers. Hoe grondig en vaak deze screening wordt geëvalueerd is afhankelijk van de gevoeligheid en het belang van de functie. De screening vindt plaats voor medewerkers, ingehuurde medewerkers en leveranciers.
- d) De processen zijn goedgekeurd door het schoolbestuur of de schoolleiding.

#### **4 - Beheerst**

4 – Beheerst

- a) De implementatie en effectiviteit van relevante wervingsprocedures en functieomschrijvingen worden periodiek geëvalueerd.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Op basis van de periodieke (zelf)evaluaties of risicoanalyses worden de implementatie en het ontwerp van de wervingsprocessen verbeterd.
- b) Tekortkomingen in het wervingsproces worden gerapporteerd aan het schoolbestuur of de schoolleiding.

### **Aan de slag**

1. Zorg ervoor dat er bij het werven van (it-)medewerkers voldoende aandacht is voor de benodigde kwalificaties en controleer het cv daarop bij de selectie van een nieuwe medewerker.
2. Beoordeel voor welke functies een screening (VOG) nodig is en neem dit op in het wervingsproces.

## **Referentie naar andere normen en kaders**

ISO A6.1, A6.2, A6.6

## **Link naar relevante P normen**

## **HR.02 Certificering, training en scholing**

### **Norm**

Opleiding, training en/of ervaring worden regelmatig getoetst om te zien of medewerkers over de benodigde competenties beschikken 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 is dit nodig?**

Door (it-)medewerkers professioneel te trainen, verklein je risico's op incidenten en verstoring van de bedrijfsprocessen. Daarnaast helpt training bij het hanteren van operationele procedures en projectbeheer.

### **1 - Ad hoc**

1 – Ad hoc

- a) Training en educatie wordt ad hoc ingevoerd.
- b) Er is geen certificering van medewerkers.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Processen voor certificering, training en educatie worden ingevoerd.
- b) Er zijn individuele persoonlijke ontwikkelplannen beschikbaar.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Processen voor training en educatie zijn ingevoerd en worden uitgevoerd.
- b) Er zijn individuele persoonlijke ontwikkelplannen beschikbaar.
- c) Educatie, training en/of ervaring worden gebruikt om regelmatig te verifiëren of medewerkers over de benodigde vaardigheden beschikken.
- d) De relevante processen zijn goedgekeurd door het schoolbestuur of de schoolleiding.

### **4 - Beheerst**

4 – Beheerst

- a) De vereiste (it-)kernvaardigheden zijn gedefinieerd en waar gepast worden kwalificatie- en certificeringprogramma's gebruikt om te zorgen dat deze worden onderhouden.
- b) Er is toezicht op de realisatie van persoonlijke ontwikkelplannen.

### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) De implementatie van de processen voor certificering, training en educatie wordt jaarlijks geëvalueerd, waarbij educatie- en trainingsmaterialen worden gecheckt op relevantie, kwaliteit en effectiviteit.

### **Aan de slag**

1. Neem scholing over informatiebeveiliging en it op in het scholingsplan van de school.
2. Bekijk ten minste jaarlijks of er aanvullende scholing nodig is.



## **Referentie naar andere normen en kaders**

ISO 7.2, A6.3

## **Link naar relevante P normen**

### **HR.03 Afhankelijkheid van individuen**

#### **Norm**

Er is een back-upplan voor kritieke medewerkers (sleutelfiguren) en afdelingen.

#### **Waarom is dit nodig?**

Om de continuïteit van een functie te waarborgen is het belangrijk dat de taken van sleutelfiguren kunnen worden overgenomen door andere medewerkers. Ook is het belangrijk dat mogelijke problemen bij de bezetting van kritieke afdelingen vroegtijdig worden gesignaleerd.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Opvolgings- en back-upplannen zijn niet ingevoerd.
- b) Single points of failure met betrekking tot medewerkers zijn niet geïdentificeerd.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Back-up en vervanging van kritieke medewerkers/functies worden op afdelingsniveau geregeld.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Opvolgingsplanning, functierotatie en back-up van medewerkers zijn ingevoerd.
- b) Er zijn trainingsprogramma's om het risico van een te grote afhankelijkheid van sleutelfiguren te verkleinen.
- c) De meeste sleutelfuncties/-posities zijn geïdentificeerd en formeel gedefinieerd door het schoolbestuur of de schoolleiding.

#### **4 - Beheerst**

4 – Beheerst

- a) Alle kritieke personen en/of afdelingen zijn in de hele organisatie geïdentificeerd en/of worden periodiek geëvalueerd.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) De effectiviteit van het proces voor de planning van opvolging en back-up van medewerkers wordt periodiek geëvalueerd.
- b) De planning voor opvolging is in overeenstemming met de organisatie- en it-strategie.

#### **Aan de slag**

1. Stel vast welke functionarissen op het gebied van it en informatiebeveiliging op sleutelfuncties zitten.
2. Benoem maatregelen voor elke sleutelfunctie voor wanneer de medewerker van de een op de andere dag niet meer beschikbaar is. Je kunt hierbij denken aan een back-up binnen de eigen organisatie die de cruciale kennis heeft en direct ingezet kan worden. Je kunt ook binnen een regionale samenwerking afspreken dat in dergelijke gevallen op basis van loonkosten tijdelijk een functionaris gedeeld kan worden.

Of je kunt werken met een lijst van organisaties die per direct een inhuurmedewerker met de juiste expertise kunnen leveren.

## **Referentie naar andere normen en kaders**

### **Link naar relevante P normen**

## **HR.04 Verandering of beëindiging van functie**

### **Norm**

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 is dit nodig?**

Verlaten medewerkers met specialistische it-kennis de organisatie? Dan kunnen processen in gevaar komen door uitval van systemen of koppelingen. Door tijdig de toegangsrechten van de vertrekkende functionaris in te trekken, verminder je de risico's van ongeautoriseerde toegang.

### **1 - Ad hoc**

1 – Ad hoc

a) Wanneer er functiewijzigingen of ontslagen plaatsvinden worden er geen of ad-hoc-acties ondernomen.

### **2 - Herhaalbaar**

2 – Herhaalbaar

a) Toegangsrechten van medewerkers worden gewijzigd, opnieuw toegewezen en/of verwijderd op basis van functiewijziging en/of ontslag, maar het tijdig intrekken van toegangsrechten is niet gewaarborgd.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

a) Goedgekeurde processen zijn ingevoerd om kennis over te dragen en toegangsrechten opnieuw toe te wijzen of in te trekken.

b) Kennisoverdracht is geregeld, verantwoordelijkheden zijn opnieuw toegewezen en toegangsrechten worden tijdig ingetrokken. Hierdoor zijn risico's geminimaliseerd en is de continuïteit van de functie gewaarborgd.

c) De stappen van functieoverdracht zijn vastgelegd.

### **4 - Beheerst**

4 – Beheerst

a) Er worden ontslaggesprekken gevoerd en de juistheid en tijdigheid van veranderingen, opnieuw toewijzen of intrekken van toegangsrechten worden periodiek geëvalueerd.

### **5 - Continu verbeteren**

5 – Continu verbeteren

a) De effectiviteit van de processen voor functiewijzigingen en/of ontslag wordt periodiek geëvalueerd en verbeterd.

### **Aan de slag**

1. Wijzigt iemand van functie of wordt een dienstverband beëindigd? Zorg dan dat kennisoverdracht geregeld wordt, de verantwoordelijkheden opnieuw worden toegewezen en toegangsrechten ingetrokken

worden.

2. Zorg dat HR een checklist van de benodigde stappen heeft en bij de manager voor vertrek van de medewerker checkt of hieraan uitvoering is gegeven.

#### **Referentie naar andere normen en kaders**

ISO A5.11, A5.18, A6.4, A6.5

#### **Link naar relevante P normen**

### **HR.05 Kennisdeling**

#### **Norm**

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 ondersteunende medewerkers het systeem en de bijbehorende infrastructuur op effectieve en efficiënte wijze kunnen leveren, ondersteunen en onderhouden.

#### **Waarom is dit nodig?**

Met goede procedures en werkinstructies kun je makkelijker kennis delen en overdragen, waardoor anderen de werkzaamheden kunnen uitvoeren. Zo kunnen medewerkers doelmatig en efficiënt gebruikmaken van systemen voor het ondersteunen van bedrijfs- en onderwijsprocessen.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Overdracht van kennis is niet ingevoerd of wordt ad hoc gedaan.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er zijn informele, gedecentraliseerde processen voor kennisoverdracht ingevoerd.
- b) Kennis en vaardigheden worden vaak overgedragen op individuele basis.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

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

#### **4 - Beheerst**

4 – Beheerst

- a) Er wordt periodiek geëvalueerd of de ondersteunende documentatie toereikend is.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Kennis en vaardigheden worden overgedragen zodat eindgebruikers het systeem op efficiënte wijze kunnen gebruiken.
- b) Kennis en vaardigheden worden overgedragen zodat operationeel en technisch supportmedewerkers in het systeem en de infrastructuur efficiënt kunnen leveren, ondersteunen en onderhouden.

## **Aan de slag**

1. Zorg ervoor dat de it-afdeling voor de benodigde gebruikersondersteuning zorgt bij it-applicaties.
2. Hou beheerdocumentatie bij volgens de hiervoor opgestelde interne werkprocedures.

## **Referentie naar andere normen en kaders**

ISO A5.6, A5.37, A6.3

## **Link naar relevante P normen**

## **HR.06 Bewustwording informatiebeveiliging**

### **Norm**

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

### **Waarom is dit nodig?**

Als je medewerkers duidelijk instrueert over en bewust maakt van hun verantwoordelijkheden bij informatiebeveiliging, kunnen zij informatiebeveiligingsrisico's helpen beperken.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er zijn geen bewustwordingsactiviteiten gedefinieerd of uitgevoerd.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Bewustwordingsactiviteiten worden uitgevoerd op afdelingsniveau.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

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

### **4 - Beheerst**

4 – Beheerst

- a) Bewustwordingsactiviteiten bevatten een verplicht e-learningprogramma dat succesvol moet worden volbracht, inclusief online examen.
- b) Afronding van e-learningmodules door medewerkers wordt bewaakt en gerapporteerd aan het management.

### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) De effecten van de bewustwordingsactiviteiten worden gemonitord.
- b) Correlatie van beveiligingsincidenten als gevolg van gebrek aan bewustwording leidt tot aanpassing van de bewustwordingsactiviteiten.

## **Aan de slag**

1. Beschrijf jaarlijks in het informatiebeveiligingsplan welke bewustwordingsactiviteiten dat jaar worden uitgevoerd. Zie norm GO.03 Plan informatiebeveiliging voor meer informatie over dit plan.
2. Zorg ervoor dat gedurende het jaar alle medewerkers in aanraking komen met bewustwordingsactiviteiten en neem dit ook mee tijdens de inwerkperiode van nieuwe medewerkers.
3. Breng informatiebeveiligingsrisico's ook onder de aandacht van leerlingen wanneer ze gebruikmaken van digitale middelen.

## **Referentie naar andere normen en kaders**

ISO A5.4, A5.27, A6.3, A6.4, A6.6, A7.7, A8.1

## **Link naar relevante P normen**

OL.04

# **5. Configuratiemanagement**

Configuratiemanagement gaat over het bijhouden van alle informatie van en over de it-componenten binnen de organisatie. Je legt vast welke hardware er is (bijvoorbeeld computers of printers), welke software gebruikt wordt (inclusief versienummers), welke updates er zijn uitgevoerd en welke instellingen er gebruikt worden bij elke component. Ook de onderlinge relaties tussen de componenten en systeemeigenaarschap worden vastgelegd. Configuratiemanagement geeft zo overzicht over alles wat er op het gebied van it binnen de organisatie gebruikt wordt.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: it-verantwoordelijke, it-leverancier

Geraadpleegd: Management, hoofd Bedrijfsvoering,

Geïnformeerd: Medewerkers van de school (waar relevant)

## **CO.01 Identificatie en onderhoud van configuratie-items**

### **Norm**

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

### **Waarom is dit nodig?**

Als er verstoringen ontstaan, is het essentieel dat je inzicht hebt in de wijzigingen van de configuratie van systemen en diensten. Onder meer omdat je dan kunt nagaan of die verstoringen samenhangen met de wijzigingen. Deze configuraties zijn vastgelegd in de configuratiedatabase. Wijzigingen in configuraties moet je ook vastleggen in de configuratiedatabase. Zo kan de database je helpen om de oorzaak van de verstoringen te vinden en krijg je inzicht in het effect van een wijziging op andere processen.

### **1 - Ad hoc**

1 – Ad hoc

a) Er is geen configuratieprocedure.

b) Werkwijzen en procedures worden uitsluitend individueel toegepast en verschillen per platform.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er is een configuratieprocedure vastgesteld om configuratie-items te identificeren en te onderhouden, maar deze procedure is niet geformaliseerd.
- b) De data-inhoud van geregistreerde items wordt niet gebruikt door gerelateerde processen, zoals change-, incident- en problemmanagement.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

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

## **4 - Beheerst**

### **4 – Beheerst**

- a) Er is een proces voor het periodiek evalueren van relevante documentatie, tijdige uitvoering en integriteit van de configuratiedatabase (inclusief licenties).
- b) De implementatie en uitvoering van relevante procedures voor het configuratiemanagement worden periodiek geëvalueerd.
- c) Er wordt regelmatig aan het management gerapporteerd, wat leidt tot verbeterplannen.
- d) Procedures en standaarden zijn onderdeel van training.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Er wordt voortdurend geanalyseerd of er afwijkingen zijn. Gevonden afwijkingen worden onderzocht.
- b) Gebreken en trends worden gerapporteerd aan het management.
- c) Gerelateerde processen zijn volledig geïntegreerd, en configuratiedata wordt geautomatiseerd gebruikt en actueel gehouden.

## **Aan de slag**

1. Stel een procedure configuratiemanagement op en stel deze vast. De procedure bevat elementen zoals het labelen van bedrijfsmiddelen en centraal registreren van de aanschaf van soft- en hardware.

## **Referentie naar andere normen en kaders**

ISO A5.9, A8.9, A8.19, A8.32

## **Link naar relevante P normen**

## **CO.02 Configuratiedatabase en baseline**

### **Norm**

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 ingevoerd.

## **Waarom is dit nodig?**

Monitoring van de middelen en wijzigingen draagt bij aan het betrouwbaar houden van de systemen van de organisatie. Met configuratiebaselines leg je voor elk systeem en elke dienst een basisconfiguratie vast. Na een wijziging kun je dan altijd teruggaan naar die baseline, als dat nodig is.

### **1 - Ad hoc**

#### **1 – Ad hoc**

- a) Basistaken op het gebied van configuratiemanagement, zoals het identificeren en bijhouden van een inventaris van configuratie-items, worden op ad-hoc basis uitgevoerd.
- b) De documentatie van de configuratie is onvolledig en onbetrouwbaar.

### **2 - Herhaalbaar**

#### **2 – Herhaalbaar**

- a) Configuratiemanagementtools worden soms gebruikt, maar er is geen standaard.
- b) Geïnstalleerde software, configuraties en documentatie worden geregistreerd, maar de gegevensinhoud van opgenomen items is beperkt.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

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

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Er worden geautomatiseerde tools voor het bijhouden van veranderingen in apparatuur en software gebruikt om de standaarden te handhaven en de stabiliteit te verbeteren.
- b) Er zijn mechanismen om wijzigingen te toetsen aan wat is vastgelegd in de centrale opslagplaats en aan de gedefinieerde baseline.
- c) Periodiek worden fysieke controles uitgevoerd.
- d) Wijzigingen die in de configuratiedatabase worden geregistreerd, worden periodiek geanalyseerd.
- e) Er wordt periodiek aan het management gerapporteerd.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a) Alle it-middelen worden in een centrale CMDB beheerd. Dit systeem bevat alle benodigde informatie over componenten en hun onderlinge relaties, alsmede informatie over reparatie, service, garantie, upgrades en technische assessments.
- b) Processen en automatisering voor software- en hardware-assetmanagement (inclusief licenties) zijn ingevoerd.
- c) Het management ontvangt periodiek (geautomatiseerde) rapporten.

## **Aan de slag**

1. Richt een CMDB in met daarin alle hardware, software, onderlinge relaties, versienummers, licenties en configuratiebaselines.

2. Hou de CMDB up-to-date. Dat betekent dat bij processen die leiden tot een wijziging in de CMDB, ook een stap is opgenomen voor het bijwerken van de CMDB.

### **Referentie naar andere normen en kaders**

ISO A5.9, A8.9

Certificeringsschema ROSA:

Integriteit van de toepassing/Herleidbaarheid

Integriteit van de toepassing/Controle integriteit

### **Link naar relevante P normen**

## **6. Incident- en problemmanagement**

Incident- en problemmanagement zijn zogeheten it-beheerprocessen. Bij incidentmanagement gaat het erom zo snel mogelijk verstoringen van de continuïteit te verhelpen en om veiligheidsincidenten sneller op te merken en verhelpen. Komt een incident veelvuldig voor? Dan gaat het over naar problemmanagement. Daar wordt de onderliggende oorzaak geanalyseerd met als doel de kwestie structureel te verhelpen.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: it-verantwoordelijke, adviseur informatiebeveiliging, it-leverancier, Privacy Officer (afhandeling datalekken)

Geraadpleegd: FG

Geïnformeerd: Management, medewerkers van de school

### **IM.01 Incidentmanagement**

#### **Norm**

Een formeel incidentmanagementproces wordt gecommuniceerd en ingevoerd. Er zijn procedures 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 is dit nodig?**

Incidentmanagement is het centrale proces voor het melden van incidenten in de it-omgeving en van (cyber)beveiligingsincidenten. Incidenten in de it-omgeving zijn nooit helemaal uit te sluiten. Daarom is het belangrijk dat je bent voorbereid als het toch mis gaat. Met een goede voorbereiding kun je de schade bij een incident beperken. Het doel van incidentmanagement is om verstoringen bij het verwerken van informatie snel en effectief te herkennen, vast te leggen en af te handelen. Incidenten zijn onverwachte gebeurtenissen of problemen die de normale werking van de it-omgeving verstoren. Ook als er iets misgaat met het veilig verwerken van informatie, wordt dat als een incident behandeld. Incidenten moet je oplossen zodat het onderwijs en ondersteunende werkprocessen door kunnen gaan.

#### **1 - Ad hoc**

1 – Ad hoc

a) Er is geen beleid voor incidentmanagement.

b) Er zijn geen rollen en verantwoordelijkheden vastgelegd.

c) Er zijn geen procedures om te garanderen dat alle incidenten en storingen worden gedocumenteerd en geanalyseerd.



- d) Incidenten worden bijgehouden en geëvalueerd op individuele basis.
- e) Reacties op informatiebeveiligingsincidenten zijn ad hoc.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er is een informeel incidentmanagementproces vastgesteld om kritische incidenten aan te pakken.
- b) Rollen en verantwoordelijkheden zijn gedeeltelijk gedefinieerd.
- c) De meeste incidenten worden gedocumenteerd en geanalyseerd, maar afwijkingen van de standaarden worden waarschijnlijk niet gedetecteerd.
- d) Er zijn geen criteria bepaald voor het categoriseren en prioriteren van incidenten op basis van impact.
- e) Incidenten worden ad hoc toegewezen. Er wordt handmatig en op individuele basis toezicht gehouden.
- f) Er is geen formele training en communicatie over de standaardprocedures.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

- a) Het incidentmanagementbeleid is formeel gedocumenteerd en gecommuniceerd.
- b) Rollen en verantwoordelijkheden van de organisatie en de leveranciers zijn duidelijk gedefinieerd.
- c) Aspecten rondom juridisch en forensisch onderzoek zijn vastgesteld en toegewezen.
- d) Het registreren van, de communicatie over, de toewijzing van en de analyse van incidenten zijn formeel belegd in de organisatie.
- e) Incidenten worden gecategoriseerd en geprioriteerd op basis van impact.
- f) (Cyber)beveiligingsincidenten worden voorkomen of gedetecteerd en er is een proces om deze tijdig en effectief aan te pakken.
- g) Informatie wordt op proactief en formeel gedeeld door medewerkers.
- h) Er wordt gemonitord of incidenten tijdig worden opgelost.
- i) Er wordt beperkt gerapporteerd aan het management over incident- en oplossingsanalyses.

## **4 - Beheerst**

### **4 – Beheerst**

- a) Incidenten worden proactief geanalyseerd om oorzaken te achterhalen.
- b) Er is een functie (responsteam) ingevoerd om beveiligingscrises te herkennen en te managen.
- c) Het incidentmanagementproces betreft belangrijke functies binnen de organisatie en bij externe serviceproviders.
- d) Op het tijdig aanpakken van incidenten wordt streng toegezien. Onopgeloste incidenten (bekende foutmeldingen waar omheen gewerkt wordt) worden gedocumenteerd en gerapporteerd als input voor problemmanagement.
- e) De kwaliteit en operationele effectiviteit van het incidentmanagementproces worden periodiek geëvalueerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) De registratie, rapportage en analyse van incidenten en oplossingen zijn volledig geautomatiseerd en geïntegreerd met configuratie- en problemmanagement.
- b) De meeste systemen zijn uitgerust met automatische detectie- en waarschuwingssystemen, die voortdurend gemonitord en beoordeeld worden.
- c) Incidentmanagement wordt voortdurend geanalyseerd voor verbetering.

## **Aan de slag**

1. Maak een incidentmanagementbeleid. Je kunt hiervoor gebruikmaken van elementen uit de handreiking Incidentmanagement en bijbehorende templates, zoals het template Incidentmanagementbeleid, waarin de processtappen zijn benoemd, de rollen en verantwoordelijkheden en de communicatielijnen.

2. Stel het incidentmanagementbeleid vast.
3. Stel het incidentmanagementbeleid (digitaal) beschikbaar voor alle medewerkers van de school, bijvoorbeeld via intranet.
4. Registreer incidenten in een register van beveiligingsincidenten en datalekken. Je kunt hiervoor gebruikmaken van het Register van (Beveiligings)incidenten en datalekken.
5. Rapporteer periodiek - bijvoorbeeld elk kwartaal - aan het schoolbestuur over de belangrijkste incidenten en de manier waarop deze zijn opgelost.

#### **Referentie naar andere normen en kaders**

ISO A5.24, A5.25, A5.26, A5.27, A5.28, A6.8

#### **Link naar relevante P normen**

GB.01, GB.02

### **IM.02 Incidentescalatie**

#### **Norm**

Er worden procedures voor incidentmanagement (of voor de servicedesk) vastgesteld die ervoor zorgen dat serviceniveaus adequaat worden geëscaleerd als incidenten niet binnen de afgesproken termijn kunnen worden opgelost. En dat zo nodig wordt voorzien in een tijdelijke oplossing. Eigenaarschap van incidenten en levenscyclusmonitoring blijven de verantwoordelijkheid van de servicedesk voor gebruikersincidenten, ongeacht wie aan de oplossing werkt.

#### **Waarom is dit nodig?**

De procedures voor incidentmanagement zorgen voor sturing op het proces en duidelijkheid over verantwoordelijkheden. Als iedereen weet wat er wordt verwacht, en wanneer geschakeld moet worden naar een hoger niveau, worden incidenten sneller en beter opgelost.

#### **1 - Ad hoc**

##### **1 – Ad hoc**

- a) Er is geen beleid om incidenten die niet opgelost kunnen worden tijdig te laten escaleren.
- b) Incidenten worden bijgehouden en geëvalueerd op individuele basis.
- c) Reacties op verstoringen van informatiebeveiliging zijn onvoorspelbaar.
- d) Er is niet vastgelegd wie verantwoordelijk is voor het oplossen van incidenten.

#### **2 - Herhaalbaar**

##### **2 – Herhaalbaar**

- a) Er is een informeel escalatieproces.
- b) Incidenten die niet tijdig kunnen worden opgelost worden geëscaleerd.
- c) Er zijn geen criteria bepaald voor het prioriteren van incidenten.
- d) Er is geen gecentraliseerde kennisbank.
- e) Responseteams zijn ongetraind en afhankelijk van enkele belangrijke individuen.

#### **3 - Bepaald (streefniveau)**

##### **3 – Bepaald**

- a) Het formeel vastgelegde beleid voor incidentmanagement bevat een escalatieprocedure.
- b) Er zijn escalatiecriteria bepaald.

- c) De escalatieprocedure is gebaseerd op serviceniveaus voor incidenten die niet meteen opgelost kunnen worden.
- d) Categoriseren en prioriteren gebeurt op basis van impactanalyse, de bepaalde criteria en serviceniveaus.
- e) De responsteams krijgen de benodigde training.
- f) De verantwoordelijkheid voor het oplossen van een incident is toegewezen.

#### **4 - Beheerst**

##### 4 – Beheerst

- a) Advies is consistent en incidenten worden tijdig en volgens een gestructureerde escalatieprocedure opgelost.
- b) Belangrijke incidenten worden aan het management gerapporteerd.
- c) Escalatieprocedures zijn algemeen bekend, begrepen en toegepast.
- d) Responsteams krijgen regelmatig training.
- e) Het escalatieproces wordt periodiek geëvalueerd.

#### **5 - Continu verbeteren**

##### 5 – Continu verbeteren

- a) Het escalatieproces wordt voortdurend geëvalueerd.
- b) Het oplossen van incidenten wordt regelmatig geanalyseerd om het proces te verbeteren en tekortkomingen en trends worden aan het management gerapporteerd.

#### **Aan de slag**

1. Heb je de pagina Incidentmanagement op de Aanpak IBP en bijbehorende templates onder norm IM.01 Incidentmanagement gevolgd? Dan is er invulling gegeven aan de escalatieprocedure en bijbehorende aspecten.
2. Geef betrokkenen bij afhandeling van incidenten de benodigde instructies en herhaal deze periodiek.

#### **Referentie naar andere normen en kaders**

ISO A5.24, A5.25, A5.26, A6.8

#### **Link naar relevante P normen**

GB.01, GB.02

### **IM.03 Incidentrespons op (cyber)beveiligingsincidenten**

#### **Norm**

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 is dit nodig?**

Als je snel en adequaat kunt reageren op (cyber)beveiligingsincidenten, beperk je de financiële schade en in sommige situaties de imagoschade voor je school als gevolg van grote verstoringen van de infrastructuur, datalekken of informatiediefstal.

#### **1 - Ad hoc**

##### 1 – Ad hoc

- a) Er zijn geen plannen of procedures om een gepaste afhandeling van (cyber)beveiligingsincidenten te

garanderen.

b) Reacties op (cyber)beveiligingsincidenten gebeuren vaak op individuele basis

## **2 - Herhaalbaar**

2 – Herhaalbaar

a) Het management erkent de noodzaak om cyberincidenten af te handelen.

b) Er is een informele procedure voor het afhandelen van (cyber)beveiligingsincidenten.

c) De ontwikkeling van maatregelen voor preventie, aanpak, voorbereiding op en herstel na een (cyber)beveiligingsincident bevindt zich in een vroeg stadium.

## **3 - Bepaald (streefniveau)**

3 – Bepaald

a) Naast de gebruikelijke incident- en problemmanagementprocedures zijn er plannen om preventie, risicobeperking, voorbereiding, tijdige reactie en herstel van (cyber)beveiligingsincidenten aan te pakken.

b) Er zijn rollen en verantwoordelijkheden vastgelegd en toegewezen.

c) De organisatie kan snel reageren op een verstoring, afhankelijk van mogelijke impact op gepaste schaal/escalatieniveau.

## **4 - Beheerst**

4 – Beheerst

a) Plannen voor coördinatie van incidentrespons betrekken alle bedrijfsonderdelen, zoals beleid, juridische afdeling, communicatie, compliance en audit en bedrijfsvoering.

b) Er worden relevante relaties onderhouden met externe partijen zoals politie, CERT en gespecialiseerde bedrijven.

c) Alle (cyber)beveiligingsincidenten worden gemeld bij het schoolbestuur en relevante autoriteiten.

d) Responsplannen zijn gebaseerd op risicoanalyse van de gecompromitteerde data en/of kwetsbaarheidsanalyse.

## **5 - Continu verbeteren**

5 – Continu verbeteren

a) Risico- en trendanalyses worden ingezet om de preventie, aanpak, voorbereiding en herstel van (cyber)beveiligingsincidenten voortdurend te verbeteren.

b) Het oplossen van (cyber)beveiligingsincidenten wordt regelmatig geanalyseerd om het proces te verbeteren. Tekortkomingen worden gerapporteerd aan het management.

## **Aan de slag**

1. Heb je de aanwijzingen op de pagina Incidentmanagement op de Aanpak IBP en de bijbehorende templates onder norm IM.01 Incidentmanagement gebruikt? Dan heb je invulling gegeven aan de preventie, risicobeperking, voorbereiding, tijdige reactie en herstel van (cyber)beveiligingsincidenten en aan de rollen en verantwoordelijkheden.

## **Referentie naar andere normen en kaders**

ISO A5.2, A5.26, A5.27

## **Link naar relevante P normen**

GB.01, GB.02

## IM.04 Problemmanagement

### Norm

Een formeel problemmanagementproces is gedefinieerd en ingevoerd. Komt een incident veelvuldig voor, dan is sprake van een probleem. Er zijn procedures ingesteld om oorzaken van (potentiële) 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 is dit nodig?

Problemmanagement draagt bij aan het verminderen van (beveiligings)incidenten, zowel in aantal als in impact ervan. Als je bij incidenten niet alleen kijkt naar een snelle oplossing, maar ook naar het achterliggende probleem, verklein je de kans dat soortgelijke incidenten zich herhalen.

### 1 - Ad hoc

1 – Ad hoc

- a) Er is geen beleid voor problemmanagement.
- b) Er zijn geen rollen en verantwoordelijkheden voor problemmanagement vastgesteld.
- c) Er zijn geen procedures om oorzaak en gevolg van incidenten te identificeren.
- d) Problemen zullen waarschijnlijk niet gedetecteerd worden.

### 2 - Herhaalbaar

2 – Herhaalbaar

- a) Er is een informeel proces voor problemmanagement.
- b) Enkele deskundige medewerkers kunnen helpen met problemen die hun expertise betreffen, maar de verantwoordelijkheid voor problemmanagement is niet toegewezen.
- c) De registratie en documentatie van problemen en de bijbehorende oplossingen zijn gebrekkig en inconsistent binnen de responsteams.

### 3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is formeel beleid voor problemmanagement en dit is gecommuniceerd.
- b) Er zijn procedures om de oorzaak van problemen te identificeren.
- c) De rollen en verantwoordelijkheden van de organisatie en leveranciers zijn duidelijk vastgesteld.
- d) Er is een formele plek in de organisatie waar problemen geregistreerd, gecommuniceerd, geanalyseerd en toegewezen worden aan verantwoordelijken.
- e) Problemen worden geprioriteerd en toegewezen aan responsteams volgens beleid.
- f) Informatie wordt proactief en op formele wijze gedeeld binnen responsteams.
- g) De managementanalyse van probleemidentificatie en -oplossing is beperkt en informeel.
- h) Bekende fouten worden geregistreerd en beheerst tot ze zijn opgelost.

### 4 - Beheerst

4 – Beheerst

- a) Problemen worden proactief geanalyseerd om oorzaken op te sporen.
- b) Externe bronnen (zoals leveranciers, gebruikersgroepen, conferenties) worden systematisch geraadpleegd om proactief problemen op te sporen.
- c) Voortgang van probleemdiagnose en -oplossing wordt bewaakt en structurele fouten worden geminimaliseerd.
- d) De meeste problemen worden geïdentificeerd, geregistreerd en gerapporteerd, en maatregelen worden genomen.
- e) Problemmanagement wordt periodiek geëvalueerd.

## 5 - Continu verbeteren

### 5 – Continu verbeteren

- a) Er worden tools gebruikt voor het documenteren, rapporteren en analyseren van problemen en oplossingen.
- b) Problemmanagement is geïntegreerd in configuratie- en changemanagement.
- c) De meeste systemen beschikken over automatische detectie- en waarschuwingssystemen, die voortdurend gemonitord en beoordeeld worden.
- d) Problemmanagement wordt geanalyseerd met het oog op voortdurende verbetering.

### Aan de slag

1. Stel een problemmanagementbeleid op. Je kunt hiervoor gebruikmaken van de handreiking Problemmanagement, het template Problemmanagementbeleid en het Problemmanagementproces, waarin de processtappen, de rollen en verantwoordelijkheden en de communicatielijnen zijn benoemd.
2. Stel het problemmanagementbeleid vast.
3. Neem problemen mee in de incidentenregistratie (zie norm IM.01 Incidentmanagement). Gebruik hier bijvoorbeeld het Problemregister voor.
4. Neem problemen mee in de periodieke rapportage aan het management voor de belangrijkste incidenten. Zie voor meer informatie norm IM.01 Incidentmanagement.

### Referentie naar andere normen en kaders

ISO A5.2, A5.24, A6.8

### Link naar relevante P normen

## 7. Changemanagement

Changemanagement – ook wel wijzigingsbeheer – gaat over het beheerst doorvoeren van wijzigingen in het it-landschap. Dit is nodig om een veranderende it-omgeving veilig te houden en de continuïteit te waarborgen. Door wijzigingen op een gestructureerde wijze door te voeren, voorkom je onnodige verstoringen in het onderwijs en de ondersteunende processen. Door changemanagement op de juiste manier in te zetten, verhoog je de digitale weerbaarheid in jouw school.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: it-verantwoordelijke, it-leverancier

Geraadpleegd: Management, adviseur informatiebeveiliging

Geïnformeerd: It-medewerkers

## CH.01 Procedures voor wijzigingen

### Norm

Procedures voor formeel changemanagement 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 is dit nodig?

Goede procedures rondom wijzigingen zorgen ervoor dat het beoordelen, autoriseren, testen, implementeren, documenteren en vrijgeven van voorgestelde wijzigingen eenduidig en gestructureerd gebeurt. Dat draagt bij aan de continuïteit en veiligheid van de bedrijfsvoering en het onderwijs. Anders kan het bijvoorbeeld

voorkomen dat wijzigingen leiden tot verstoringen in de ict, en dat kan weer leiden tot verstoringen in het onderwijs of de bedrijfsvoering.

## **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen beleid of procedure voor wijzigingsbeheer.
- b) (Verzoeken voor) wijzigingen worden niet op een gestandaardiseerde of consistente manier behandeld.
- c) Er zijn geen rollen en verantwoordelijkheden vastgesteld.
- d) Wijzigen worden niet formeel goedgekeurd.
- e) Wijzigingen worden niet of gebrekkig gedocumenteerd.

## **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is beleid voor wijzigingsbeheer om kritische wijzigingen aan te pakken.
- b) Er is een wijzigingsbeheerprocedure die meestal wordt uitgevoerd bij een wijziging.
- c) Rollen en verantwoordelijkheden zijn gedeeltelijk vastgesteld.
- d) Het proces is informeel en er kunnen ongeautoriseerde wijzigingen doorgevoerd worden.
- e) Er is versiebeheer ingevoerd voor essentiële systeemparemeters.

## **3 - Bepaald (streefniveau)**

3 – Bepaald

- a. Het beleid voor wijzigingsbeheer en de werkwijzen zijn gedocumenteerd, gestandaardiseerd en gecommuniceerd.
- b. Er is een formeel wijzigingsbeheerproces voor het wijzigen van applicaties, procedures, processen, systemen en diensten, en de onderliggende platformen en infrastructuur.
- c. Het proces omvat alle componenten van overzetten naar productie, inclusief autorisatie, impactanalyse, release van het management, bijhouden van wijzigingen en rollbackprocedures.
- d. Rollen en verantwoordelijkheden zijn vastgesteld en toegewezen. (Verzoeken voor) wijzigingen worden op een gestandaardiseerde manier behandeld.
- e. Wijzigingen worden gedocumenteerd. Documentatie is correct en actueel.
- f. Er is, of wordt een systeem voor versiebeheer ingevoerd.

## **4 - Beheerst**

4 – Beheerst

- a) Het beleid voor wijzigingsbeheer is volledig opgenomen in de organisatie en wordt consequent toegepast voor alle wijzigingen.
- b) De kwaliteit en effectiviteit van het wijzigingsbeheerproces wordt periodiek geëvalueerd.
- c) Er wordt aan het schoolbestuur of de schoolleiding gerapporteerd.

## **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Het beleid voor wijzigingsbeheer wordt regelmatig geëvalueerd en herzien.
- b) Rollen en verantwoordelijkheden worden voortdurend geëvalueerd.
- c) Uitzonderingen worden geanalyseerd en onderzocht.
- d) Tekortkomingen en trends worden regelmatig aan het management gerapporteerd. Op basis hiervan worden verbeterplannen gemaakt.
- e) De eisen aan rapportage worden regelmatig geëvalueerd en herzien.

## **Aan de slag**

1. Stel een procedure op voor changemanagement. Zorg dat hierin de processtappen, de rollen en verantwoordelijkheden, impactbeoordelingen, noodprocedures, testplannen en de promotie naar productie zijn benoemd.
2. Stel de changemanagementprocedure vast.
3. Bewaar de documentatie rondom wijzigingen, zodat herleidbaar is welk proces gevolgd is.

## **Referentie naar andere normen en kaders**

ISO 8.1, A8.32

## **Link naar relevante P normen**

## **CH.02 Impactassessment, prioriteren en autoriseren**

### **Norm**

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 is dit nodig?**

Met een structurele aanpak voor het beoordelen van wijzigingsverzoeken en hun mogelijke impact, verminder je het risico op verstoring, ongeoorloofde wijziging of verlies van (vertrouwelijke) data.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen procedure voor assessment, prioritering en autorisatie van wijzigingen.
- b) Rollen en verantwoordelijkheden zijn niet vastgesteld.
- c) Impact assessments voor wijzigingsverzoeken worden op ad-hocbasis uitgevoerd en er kunnen ongeautoriseerde wijzigingen plaatsvinden.
- d) Het proces voor categoriseren en prioriteren van wijzigingen is niet gestandaardiseerd.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er wordt een analyse gedaan van de impact van it-wijzigingen.
- b) Criteria voor de analyse zijn in ontwikkeling.
- c) Er is een informeel proces voor categoriseren, prioriteren en autoriseren van wijzigingen.
- d) Rollen en verantwoordelijkheden zijn gedeeltelijk vastgesteld.
- e) Bij het goedkeuringsproces worden vooral de proceseigenaren betrokken.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er is een formele procedure voor categoriseren, prioriteren en autoriseren van wijzigingen en deze is gecommuniceerd.
- b) Voorafgaand aan de wijziging wordt een impactassessment uitgevoerd. Implicaties op het gebied van (cyber)veiligheid, juridische zaken, contracten en wet- en regelgeving worden in dit proces meegenomen.
- c) Er is een formele procedure voor het autoriseren van wijzigingen.
- d) Elk wijzigingsverzoek wordt formeel goedgekeurd door de proceseigenaar en de stakeholders.
- e) Prioritering en categorisering zijn gebaseerd op vooraf vastgestelde criteria.



## **4 - Beheerst**

### **4 – Beheerst**

- a) De procedure voor assessment, categorisering, prioritering en autorisatie van wijzigingen wordt consistent uitgevoerd.
- b) Alle wijzigingen worden gedegen gepland en beoordeeld op impact om de kans op post-productie problemen te minimaliseren.
- c) Het aantal verstoringen en datafouten ten gevolge van verkeerde specificaties en/of incomplete impact assessment is beperkt tot een minimum.
- d) De operationele effectiviteit van de procedures wordt periodiek geëvalueerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) De assessmentprocedure wordt regelmatig geëvalueerd en geactualiseerd.
- b) De prestatie-indicatoren worden regelmatig geëvalueerd.
- c) Het schoolbestuur ontvangt regelmatig rapportages die als input kunnen dienen voor verbeterplannen.
- d) Rapportage-eisen worden regelmatig geëvalueerd en geactualiseerd.

## **Aan de slag**

1. Stel een procedure op voor changemanagement. Zorg dat hierin de processtappen, de rollen en verantwoordelijkheden, impactbeoordelingen, noodprocedures, testplannen en de promotie naar productie zijn benoemd.
2. Stel de changemanagementprocedure vast. Bewaar de documentatie rondom wijzigingen, zodat herleidbaar is welk proces is gevolgd.

## **Referentie naar andere normen en kaders**

ISO 8.1, A8.32

## **Link naar relevante P normen**

## **CH.03 Noodwijzigingen doorvoeren**

### **Norm**

Wijzigingen tijdens een noodsituatie die onmiddellijk doorgevoerd moeten worden, worden op de juiste manier afgehandeld om de impact op systemen en it-toepassingen te minimaliseren. De noodsituatiewijziging wordt na implementatie geregistreerd, geëvalueerd, getest en goedgekeurd door het schoolbestuur.

### **Waarom is dit nodig?**

Om een noodsituatie op te lossen kan een wijziging nodig zijn. Het doorlopen van het normale changemanagementproces duurt dan te lang. Daarom is er voor noodsituaties een route om direct te handelen. Achteraf kun je dan alsnog de benodigde stappen uit het standaardwijzigingsproces uitvoeren, zodat de wijziging goed beheerd wordt.

## **1 - Ad hoc**

### **1 – Ad hoc**

- a) Er is geen procedure voor wijzigingsbeheer voor noodwijzigingen.
- b) (Verzoeken voor) noodwijzigingen worden niet op een gestructureerde manier afgehandeld.
- c) Er is geen of gebrekkige documentatie van noodwijzigingen.
- d) Rollen en verantwoordelijkheden zijn niet gedefinieerd.
- e) Er vindt geen formele goedkeuring van noodwijzigingen plaats.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er is een (informeel) wijzigingsbeheer proces voor noodwijzigingen, die de meest kritieke aspecten van het proces omvat.
- b) Rollen en verantwoordelijkheden zijn gedeeltelijk gedefinieerd.
- c) Na de noodwijziging wordt het beheer niet altijd volledig afgemaakt.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

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

## **4 - Beheerst**

### **4 – Beheerst**

- a) De wijzigingsbeheerprocedure voor noodwijzigingen, inclusief de evaluatie na de implementatie, wordt consequent gevolgd voor alle noodwijzigingen.
- b) De documentatie is correct en actueel.
- c) Er is een proces voor de bewaking van de kwaliteit en de performance van het wijzigingsbeheerproces voor noodwijzigingen.
- d) De kwaliteit en effectiviteit van het proces worden periodiek geëvalueerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Het wijzigingsbeheerproces voor noodwijzigingen wordt regelmatig geëvalueerd en geactualiseerd.
- b) Uitzonderingen worden geanalyseerd en onderzocht.
- c) Er wordt regelmatig aan het management gerapporteerd. Dat levert input op voor verbeterplannen.
- d) Rapportage-eisen worden regelmatig geëvalueerd en geactualiseerd.
- e) Rollen en verantwoordelijkheden worden regelmatig geëvalueerd.

## **Aan de slag**

1. Stel een procedure op voor changemanagement. Zorg dat hierin de processtappen, de rollen en verantwoordelijkheden, impactbeoordelingen, noodprocedures, testplannen en de promotie naar productie zijn benoemd.
2. Stel de changemanagementprocedure vast. Bewaar de documentatie rondom wijzigingen, zodat herleidend is welk proces is gevolgd.

## **Referentie naar andere normen en kaders**

ISO 8.1, A8.32

Certificeringsschema ROSA:  
Beschikbaarheid/Onderhoud

## **Link naar relevante P normen**

### **CH.04 Testomgeving**

#### **Norm**

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

#### **Waarom is dit nodig?**

In een representatieve testomgeving kun je wijzigingen testen zonder dat het gevolgen heeft voor de productieomgeving. Je ziet wél wat het effect van de wijziging is in de productieomgeving.

#### **1 - Ad hoc**

##### **1 – Ad hoc**

- a) Er is geen beveiligde testomgeving gedefinieerd en ingericht voor het ontwikkelen en testen van wijzigingen.
- b) Er is geen beleid voor het gebruik van een testomgeving.
- c) Het is waarschijnlijk dat er door gebrekkig wijzigingsbeheer fouten ontstaan die leiden tot verstoringen in de productieomgeving.

#### **2 - Herhaalbaar**

##### **2 – Herhaalbaar**

- a) Er is een informeel beleid voor het gebruik van een testomgeving voor het ontwikkelen en testen van wijzigingen.
- b) Wijzigingen worden buiten de productieomgeving ontwikkeld en getest.
- c) De testomgeving is voor de kritieke aspecten representatief voor de productieomgeving.

#### **3 - Bepaald (streefniveau)**

##### **3 – Bepaald**

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

#### **4 - Beheerst**

##### **4 – Beheerst**

- a) Er is een proces voor de bewaking van het gebruik van de testomgeving, en incidenten worden beoordeeld en opgelost.
- b) De test- en productieomgevingen worden periodiek geëvalueerd om te garanderen dat de testomgeving nog voldoende representatief is voor de productieomgeving.
- c) De beveiliging van de testomgeving en het testdatamanagement wordt periodiek geëvalueerd.

#### **5 - Continu verbeteren**

##### **5 – Continu verbeteren**

- a) Beleid wordt voortdurend geëvalueerd en verbeterd.
- b) Rollen en verantwoordelijkheden worden voortdurend geëvalueerd.

- c) Er wordt regelmatig aan het management gerapporteerd. Dat levert input op voor verbeterplannen.
- d) De eisen voor rapportage worden regelmatig geëvalueerd en geactualiseerd.
- e) Er zijn tools ingevoerd voor het creëren van subsets en het anonimiseren van data.

#### **Aan de slag**

1. Stel een procedure op voor changemanagement. Zorg dat hierin de processtappen, de rollen en verantwoordelijkheden, impactbeoordelingen, noodprocedures, testplannen en de promotie naar productie zijn benoemd.
2. Stel de changemanagementprocedure vast.
3. Bewaar de documentatie rondom wijzigingen, zodat herleidbaar is welk proces is gevolgd.
4. Gebruik geen productiedata, zeker niet wanneer deze persoonsgegevens bevat. Test met representatieve testdata.

#### **Referentie naar andere normen en kaders**

ISO 8.1, A8.4, A8.31, A8.33

Certificeringsschema ROSA: Vertrouwelijkheid/Scheiding omgevingen

#### **Link naar relevante P normen**

### **CH.05 Testen van wijzigingen**

#### **Norm**

Voorafgaand aan migratie naar de productieomgeving worden wijzigingen op onafhankelijke wijze getest in overeenstemming met het gedefinieerde testplan. Het plan houdt rekening met beveiliging en prestaties.

#### **Waarom is dit nodig?**

Met zorgvuldig testen kun je fouten ontdekken voordat je de wijzigingen in de productieomgeving doorvoert. Dit draagt bij aan het borgen van de continuïteit van de bedrijfsvoering en de betrouwbaarheid van de gegevensverwerking.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen beleid voor het testen van wijzigingen.
- b) Rollen en verantwoordelijkheden voor het testen van wijzigingen zijn niet vastgelegd.
- c) Testen wordt individueel/ad hoc gedaan.
- d) Er worden geen testplannen gemaakt voordat het testen plaatsvindt.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is een informele procedure voor het testen van wijzigingen ingevoerd.
- b) Rollen en verantwoordelijkheden zijn gedeeltelijk vastgesteld.
- c) Er zijn testplannen gemaakt, maar er zijn geen formele criteria voor de inhoud van testplannen.
- d) Er zijn gedeeltelijk maatregelen ingevoerd om ervoor te zorgen dat wijzigingen volgens het testplan getest worden.
- e) Testresultaten worden gedeeltelijk gedocumenteerd.
- f) Er zijn geen criteria voor het bewaren of verwijderen van testresultaten.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a) Formeel beleid voor het testen van wijzigingen is gedocumenteerd en gecommuniceerd.
- b) Rollen en verantwoordelijkheden zijn vastgesteld en toegewezen.
- c) Er worden testplannen gemaakt voordat de tests worden uitgevoerd.
- d) Er zijn criteria vastgesteld om te zorgen dat belangrijke elementen, zoals beveiliging en prestatie, opgenomen zijn in het testplan.
- e) Wijzigingen worden onafhankelijk volgens de testplannen getest.
- f) Er is een beheerprocedure ingevoerd voor het bewaren en verwijderen van testresultaten.
- g) Fallback- of backoutplannen worden voorbereid en getest voordat wijzigingen in productie worden genomen.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Alle wijzigingen van essentiële applicaties worden geëvalueerd en getest zodat er geen negatieve gevolgen zijn voor de bedrijfsvoering of de beveiliging.
- b) Wijzigingen worden alleen getest in de testomgeving.
- c) Prestatie- en beveiligingseisen zijn gevalideerd.
- d) De testprocedures, testplannen en uitvoering van testprocedures worden periodiek geëvalueerd.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a) Beleid wordt voortdurend geëvalueerd en verbeterd.
- b) Rollen en verantwoordelijkheden worden voortdurend geëvalueerd.
- c) Alle incidenten met wijzigingsbeheer/testprocessen worden geëvalueerd en opgelost.
- d) Er wordt regelmatig aan het management gerapporteerd. Dat levert input op voor verbeterplannen.
- e) De eisen aan de rapportages worden regelmatig geëvalueerd en geactualiseerd.

### **Aan de slag**

1. Stel een procedure op voor changemanagement. Zorg dat hierin de processtappen, de rollen en verantwoordelijkheden, impactbeoordelingen, noodprocedures, testplannen en de promotie naar productie zijn benoemd.
2. Stel de changemanagementprocedure vast.
3. Bewaar de documentatie rondom wijzigingen, zodat herleidbaar is welk proces is gevolgd. Maak per wijziging een testplan of zorgt dat een standaardtestaanpak is opgenomen in je changemanagementprocedure en gebruik dit bij het testen van de wijziging.
4. Zorg ervoor dat de tester niet betrokken is geweest bij de ontwikkeling van de softwarewijziging.

### **Referentie naar andere normen en kaders**

ISO 8.1, A8.4, A8.29, A8.32, A8.33

Certificeringsschema ROSA:

Vertrouwelijkheid/Scheiding omgevingen

Beschikbaarheid/Testen

## Link naar relevante P normen

# CH.06 Overzetten naar productieomgeving

## Norm

Na het testen wordt het gewijzigde systeem op gecontroleerde wijze en volgens het implementatieplan overgezet naar de productieomgeving. 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 is dit nodig?

Als je een toepassing volgens het implementatieplan gecontroleerd overzet naar de productieomgeving, verminder of voorkom je verstoringen van de bedrijfsvoering. Ook voorkom je hiermee ongeautoriseerde wijzigingen. Als je het gewijzigde systeem een tijdje gebruikt naast het oude, kun je zien of het nieuwe systeem goed functioneert. Bij problemen kun je altijd terugvallen op het oude systeem.

## 1 - Ad hoc

### 1 – Ad hoc

- a) Er is geen beleid voor de overdracht van gewijzigde systemen naar productie.
- b) De implementatieplannen worden ad hoc ontworpen.
- c) Er zijn geen rollen of verantwoordelijkheden gedefinieerd.

## 2 - Herhaalbaar

### 2 – Herhaalbaar

- a) Er is een informeel beleid voor de overdracht van gewijzigde systemen dat essentiële aspecten, zoals goedkeuring van het proces, bevat.
- b) Rollen en verantwoordelijkheden zijn gedeeltelijk gedefinieerd.
- c) Er worden implementatieplannen gemaakt, maar er zijn geen formele criteria voor de inhoud.
- d) Om overdracht volgens het gedefinieerde implementatieplan te laten verlopen zijn er gedeeltelijk beheersmaatregelen ingevoerd.
- e) Doorgaans worden acceptatietests uitgevoerd.

## 3 - Bepaald (streefniveau)

### 3 – Bepaald

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

## 4 - Beheerst

### 4 – Beheerst

- a) Er is een procedure voor het updaten van systeemdokumentatie, relevante calamiteitenplannen, etc.

- b) Het overdrachtsbeleid wordt consequent ingevoerd.
- c) Een wijziging wordt pas afgesloten als alle activiteiten en registraties zijn ingevoerd en geëvalueerd.
- d) De overdracht van in productie te nemen systemen wordt regelmatig geëvalueerd

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Beleid, rollen en verantwoordelijkheden worden voortdurend geëvalueerd en verbeterd.
- b) Alle incidenten tijdens testen en implementatie worden geëvalueerd en opgelost.
- c) Er wordt regelmatig aan het management gerapporteerd. Dat levert input op voor verbeteringsplannen.
- d) Rapportage-eisen worden regelmatig geëvalueerd en geactualiseerd.

### **Aan de slag**

1. Stel een procedure op voor changemanagement. Zorg dat hierin de processtappen, de rollen en verantwoordelijkheden, impactbeoordelingen, noodprocedures, testplannen en de promotie naar productie zijn benoemd.
2. Stel de changemanagementprocedure vast.
3. Bewaar de documentatie rondom wijzigingen, zodat herleidbaar is welk proces is gevolgd. Bepaal voorafgaand aan het overbrengen van de wijziging acceptatiecriteria en toets hierop.

### **Referentie naar andere normen en kaders**

ISO A8.29, A8.32

Certificeringsschema ROSA: Vertrouwelijkheid/Scheiding omgevingen

### **Link naar relevante P normen**

## **8. Systeemontwikkeling**

Binnen het domein Systeemontwikkeling gaat het om de veilige systeem- en softwareontwikkeling, bijvoorbeeld door de principes van security by design, privacy by design en functiescheiding toe te passen en te zorgen voor een zorgvuldige dataconversie.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: it-verantwoordelijke, it-leverancier

Geraadpleegd: Management, adviseur informatiebeveiliging

Geïnformeerd: It-medewerkers

## **SD.01 Methodiek veilige softwareontwikkeling en -implementatie**

### **Norm**

Er is een gestructureerde aanpak voor de interne ontwikkeling en aanschaf van software ingevoerd, in de vorm van een levenscyclus voor veilige softwareontwikkeling. Deze aanpak zorgt ervoor 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 school- en it-management.

## **Waarom is dit nodig?**

Een gestructureerde aanpak zorgt ervoor dat de ontwikkeling en aanschaf van software gebeurt in lijn met de strategie van de organisatie. Dit draagt eraan bij dat software op een veilige manier wordt ontwikkeld en voldoet aan de functionele, technische en beveiligingseisen, goedkeuringsnormen en de informatiearchitectuur. Daarmee voorkom je digitaal onveilige situaties.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen gestructureerde aanpak.
- b) Systeem- en softwareontwikkeling gebeuren ad hoc.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er zijn richtlijnen voor veilig coderen, maar die worden niet altijd toegepast.
- b) Evaluatie van beveiligingseisen en broncodes vindt plaats op individueel initiatief.
- c) Er zijn geen formele beveiligingsmijlpalen ingevoerd in projectmanagementmethodiek en beveiligingstesten.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) De organisatie heeft een gestructureerde aanpak voor interne ontwikkeling en aanschaf van software ingevoerd.
- b) Er zijn verplichte standaarden voor veilig coderen bepaald. Security by design, privacy by design en privacy by default worden geborgd door richtlijnen en standaarden.
- c) Voor elke nieuwe ontwikkeling of aanschaf is goedkeuring nodig van het juiste niveau van het school- of it-management.
- d) De methodiek voor toetsing van softwarekwaliteit bevat verplichte ‘mijlpalen voor informatiebeveiliging’ (met inbegrip van risicobeoordeling, broncodebeoordeling en tests) die niet kunnen worden omzeild. Deze worden gedocumenteerd.
- e) Bewustwordingstraining voor beveiliging wordt op vrijwillige basis gevolgd.

### **4 - Beheerst**

4 – Beheerst

- a. De effectiviteit van een formele en gestructureerde aanpak wordt periodiek geëvalueerd en indien nodig herzien.
- b. Er is een verplicht beveiligings- en risicotrainingsprogramma voor ontwikkelaars.

### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Op basis van ontwikkelingen in dreigingen worden periodiek risicoanalyses uitgevoerd. De scope van deze analyses omvat de ingevoerde softwareproducten en de ontwikkelingsmethodiek zelf.
- b) Restrisico's worden gerapporteerd aan het verantwoordelijke (senior) it-management

## **Aan de slag**

1. Stel een procedure op voor de ontwikkeling van nieuwe software. Zorg dat binnen deze procedure de verantwoordelijkheden zijn belegd en standaarden voor veilig coderen en secure code review zijn opgenomen.
2. Besteed periodiek binnen het ontwikkelteam aandacht aan training voor veilige softwareontwikkeling.
3. Zorg dat informatiebeveiligingseisen voor softwareontwikkeling deel uitmaken van een aanbesteding.



## **Referentie naar andere normen en kaders**

ISO 8.1, A5.8, A8.25, A8.26, A8.27, A8.28, A8.29, A8.31, A8.30, A8.32

Certificeringsschema ROSA:

Beschikbaarheid/Ontwerp

Integriteit van de gegevens/Application controls

Integriteit van de toepassing/Controle integriteit

## **Link naar relevante P normen**

PR.06

## **SD.02 Toegang productieomgeving door ontwikkelaars**

### **Norm**

Medewerkers en 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 en ontwikkelaars die verantwoordelijk zijn voor het vrijgeven van de broncode voor productie hebben geen schrijftoegang tot de test- of ontwikkelomgeving.

### **Waarom is dit nodig?**

Scheiding van taken tussen ontwikkelaars voorkomt ongeoorloofde toegang tot programma's en gegevens. Ook kunnen ontwikkelaars niet op eigen initiatief wijzigingen doorvoeren. Als er geen scheiding van taken is, kan een ontwikkelaar bijvoorbeeld zijn eigen geschreven code doorvoeren en is er geen controle op de kwaliteit van de software. Dit kan grote negatieve gevolgen hebben, en dat wil je voorkomen.

### **1 - Ad hoc**

1 – Ad hoc

a) Er is geen beleid voor toegangsrestricties tot de productieomgeving voor ontwikkelaars.

### **2 - Herhaalbaar**

2 – Herhaalbaar

a) Er is een beperkt beleid bepaald voor toegang tot productie voor ontwikkelaars.

b) Ontwikkelaars hebben geen schrijftoegang tot de productieomgeving.

c) Bij kritieke incidenten wordt aan ontwikkelaars schrijftoegang tot productie verleend.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

a) Een samenhangend beleid is bepaald, ingevoerd en goedgekeurd door het schoolbestuur of de schoolleiding.

b) Ontwikkelaars hebben geen schrijftoegang tot productie, en systeembeheerders die software overzetten naar productie hebben geen schrijftoegang tot de ontwikkel-, test- en acceptatieomgeving.

c) Uitzonderingen op het beleid worden vooraf goedgekeurd door de systeem-/proceseigenaar en tijdens de tijdelijke schrijftoegang wordt gebruikgemaakt van logging en/of het vierogenprincipe.

### **4 - Beheerst**

4 – Beheerst

a) De effectiviteit van de implementatie en de uitvoering van het beleid worden periodiek geëvalueerd en gedocumenteerd.

- b) Verbeteringen worden bepaald op basis van de evaluatie.
- c) De logs van bij uitzondering toegestane toegang worden periodiek beoordeeld.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Voor de schrijftoegang tot productie wordt gebruik gemaakt van realtime monitoring en detectie. Dit is ingevoerd door middel van geautomatiseerde detectietechnologie, bijvoorbeeld SIEM.
- b) Uitzonderingen worden maandelijks aan het schoolbestuur of de schoolleiding gerapporteerd.

### **Aan de slag**

1. Stel een richtlijn op voor het gebruik van ontwikkel, test, acceptatie en productie omgevingen.

## **Referentie naar andere normen en kaders**

ISO A5.15, A8.2, A8.4, A8.25

Certificeringsschema ROSA: Vertrouwelijkheid/Scheiding omgevingen

## **Link naar relevante P normen**

## **SD.03 Dataconversie en/of migratie**

### **Norm**

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

### **Waarom is dit nodig?**

De kwaliteit van data is erg belangrijk. Het veranderen van de weergave van gegevens in een database van één vorm naar een andere, bijvoorbeeld door verandering van softwaresysteem, vereist dan ook een uiterst accuraat proces met helder gedefinieerde beheersmaatregelen. Dankzij beheersmaatregelen kun je afwijkingen tijdig detecteren. Daarmee waarborg je de integriteit en bijvoorbeeld nauwkeurigheid en volledigheid van de gegevens en het systeem. Zo weet je zeker dat de informatie in systemen klopt.

## **1 - Ad hoc**

### **1 – Ad hoc**

- a) Er zijn geen beheersmaatregelen gedefinieerd voor dataconversie en/of -migratie.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er zijn beperkte beheersmaatregelen ingevoerd om de juistheid en volledigheid van dataconversie/-migratie te valideren.
- b) De gedefinieerde beheersmaatregelen zijn niet volledig gedocumenteerd.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

- a) Er wordt een risico- en impactanalyse uitgevoerd ter rechtvaardiging van de gedefinieerde beheersmaatregelen.
- b) Het ontwerp van de beheersmaatregelen is gedocumenteerd en formeel aanvaard door de eigenaar van het systeem of het proces.
- c) De beheersmaatregelen waarborgen de juistheid en volledigheid van de dataconversie/-migratie en bewaken

de integriteit van de data.

d) De resultaten van de (handmatige en/of geautomatiseerde) uitgevoerde integriteitscontroles worden gedocumenteerd en beoordeeld door de eigenaar van het systeem of het proces om de dataconversie formeel te accepteren.

#### **4 - Beheerst**

4 – Beheerst

a) Een evaluatie van het dataconversie/-migratieproces wordt uitgevoerd door het projectteam.

b) Leer- en verbeterpunten worden geïdentificeerd en gedocumenteerd voor toekomstig gebruik.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

a) De aanpak van conversie/migratie is ingebed in de projectmanagementmethodiek.

b) Controles op juistheid, volledigheid en integriteit zijn volledig geautomatiseerd. Handmatige interventies zijn uitzonderlijk.

#### **Aan de slag**

1. Besteed bij dataconversie aandacht aan zaken als impactanalyse en beheersmaatregelen voor integriteit van de data.

#### **Referentie naar andere normen en kaders**

#### **Link naar relevante P normen**

## **9. Datamanagement**

Datamanagement gaat over het onderhouden van de volledigheid, beschikbaarheid en juistheid van gegevens en over de bescherming van die gegevens. Ook is het bij datamanagement belangrijk dat er eigenaarschap is toegewezen voor alle informatie en informatiesystemen en dat deze geclassificeerd zijn voor het juiste beschermingsniveau.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: It-verantwoordelijke, management

Geraadpleegd: Eindverantwoordelijke voor applicatie en/of data, adviseur informatiebeveiliging

Geïnformeerd: medewerkers van de school

### **DM.01 Data- en systeemeigenaarschap**

#### **Norm**

De organisatie beschikt over procedures en hulpmiddelen om de verantwoordelijkheid voor en eigenaarschap van informatie en informatiesystemen aan te wijzen. Eigenaren beslissen over het classificeren van informatie en informatiesystemen en beschermen ze in overeenstemming met deze classificatie.

#### **Waarom is dit nodig?**

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

## **1 - Ad hoc**

### **1 – Ad hoc**

- a) Er is geen formeel beleid voor data-eigenaarschap.
- b) (Informatie)systeemeigenaarschap wordt niet of informeel aangepakt.
- c) Er zijn geen rollen en verantwoordelijkheden voor data-eigenaarschap toegewezen.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er is beleid voor (informatie)systeem- en data-eigenaarschap.
- b) Het beleid geeft een duidelijke omschrijving van rollen, verantwoordelijkheden en eigenaarschap.
- c) Niet voor alle data en (informatie)systemen zijn verantwoordelijkheden toegewezen.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

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

## **4 - Beheerst**

### **4 – Beheerst**

- a) Beleid en procedures zijn ingevoerd in de organisatie en worden toegepast op alle applicatiesystemen, enterprisearchitectuur, interne en externe datacommunicatie.
- b) Eigenaarschap van belangrijke data (en systemen) wordt periodiek geëvalueerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Het voldoen aan het datamanagementbeleid wordt periodiek aan het schoolbestuur of de schoolleiding gerapporteerd.
- b) Het beleid wordt jaarlijks geëvalueerd, geactualiseerd en goedgekeurd door het schoolbestuur of de schoolleiding.

## **Aan de slag**

1. Zorg ervoor dat data- en systeemeigenaarschap onderdeel uitmaken van het informatiebeveiligingsbeleid. Maak je gebruik van het template IBP-beleid uit de norm GO.02 Beleid informatiebeveiliging? Dan geef je invulling aan de eisen die gesteld worden aan het beleid in volwassenheidsniveau 3. Geef invulling aan dataclassificatie op basis van het certificeringsschema ROSA.

## **Referentie naar andere normen en kaders**

ISO A5.2, A5.9, A5.10, A5.12, A5.13

## **Link naar relevante P normen**

PR.07

## DM.02 Dataclassificatie

### Norm

Er is een dataclassificatieschema dat voor de hele organisatie geldt. Hierin staat hoe kritisch en gevoelig (bijvoorbeeld openbaar, vertrouwelijk, geheim) organisatiegegevens zijn. Het dataclassificatieschema wordt gebruikt als basis voor het toepassen van maatregelen zoals toegangscontrole, archivering en versleuteling. Een dataclassificatieschema bevat daarom details over het eigenaarschap van gegevens, passende (informatie)beveiligingsniveaus en beschermingsmaatregelen en een korte beschrijving van eisen voor het bewaren en vernietigen van gegevens en een beschrijving van de gevoeligheid.

### Waarom is dit nodig?

Organisatiegegevens zijn waardevol en van cruciaal belang. Het is daarom uiterst belangrijk deze zorgvuldig te beschermen. Om dit goed te kunnen doen, is een dataclassificatieschema nodig. Een dataclassificatieschema helpt je om de beveiligingsmaatregelen in lijn te brengen met de eisen die je school stelt voor informatie van die betreffende classificatie. Op deze manier neem je de juiste maatregelen behorend bij het type gegevens dat je verwerkt. Hierdoor creëer je een veilige situatie toegespitst op de gevoeligheid en het beveiligingsniveau van de betreffende gegevens.

### 1 - Ad hoc

1 – Ad hoc

- a) Er is geen dataclassificatieschema.
- b) De organisatie maakt geen verschil tussen de niveaus van gevoeligheid van data.

### 2 - Herhaalbaar

2 – Herhaalbaar

- a) De classificatie van data is informeel en ad hoc.
- b) Individuele interpretaties van dataclassificatieschema's worden toegepast.
- c) Data-eigenaren (indien toegewezen) bepalen zelf de gevoeligheid van de data en eventuele behoefte aan extra maatregelen.

### 3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er zijn een dataclassificatieschema en richtlijnen voor het gebruik daarvan ingevoerd en toegepast binnen de hele organisatie.
- b) Eigendom van data, definities en eisen voor verschillende niveaus van dataclassificatie worden allemaal nadrukkelijk beschreven in de richtlijnen.
- c) De richtlijnen worden gebruikt als een basis voor het toepassen van de benodigde beheersmaatregelen voor kritische processen en/of applicaties.
- d) Het classificatieschema is goedgekeurd door het schoolbestuur of de schoolleiding.

### 4 - Beheerst

4 – Beheerst

- a) De richtlijnen worden gebruikt als basis voor het toepassen van de benodigde beheersmaatregelen voor alle businessprocessen en applicaties binnen de gehele organisatie.
- b) De implementatie en uitvoering van relevante procedures en de juistheid en volledigheid van de classificatieschema's worden periodiek geëvalueerd.

### 5 - Continu verbeteren

5 – Continu verbeteren

- a) (Wijzigingen in) dataclassificatie wordt volledig ondersteund door geautomatiseerde tools, workflowproces-

sing en geïntegreerde dashboards.

b) Dataclassificatie is onderdeel van informatiemanagement en datalifecyclemanagement.

### **Aan de slag**

1. Stel vast dat het certificeringsschema IBP ROSA wordt toegepast voor het classificeren van applicaties binnen de organisatie.
2. Geef door consequente toepassing van het certificeringsschema IBP ROSA invulling aan alle aspecten van het Toetsingskader.

### **Referentie naar andere normen en kaders**

ISO A5.12, A5.13, A5.33

Certificeringsschema ROSA: Vertrouwelijkheid/Levenscyclus gegevens

### **Link naar relevante P normen**

PR.07

## **DM.03 Beveiligingseisen voor datamanagement**

### **Norm**

Beleid en procedures zijn vastgesteld en ingevoerd om informatiebeveiligingseisen te identificeren en toe te passen op de ontvangst, verwerking, opslag en doorgifte van relevante gegevens. Dit is in lijn met de doelstellingen van de school, het informatiebeveiligingsbeleid en wettelijke vereisten, bijvoorbeeld privacy van bepaalde gegevens.

### **Waarom is dit nodig?**

Met beleid en procedures voor de ontvangst, verwerking, opslag en doorgifte van gegevens verklein je het risico dat je school wet- en regelgeving overtreedt.

### **1 - Ad hoc**

1 – Ad hoc

a) Er is geen beleid voor veilig datamanagement vastgelegd.

### **2 - Herhaalbaar**

2 – Herhaalbaar

a) Beperkte en informele informatieveiligheidswensen voor datamanagement zijn bepaald.

b) Er is geen organisatiebreed beleid om informatieveiligheidswensen voor datamanagement te bepalen of toe te passen.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

a) Er is een beleid bepaald, ingevoerd en gecommuniceerd om gevoelige data te beschermen tegen ongeautoriseerde toegang en incorrecte uitwisseling.

b) Het beleid is vastgesteld door het schoolbestuur of de schoolleiding.

c) Er is een formeel proces dat gevoelige data identificeert en uitspraken doet over vertrouwelijkheid en het voldoen aan relevante wet- en regelgeving (zoals dataprivacy).

d) Er is overeenstemming met proceseigenaren over dataclassificatie.

e) De eisen voor essentiële (informatie)systemen zijn in overeenstemming met organisatiedoelen. De eisen zijn

opgesteld voor fysieke en logische toegang tot dataoutput, waarvan de vertrouwelijkheid duidelijk gedefinieerd en afgewogen is.

#### **4 - Beheerst**

4 – Beheerst

- a) De implementatie en uitvoering van procedures omtrent informatieveiligheidseisen voor datamanagement worden periodiek geëvalueerd.
- b) De eisen voor alle informatiesystemen ten aanzien van onder andere fysieke beveiliging, back-up van gevoelige data en opslag in de cloud zijn vastgesteld.
- c) Er zijn bewustwordingsprogramma's ontwikkeld om werknemers bewust te maken van het belang van veilig omgaan met en verwerken van gevoelige data.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) De definitie en toepassing van (informatie)veiligheidseisen zijn opgenomen in informatiemanagement of datalifecyclemanagement.
- b) Bij het opstellen van (informatie)veiligheidseisen voor datamanagement wordt rekening gehouden met efficiëntie en kosten.

#### **Aan de slag**

1. Pas de beveiligingseisen van het certificeringsschema IBP ROSA toe.

#### **Referentie naar andere normen en kaders**

ISO A5.10, A5.14, A5.33, A5.34, A7.7, A7.10, A8.26, A8.33

Certificeringsschema ROSA: Vertrouwelijkheid/Levenscyclus gegevens  
Vertrouwelijkheid/Transport en fysieke opslag

#### **Link naar relevante P normen**

### **DM.04 Inrichting van opslag en retentie**

#### **Norm**

Er zijn procedures gedefinieerd en ingevoerd om gegevens effectief en efficiënt op te slaan, te bewaren en archiveren. Daarmee voldoet de school aan de organisatiedoelstellingen, het informatiebeveiligingsbeleid en wettelijke vereisten.

#### **Waarom is dit nodig?**

Als school stel je alles in het werk om leerlingen, medewerkers en ouders te beschermen. Op alle vlakken, dus ook wanneer het aankomt op het beschermen van de organisatiegegevens. Organisationsgegevens zijn kostbaar en verdienen het om uiterst zorgvuldig behandeld te worden. Je wilt natuurlijk te allen tijde voorkomen dat deze worden gestolen of op straat komen te liggen. Als school moet je bij het verwerken van gegevens voldoen aan wet- en regelgeving. Daarnaast heeft de school haar eigen doelstellingen. Goed omschreven en ingevoerde procedures helpen je om aan de regelgeving en schooldoelstellingen te voldoen. Je bent hierdoor in staat om data veilig op te slaan en zorgt ervoor dat data tijdig wordt gearchiveerd.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er zijn geen procedures voor dataopslag, -bewaring en -archivering.
- b) Dataopslag is ongestructureerd.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er zijn beperkte eisen gedefinieerd voor dataopslagtechnieken.
- b) Er zijn enkele informele richtlijnen voor bewaring en archivering.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

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

## **4 - Beheerst**

### **4 – Beheerst**

- a) Afspraken en maatregelen over het opslaan en bewaren worden periodiek geëvalueerd om te bewerkstelligen dat deze nog steeds in overeenstemming zijn met de organisatiedoelen.
- b) De implementatie en uitvoering van relevante procedures voor het opslaan, bewaren en archiveren van data worden periodiek geëvalueerd.
- c) Datamanagementtechnieken zoals Command Query Responsibility Segregation (CQRS: leesacties zijn gescheiden van schrijfacties) worden bewaakt of ingevoerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Data- en bewaarmaatregelen zijn onderdeel van informatiemanagement en datalifecyclemanagement.
- b) Implementatie, uitvoering en kosten van de datalifecyclemanagementprocedures worden regelmatig geëvalueerd en gerapporteerd aan het schoolbestuur of de schoolleiding.
- c) Datamanagementtechnieken zoals Event Sourcing (ES) worden gevolgd of ingevoerd.

## **Aan de slag**

1. Maak gebruik van een eenduidige wijze voor het opslaan, bewaren en archiveren van data. Neem dit onderwerp op in het IBP-beleid.
2. Stel termijnen vast voor archivering en verwijderen voor alle data- en document-typen. Maak hiervoor gebruik van het Bewaartermijnenoverzicht.

## **Referentie naar andere normen en kaders**

ISO A5.33, A5.34, A7.10, A8.13

Certificeringsschema ROSA: Vertrouwelijkheid/Levenscyclus gegevens  
Vertrouwelijkheid/Transport en fysieke opslag

## **Link naar relevante P normen**

PR.07



## **DM.05 Uitwisseling van (gevoelige) gegevens**

### **Norm**

Er zijn beleid en procedures vastgesteld en ingevoerd om aan de eisen van de bescherming van gegevens en software te voldoen op het moment dat gegevens en software worden uitgewisseld binnen de school of met een externe partij. Gevoelige gegevens worden alleen uitgewisseld via een vertrouwd pad of medium waarbij maatregelen zijn genomen om de authenticiteit van de inhoud, bewijs van versturen, bewijs van ontvangst en onweerlegbaarheid van de oorsprong aan te tonen.

### **Waarom is dit nodig?**

Het implementeren en vaststellen van beleid en procedures is van belang voor de bescherming van gegevens tijdens de uitwisseling van deze gegevens. Op deze manier verklein je de kans op ongeautoriseerde toegang of openbaarmaking van gevoelige informatie.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen beleid of richtlijn voor de uitwisseling van (gevoelige) data binnen de organisatie of met externe partijen.
- b) De organisatie biedt de mogelijkheid om veilig bestanden en documenten uit te wisselen, maar deze mogelijkheden worden niet (consequent) gebruikt.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is een informeel beleid voor data-uitwisseling.
- b) Iedereen binnen de school gebruikt de technieken voor veilige data-uitwisseling die de organisatie biedt.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Het IBP-beleid en de procedures zijn gedefinieerd en ingevoerd om data en software te beschermen en uitwisseling mogelijk te maken.
- b) Het IBP-beleid is goedgekeurd door het schoolbestuur of de schoolleiding en wordt algemeen toegepast.
- c) Bedrijfsdata wordt geclassificeerd naar de mate van vertrouwelijkheid.
- d) Data die uitgewisseld wordt buiten de organisatie moet voor versturen versleuteld worden.
- e) Logs van essentiële applicaties worden geëvalueerd en incorrecte of incomplete data uitwisselingen worden tegengehouden.

### **4 - Beheerst**

4 – Beheerst

- a) Voordat gevoelige data worden verstuurd, wordt de verwerking ervan met application controls gevalideerd.
- b) De relevante applicaties die betrokken zijn bij het loggen en stoppen van incorrecte of incomplete data-uitwisselingen worden periodiek geëvalueerd.
- c) Het data-uitwisselingsbeleid en de effectiviteit daarvan worden periodiek geëvalueerd.

### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) De data-uitwisselingsmethodiek wordt ondersteund door geautomatiseerde (realtime) tooling, workflowprocessing en geïntegreerde dashboards.
- b) Er wordt periodiek gerapporteerd over data-uitwisseling.

## **Aan de slag**

1. Leg in het IBP-beleid vast op welke wijze data en software beschermd zijn. Leg ook vast welke middelen de organisatie inzet om gevoelige data uit te wisselen. Meer informatie over het IBP-beleid lees je in Norm GO.02 Beleid informatiebeveiliging.
2. Houd bij uitwisselingen van data via applicaties toezicht op de logdata, zodat incorrecte en incomplete data-uitwisselingen gestopt worden.

## **Referentie naar andere normen en kaders**

ISO A5.12, A5.14, A5.15, A8.20, A8.21, A8.22, A8.26

## **Link naar relevante P normen**

SW.02

## **DM.06 Verwijdering van data**

### **Norm**

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

### **Waarom is dit nodig?**

Met goede procedures voor het verwijderen van data of hardware verklein je de kans dat er data in de verkeerde handen komt. Op deze manier bescherm je jouw medewerkers en leerlingen. Ook voldoe je hierdoor als school aan de gestelde wet- en regelgeving.

### **1 - Ad hoc**

1 – Ad hoc

- a) Data wordt ad hoc verwijderd.
- b) Er zijn geen formeel vastgelegde procedures voor opschoning en verwijdering van data.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er zijn informele procedures ingevoerd zodat apparatuur en media die gevoelige data bevatten worden verwijderd via een centraal punt in de organisatie.
- b) De verantwoordelijkheden voor dataverwijdering zijn gedeeltelijk gedefinieerd.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er zijn procedures formeel vastgelegd en ingevoerd voor het verwijderen of overdragen van data en hardware om erop toe te zien dat wordt voldaan aan organisatiedoelstellingen en wet- en regelgeving voor het beschermen van (gevoelige) data en software.
- b) Apparatuur en media met gevoelige informatie worden zoveel mogelijk opgeschoond voor gebruik of verwijdering.
- c) De verantwoordelijkheden voor verwijderingsprocedures zijn duidelijk gedefinieerd.

#### **4 - Beheerst**

4 – Beheerst

- a) Niet-opgeschoonde apparatuur en media worden gedurende het verwijderingsproces op een beveiligde manier getransporteerd.
- b) Verwijderde apparatuur en media met gevoelige informatie zijn gedocumenteerd zodat ze te traceren zijn.
- c) De implementatie en uitvoering van relevante procedures voor dataverwijdering worden periodiek geëvalueerd.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Er is een procedure voor de verwijdering van actieve media van de media-inventaris bij verwijdering van het medium.
- b) Er is een procedure voor het onderhoud van de inventaris zodat recente verwijderingen meegenomen worden in het logbestand.
- c) Dataverwijdering is een integraal onderdeel van de informatiemanagement en datalifecyclemanagement

#### **Aan de slag**

1. Zorg ervoor dat een gecertificeerde dienstverlener data verwijdert voor apparatuur en media worden afgevoerd.
2. Wordt apparatuur doorgegeven? Zorg dan dat it alle data van de vorige gebruiker zorgvuldig verwijdert.
3. Let specifiek op de verwijdering van beeldmateriaal bij apparatuur en media van school die door leerlingen worden gebruikt. Wijs hier expliciet op bij inlevering van een device.

#### **Referentie naar andere normen en kaders**

ISO A7.10, A7.14, A8.10

Certificeringsschema ROSA: Vertrouwelijkheid/Levenscyclus gegevens

#### **Link naar relevante P normen**

PR.07

## **10. Identity- en accessmanagement**

Identity- en accessmanagement (IAM) – ook wel identiteits- en toegangsbeheer genoemd – zorgt voor het beheren van de logische toegang tot informatie, informatiediensten en externe koppelingen. Met logische toegang wordt de toegang tot systemen bedoeld. Het gaat hierbij onder andere om beleid rondom toegangsrechten, functiescheiding en superuserrechten om de informatie van jouw organisatie, medewerkers en leerlingen te beveiligen tegen ongeoorloofde toegang.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: It-verantwoordelijke, applicatiebeheerder

Geraadpleegd: Management, IBP-verantwoordelijke

Geïnformeerd: Medewerkers van de school

## **ID.01 Toegangsrechten toewijzen**

### **Norm**

De organisatie heeft in een autorisatiematrix toegangsgroepen of rollen gedefinieerd op basis van – door het schoolbestuur – vastgestelde regels, waaronder functiescheiding. Er zijn procedures vastgesteld die tijdige initiatie en update in de autorisatiematrices voor alle toepassingen regelen. Het schoolbestuur 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, token of biometrische informatie.

### **Waarom is dit nodig?**

Door toegangsrechten toe te wijzen aan groepen of rollen, maak je scheiding van functies mogelijk en schep je een duidelijke grondslag voor de toekenning van rechten aan personen. Als je alle activiteiten kunt herleiden tot een persoon, kun je bij incidenten nagaan wie wat wanneer gedaan heeft. Dit komt de betrouwbaarheid van gegevens en continuïteit ten goede.

### **1 - Ad hoc**

#### 1 – Ad hoc

- a) Er is geen beleid voor informatietoegang.
- b) Er is geen SOLL-autorisatiematrix.
- c) Niet alle activiteiten kunnen getraceerd worden naar uniek identificeerbare gebruikers.

### **2 - Herhaalbaar**

#### 2 – Herhaalbaar

- a) Er is informeel beleid voor informatietoegang ingevoerd.
- b) Er is een SOLL-autorisatiematrix gedefinieerd, maar niet formeel vastgesteld.
- c) Activiteiten van gebruikers met veel rechten kunnen getraceerd worden naar uniek identificeerbare gebruikers.
- d) De gedefinieerde rollen en toegangsrechten van gebruikers zijn volgens organisatiebehoeften.
- e) Functie-eisen zijn verbonden aan gebruiker-id's.

### **3 - Bepaald (streefniveau)**

#### 3 – Bepaald

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

### **4 - Beheerst**

#### 4 – Beheerst

- a) (Kosteneffectieve) technische en beleidsmatige maatregelen voor gebruikersidentificatie, gebruikersauthenticatie en het afdwingen van gebruikersrechten worden up-to-date gehouden en periodiek geëvalueerd en gedocumenteerd.
- b) Op basis van de evaluaties worden verbeteringen bepaald.

### **5 - Continu verbeteren**

#### 5 – Continu verbeteren

- a) De werking en verbeteringen van de procedures rondom toegangsrechten en toepassingen worden voortdurend gevolgd.

## **Aan de slag**

1. Maak logische toegangsbeveiliging onderdeel van het IBP-beleid. Zie voor meer informatie over het IBP-beleid norm GO.02 Beleid informatiebeveiliging.
2. Laat een autorisatiematrix vaststellen door de systeem- of proceseigenaar voor alle kritische applicaties. Denk hierbij aan financiële administratie, personeelsadministratie, leerlingenadministratie, LAS en elektronische leeromgevingen. Hiermee wordt voorkomen dat op individueel niveau telkens opnieuw toegangsrechten bepaald moeten worden en het maakt uitzonderingen goed te beargumenteren. Gebruikers krijgen alleen toegang tot de systemen en informatie op een need to know basis. Dat wil zeggen op basis van wat ze vanuit hun rol nodig hebben.
3. Onderzoek minimaal elk kwartaal of de toegekende toegangsrechten overeenkomen met de vastgestelde autorisatiematrix. Leg afwijkingen voor aan de systeemeigenaar.
4. Zorg ervoor dat elke applicatie werkt met identificatie, authenticatie en autorisatie van gebruikers.
5. Sla gebruiker-id's en toegangsrechten centraal op.

## **Referentie naar andere normen en kaders**

ISO A5.2, A5.3, A5.15, A5.16, A5.17, A5.18, A8.2

Certificeringsschema ROSA:

Integriteit van de gegevens/Herleidbaarheid

## **Link naar relevante P normen**

## **ID.02 Administratie van toegangsrechten**

### **Norm**

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

### **Waarom is dit nodig?**

Een goede administratie van toegangsrechten maakt het mogelijk om de continuïteit van de processen te waarborgen. Stel je voor dat een medewerker vertrekt zonder dat de toegangsrechten goed zijn gedocumenteerd en beheerd. Dit kan problemen veroorzaken, zoals het niet kunnen openen van belangrijke gegevens of het uitvoeren van cruciale taken. Daarnaast maakt een goede administratie de rechten van de individuele gebruiker zichtbaar. Dit betekent dat het duidelijk is wie toegang heeft tot welke systemen, gegevens of functies binnen je organisatie. Deze transparantie is vanwege veiligheid, compliance en verantwoording. Het stelt je in staat om te controleren of gebruikers alleen toegang hebben tot wat ze nodig hebben voor hun functie en zo risico's op misbruik van data of datalekken te minimaliseren. Bovendien draagt het bij aan het vertrouwen van medewerkers en leerlingen dat hun gegevens veilig worden beheerd en behandeld.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen beleid voor gebruikersaccounts en bijbehorende rechten.
- b) Er is geen administratieve procedure voor het vastleggen van gebruikers en rollen.
- c) Toegangsrechten worden ad hoc toegekend afhankelijk van individuen.

d) Gebruikers zouden meer rechten kunnen hebben dan volgens het need-to-know/need-to-have-principe nodig is.

## **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is informeel beleid voor alle gebruikersaccounts en toegangsrechten (intern, extern, administrator) en omstandigheden (normaal, noodgeval).
- b) Er is een administratieve procedure voor het vastleggen van accounts en rechten, maar deze is niet formeel vastgesteld.
- c) Toegang tot informatie is bepaald op basis van informatierisicomanagement en komt overeen met beleids- en beveiligingseisen.
- d) Accounts worden geblokkeerd en toegangsrechten ingetrokken als een gebruiker ontslag neemt of ontslagen wordt.

## **3 - Bepaald (streefniveau)**

3 – Bepaald

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

## **4 - Beheerst**

4 – Beheerst

- a) De toegangsrechten van werknemers worden periodiek vergeleken met hun verantwoordelijkheden.
- b) Op basis van deze vergelijkingen worden verbeteringen voorgesteld.

## **5 - Continu verbeteren**

5 – Continu verbeteren

- a) De performance en verbetering van accountbeheer en gerelateerde toegangsrechten worden voortdurend gemonitord.
- b) Tools (zoals provisioning) voor identity- en accessmanagement zijn succesvol ingevoerd.

## **Aan de slag**

1. Zie norm ID.01 voor beleid en rol gebaseerde toegang.
2. Stel een proces op voor het toekennen en wijzigen van toegangsrechten.

## **Referentie naar andere normen en kaders**

ISO A5.2, A5.3, A5.15, A5.16, A5.17, A5.18, A6.5, A8.2, A8.3, A8.4, A8.5

## **Link naar relevante P normen**

## **ID.03 Monitoring en toegang superusers**

### **Norm**

Het schoolbestuur 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 is dit nodig?**

Superuseraccounts zijn accounts met verhoogde rechten die gebruikers vaak onbeperkte toegang geven tot alle delen van een computersysteem, inclusief gevoelige bestanden en instellingen. De gevolgen van verkeerd gebruik kunnen verstrekkend zijn. Superusers kunnen bepaalde beheertaken uitvoeren, die ‘gewone’ gebruikers niet kunnen uitvoeren. Zij hebben de mogelijkheid om belangrijke systeeminstellingen te wijzigen en kritieke bestanden te benaderen. Als kwaadwillende personen of malware toegang krijgen tot deze rechten, kunnen ze schade aanbrengen aan het systeem, gegevens stelen of schadelijke acties uitvoeren. Het is belangrijk om de superuserrechten te beperken en te monitoren om ongeoorloofde toegang en verstoringen te verminderen.

### **1 - Ad hoc**

#### **1 – Ad hoc**

- a) Er is geen beleid voor invulling en gebruik van superuserrechten.
- b) Er is geen procedure voor het toekennen van superuserrechten.
- c) Er is geen gedefinieerde groep individuen aan wie superuserrechten toegekend mogen worden.

### **2 - Herhaalbaar**

#### **2 – Herhaalbaar**

- a) Er is een informeel beleid voor het gebruik en een informele procedure voor de toekenning van superuserrechten.
- b) De individuen die geautoriseerd zijn om superuserrechten toe te kennen zijn goedgekeurd door het schoolbestuur.
- c) Gebruik van de superuserrechten wordt vastgelegd en in geval van een incident geanalyseerd.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a) Er is een formele procedure voor superuserrechten gedefinieerd, gedocumenteerd en gecommuniceerd.
- b) De personen met superuserrechten en de bijbehorende superuserrechten zijn vastgelegd en toekenning is goedgekeurd door het schoolbestuur.
- c) Gebruik van de superuserrechten wordt gelogd en geëvalueerd.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Gebruik van de superuserrechten wordt voortdurend gemonitord.
- b) De superuserprocedure en de superusertoegang wordt periodiek geëvalueerd.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a) Op basis van de periodieke evaluaties wordt de superuserprocedure verbeterd (als onderdeel van IAM).
- b) Tekortkomingen en trends worden gerapporteerd aan het schoolbestuur.

### **Aan de slag**

1. Verwerk de kaders voor superuserrechten in het IBP-beleid. Zie voor meer informatie over het opstellen van je IBP-beleid norm ID.01 Beleid informatiebeveiliging.
2. Zorg voor een goede, up-to-date administratie van de superuserrechten en de personen aan wie deze rechten zijn toegekend.

3. Log elk gebruik van superuserrechten.
4. Evalueer periodiek of de superuserrechten volgens de kaders zijn gebruikt en of de toekenning nog altijd nodig is.

#### **Referentie naar andere normen en kaders**

ISO A8.2, A8.5, A8.15

Certificeringsschema ROSA:

Integriteit van de toepassing/Herleidbaarheid

#### **Link naar relevante P normen**

### **ID.04 Noodprocedure superuserrechten**

#### **Norm**

Er is een procedure vastgesteld om in geval van nood toegang van accounts met superuserrechten te beheren.

#### **Waarom is dit nodig?**

Om tijdens een noodgeval adequaat te kunnen handelen is een noodprocedure nodig. Tijdens een noodgeval kan het nodig zijn om bepaalde handelingen uit te voeren die alleen gedaan kunnen worden met een superuseraccount. De reguliere procedure voor de toekenning van deze accounts is bij een noodsituatie mogelijk te complex. Denk aan het uitvallen van een kritiek systeem, waarbij een superuseraccount nodig is om het te kunnen herstellen. Het kan dan voor de continuïteit nodig zijn dat iemand zonder superuserrechten handelingen kan uitvoeren die eigenlijk voorbehouden zijn aan gebruikers met superuserrechten.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen noodprocedure.
- b) Het gebruik van noodtoegang met superuserrechten wordt niet of ad hoc gemonitord.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is een noodprocedure maar deze is niet formeel vastgesteld.
- b) Er is bepaald welke individuen geautoriseerd zijn om tijdelijke superuserrechten toe te kennen.
- c) Noodingrepen worden vastgelegd.
- d) Na elke noodtoegang worden wachtwoorden gewijzigd.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

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

#### **4 - Beheerst**

4 – Beheerst

- a) De implementatie en de uitvoering van de noodprocedure worden periodiek geëvalueerd.



## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Geautomatiseerde Privileged Access Management (PAM) tools zijn ingevoerd.
- b) Op basis van de periodieke evaluaties worden de noodprocedure en de implementatie daarvan verbeterd.
- c) Tekortkomingen en trends worden aan het schoolbestuur of de schoolleiding gerapporteerd.

### **Aan de slag**

1. Zorg ervoor dat een noodprocedure voor kritieke accounts onderdeel is van het proces rondom toegangsrechten.
2. Indien de noodprocedure wordt gebruikt, leg dit dan vast.
3. Evalueer na afloop van de noodsituatie de noodprocedure en voer eventueel verbeteringen door. Ga na of gebruik ervan volgens alle afspraken heeft plaatsgevonden.

### **Referentie naar andere normen en kaders**

ISO A8.2, A8.15

### **Link naar relevante P normen**

## **ID.05 Periodieke beoordeling van toegangsrechten**

### **Norm**

Het management beoordeelt periodiek de gebruikerstoegang die ingevoerd is voor de relevante applicaties (IST-situatie) om de juistheid van 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 is dit nodig?**

Je wil voorkomen dat iemand ongeautoriseerd toegang krijgt tot het besturingssysteem, gegevens en applicaties. Daarom controleert het management periodiek de toegangsrechten.

### **1 - Ad hoc**

#### **1 – Ad hoc**

- a) Er is geen formeel vastgelegde procedure voor identity- en accessmanagement voor besturingssystemen en -applicaties.
- b) Er is geen SOLL-situatie gedefinieerd.
- c) Evaluatie wordt ad hoc door individuen gedaan.

### **2 - Herhaalbaar**

#### **2 – Herhaalbaar**

- a. Er is een procedure voor identity- en accessmanagement voor besturingssystemen en -applicaties, maar deze is niet formeel vastgelegd.
- b. Er worden ad hoc SOLL-IST-evaluaties uitgevoerd voor gebruikers met veel privileges (verkopers, leveranciers, zakenpartners).

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a) De procedures voor identity- en accessmanagement en SOLL-IST-evaluaties zijn gedefinieerd, gedocumen-

teerd en formeel vastgelegd.

b) De SOLL- en IST-matrices worden voor alle gebruikers periodiek vergeleken, geëvalueerd en goedgekeurd door het management.

c) Ongepaste toegangsrechten worden ingetrokken.

d) De procedures voor identity- en accessmanagement en de SOLL-IST-evaluaties worden periodiek geëvalueerd en zijn effectief.

#### **4 - Beheerst**

4 – Beheerst

a) Op basis van periodieke evaluaties worden de procedures voor het beheer van toegangsrechten en SOLL-IST evaluaties gereviewd en verbeterd (als onderdeel van IAM).

#### **5 - Continu verbeteren**

5 – Continu verbeteren

a) Tekortkomingen en trends worden automatisch gerapporteerd aan het schoolbestuur of de schoolleiding en indien van toepassing worden toegangsrechten automatisch ingetrokken volgens gerapporteerde uitzonderingen.

b) Periodiek worden er databasechecks uitgevoerd om de huidige processen te toetsen in relatie tot de functiescheidingsmatrix. Hierbij wordt gekeken naar ongebruikelijke transacties en gebieden voor verbetering (bijvoorbeeld met procesminingtechnieken).

#### **Aan de slag**

1. Zorg dat de periodieke controle op de toegekende rechten en rollen opgenomen is in het proces rondom toegangsrechten. Blijkt uit controle dat er ongepaste toegangsrechten zijn? Geef dan opdracht aan it om deze rechten in te trekken.

#### **Referentie naar andere normen en kaders**

ISO A5.1, A5.18, A8.2

Certificeringsschema ROSA: Vertrouwelijkheid/Logische toegang

#### **Link naar relevante P normen**

## **11. Securitymanagement**

Securitymanagement gaat over de meer technische kant van informatiebeveiliging: ervoor zorgen dat risico's op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zoveel mogelijk geadresseerd en gemitigeerd worden. Hierbij kun je denken aan dreigingen en kwetsbaarheden, bescherming tegen malware en borging van informatiebeveiliging bij mobiele apparaten.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Hoofd it, adviseur informatiebeveiliging

Geraadpleegd: IBP-verantwoordelijke

Geïnformeerd: Medewerkers van de school

### **SM.01 Beveiligingsbaselines**

#### **Norm**

Beveiligingsbaselines 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 schoolbestuur of de schoolleiding. De verantwoordelijke it-medewerkers worden hiervan op de hoogte gesteld. Ingevoerde beveiligingsinstellingen voor it-middelen worden periodiek beoordeeld op naleving van beveiligingsbaselines. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

### **Waarom is dit nodig?**

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

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er zijn geen beveiligingsbaselines.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er zijn beveiligingsbaselines gedefinieerd voor de belangrijkste it-infrastructuurcomponenten.
- b) Beveiligingsbaselines worden ad hoc ingevoerd en afwijkingen van de baselines worden niet gedocumenteerd.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Beveiligingsbaselines zijn gedefinieerd, goedgekeurd door het schoolbestuur of de schoolleiding en gecommuniceerd naar verantwoordelijk it-medewerkers.
- b) De ingevoerde beveiligingsinstellingen voor it-middelen worden periodiek gecontroleerd op overeenstemming met de beveiligingsbaselines.
- c) Resultaten worden gedocumenteerd, afwijkingen worden gedocumenteerd en goedgekeurd (of gecorrigeerd).
- d) Voor nieuwe it-infrastructuurcomponenten en projectmanagementprocessen wordt implementatie van beveiligingsbaselines afgedwongen.
- e) Periodiek wordt aan het schoolbestuur of de schoolleiding gerapporteerd in hoeverre aan de baseline wordt voldaan.

#### **4 - Beheerst**

4 – Beheerst

- a) Beveiligingsbaselines worden periodiek geëvalueerd en indien nodig geactualiseerd.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Door middel van continue monitoring en/of audittools wordt bewaakt in welke mate aan de beveiligingsbaselines wordt voldaan.
- b) Afwijkingen van de baselines worden realtime gerapporteerd en indien nodig gecorrigeerd.

### **Aan de slag**

1. Bepaal welke minimale beveiligingsinstellingen nodig zijn voor veilig gebruik van bedrijfskritische applicaties. Leg dit vast in een beveiligingsbaseline. Het schoolbestuur moet deze beveiligingsbaseline vaststellen.
2. Controleer de instellingen van applicaties minimaal jaarlijks op de beveiligingsbaseline. Doe dit standaard na elke wijziging.
3. Documenteer en corrigeer afwijkingen in het incidentenregister. Wordt de afwijking niet gecorrigeerd? Documenteer dan de acceptatie ervan.

4. Neem bij de ontwikkeling van it-middelen de implementatie van de beveiligingsbaselines mee.
5. Rapporteer over afwijkingen op de baseline in de periodieke incidentenrapportage aan het bestuur.

#### **Referentie naar andere normen en kaders**

ISO A5.8, A5.36, A5.37

#### **Link naar relevante P normen**

### **SM.02 Authenticatiemechanismes**

#### **Norm**

Alle gebruikers (intern, extern en tijdelijk) en hun activiteiten op it-systemen moeten uniek en identificeerbaar zijn. Het management is verantwoordelijk voor de periodieke controle van de lijst met actieve id's in relevante applicaties. Dit is nodig om te bepalen of unieke gebruiker-id's zijn doorgevoerd, zodat activiteiten traceerbaar zijn. Daarnaast moet het management ervoor zorgen dat algemene- en systeemaccounts geblokkeerd zijn of op andere wijze beschermd zijn. Alle onjuiste of inactieve gebruiker-id's die tijdens het controleproces worden opgemerkt, worden direct gedeactiveerd.

#### **Waarom is dit nodig?**

Authenticatiemechanismes zorgen voor geoorloofde toegang tot programma's en gegevens, doordat je daarmee activiteiten kunt herleiden tot gebruikers. Daarnaast voorkom je ongeoorloofde toegang als je de identiteit van gebruikers kunt vaststellen.

#### **1 - Ad hoc**

##### **1 – Ad hoc**

- a) Er is geen beleid voor beheer van gebruikersauthenticatie.
- b) Er is geen procedure voor identity- en accessmanagement.
- c) Authenticatie niet afgedwongen voor het verlenen van toegang.
- d) Niet alle systeempromessen en activiteiten van gebruikers kunnen getraceerd worden naar een uniek identificeerbare gebruiker.
- e) Ad-hoc maatregelen zijn afhankelijk van individuen.

#### **2 - Herhaalbaar**

##### **2 – Herhaalbaar**

- a) Er is een informeel beleid voor gebruikersauthenticatie.
- b) Er zijn administratieve procedures voor identificatie, authenticatie en autorisatie van gebruikers, maar deze zijn niet formeel.
- c) Voor het verlenen van toegang wordt authenticatie afgedwongen.
- d) Alle activiteiten van gebruikers kunnen getraceerd worden naar uniek identificeerbare gebruikers.
- e) De rollen die zijn vastgelegd voor het verlenen van toegang zijn in lijn met de organisatiebehoeften, gebaseerd op need-to-know en goedgekeurd door de proceseigenaar.
- f) Functie-eisen zijn gekoppeld aan gebruiker-id's.
- g) Systeem- of generieke gebruiker-id's zijn beschermd.

#### **3 - Bepaald (streefniveau)**

##### **3 – Bepaald**

- a) Formeel beleid en procedures voor gebruikersauthenticatie en identity- en accessmanagement zijn gedefinieerd, gedocumenteerd, geformaliseerd en gecommuniceerd. Hieronder valt ook de toestemmingsprocedure voor de data- of systeemeigenaar die toegangsrechten toekent.
- b) Voor logische toegang tot alle systemen en bronnen wordt gebruikgemaakt van toegangsbepaling en

authenticatiebeheer voor alle gebruikers.

c) Er is een strikte functiescheiding voor het aanvragen, toekennen, implementeren en intrekken van toegangsrechten van gebruikers.

d) Gebruiker-id's en toegangsrechten worden bijgehouden in een centrale opslag.

e) Ongepaste of inactieve gebruikersrechten worden tijdig uitgeschakeld.

f) Het gebruik van tweefactorauthenticatie wordt afgedwongen voor toegang vanaf niet-vertrouwde omgevingen en kritieke systemen. Een bedrijfskritische applicatie waar (jonge) leerlingen op inloggen kan hierop een uitzondering zijn, omdat dit simpelweg te veel vraagt van de gebruiker. Voer in dat geval een risicoanalyse uit voor benodigde mitigerende maatregelen.

#### **4 - Beheerst**

4 – Beheerst

a) De implementatie en uitvoering van relevante procedures worden periodiek geëvalueerd en vastgelegd. Op basis van deze evaluaties worden verbeteringen doorgevoerd.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

a) De performance en verbetering van identity- en accessmanagement, authenticatietechnieken en -controls worden voortdurend gemonitord.

#### **Aan de slag**

1. Definieer de kaders voor authenticatie in het IBP-beleid. Zie voor meer informatie over het opstellen van een IBP-beleid norm GO.02 Beleid informatiebeveiliging. Richt een proces in voor het aanvragen, toekennen, toewijzen en intrekken van toegang.
2. Houd gebruiker-id's en toegangsrechten op een centrale plek bij.
3. Controleer periodiek op inactieve gebruikers en schakel deze inactieve gebruikers uit.
4. Pas tweefactorauthenticatie toe voor toegang vanaf niet-vertrouwde omgevingen en kritieke systemen.

#### **Referentie naar andere normen en kaders**

ISO A5.3, A5.8, A5.15, A5.16, A5.17, A5.18, A8.3

Certificeringsschema ROSA:

Vertrouwelijkheid/Logische toegang

#### **Link naar relevante P normen**

### **SM.03 Mobiele apparaten en telewerken**

#### **Norm**

Informatiebeveiliging wordt geborgd bij het gebruik van mobiele apparaten en telewerkfaciliteiten. Mobile Device Management, versleuteling en bescherming tegen malware zijn aanwezig om de risico's te beperken.

#### **Waarom is dit nodig?**

Het gebruik van Mobile Device Management, versleuteling en bescherming tegen malware helpen bij de bescherming van gegevens van de organisatie.

## **1 - Ad hoc**

### **1 – Ad hoc**

- a) Beleid voor het gebruik en beveiliging van mobiele apparaten en/of telewerkfaciliteiten ontbreekt.
- b) Procedures voor het aanvragen, goedkeuren, verstrekken en accepteren van mobiele apparaten en/of telewerkfaciliteiten ontbreken.
- c) Bedrijfsgegevens worden mogelijk niet versleuteld opgeslagen op mobiele apparaten.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er is informeel beleid voor het beveiligen van mobiele apparaten en/of telewerkfaciliteiten.
- b) Er is een informele procedure voor het aanvragen, goedkeuren, verstrekken en accepteren van mobiele apparaten en/of telewerkfaciliteiten
- c) Toegang tot een mobiel apparaat wordt alleen verleend na gebruik van een (sterk) wachtwoord.
- d) Er worden geen (niet versleutelde) organisatiegegevens opgeslagen op mobiele apparaten (zero footprint).

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

- a) Formeel beleid en procedures voor het beveiligen van mobiele apparaten en/of telewerkfaciliteiten worden gedocumenteerd en gecommuniceerd (Mobile Device Management).
- b) Anti-malwaresoftware op mobiele apparaten wordt up-to-date gehouden.
- c) In geval van verlies of diefstal van een apparaat wordt de communicatie met gecentraliseerde applicaties afgesloten.
- d) Er worden geen organisatiegegevens opgeslagen op telewerkfaciliteiten thuis of elders (zero footprint).
- e) De vertrouwde (logische) werkplek is beschermd tegen malware.
- f) Bedrijfsgegevens in niet vertrouwde omgevingen worden alleen afgedrukt na een risicobeoordeling.

## **4 - Beheerst**

### **4 – Beheerst**

- a) De implementatie en uitvoering van Mobile Device Management wordt periodiek geëvalueerd en gedocumenteerd. Op basis van evaluaties worden verbeteringen vastgesteld.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Prestaties en verbeteringen van beveiligde mobiele apparaten en/of telewerkfaciliteiten worden continu gemonitord.

## **Aan de slag**

1. Maak gebruik van Mobile Device Management of Mobile Application Management (MDM/MAM) voor het beveiligen van mobiele apparaten of telewerkfaciliteiten. Neem dit op in het IBP-beleid. Zie voor meer informatie over het opstellen van IBP-beleid norm GO.02 Beleid informatiebeveiliging. Het MDM of MAM moet dusdanig zijn ingesteld dat invulling wordt gegeven aan de elementen van volwassenheidsniveau 3.
2. Er is een Gedragscode Veilig gebruik ict-middelen en persoonsgegevens opgesteld voor zowel leerlingen als medewerkers. Je kunt hiervoor de Voorbeeldgedragscode Veilig gebruik ict-middelen en persoonsgegevens gebruiken.

## **Referentie naar andere normen en kaders**

ISO A6.7, A8.1

## **Link naar relevante P normen**

### **SM.04 Logging systeemactiviteiten**

#### **Norm**

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

#### **Waarom is dit nodig?**

Logging helpt om ongepaste of ongebruikelijke activiteiten op tijd op te merken en vervolgacties uit te voeren. Logging is het vastleggen van gebeurtenissen en activiteiten die plaatsvinden in het systeem. Dit proces omvat het registreren van relevante informatie, zoals tijdstippen, uitgevoerde acties, foutmeldingen en andere relevante gegevens. De bewaartermijnen moeten aansluiten bij wet- en regelgeving.

#### **1 - Ad hoc**

##### **1 – Ad hoc**

- a) Eisen voor logging zijn gedeeltelijk gedefinieerd en gedocumenteerd.
- b) Logging wordt niet structureel en slechts ad hoc geëvalueerd en is afhankelijk van individuen.

#### **2 - Herhaalbaar**

##### **2 – Herhaalbaar**

- a) Eisen zijn gedocumenteerd maar niet formeel vastgelegd.
- b) Er is een procedure voor de evaluatie van logging gedefinieerd maar niet formeel vastgelegd.
- c) Logging is ingevoerd voor relevante it-componenten en wordt periodiek geëvalueerd.
- d) Activiteiten van administrators en operators worden ook gelogd en periodiek geëvalueerd.
- e) Interne systeemklokken worden gesynchroniseerd.
- f) Er zijn bewaartermijnen vastgesteld voor logs en toegangsrechten.

#### **3 - Bepaald (streefniveau)**

##### **3 – Bepaald**

- a) 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 een risicoanalyse.
- b) De procedure is volgens de vereisten vastgesteld door de school.
- c) Het loggen van ongebruikelijke activiteiten en incorrecte of gebrekkige logging wordt gedocumenteerd, geanalyseerd en opgevolgd met gepaste maatregelen.

#### **4 - Beheerst**

##### **4 – Beheerst**

- a) De implementatie en uitvoering van relevante procedures en werkwijzen worden periodiek geëvalueerd en gedocumenteerd. Verbeteringen worden bepaald op basis van deze evaluaties.

#### **5 - Continu verbeteren**

##### **5 – Continu verbeteren**

- a) Geautomatiseerde detectie- en responsetechnologie, zoals SIEM (Security Incident en Event Management-systeem), is volledig ingevoerd.
- b) De performance en verbeteringen van de loggingprocedures worden voortdurend bewaakt.

## **Aan de slag**

1. Bepaal op basis van een expliciete risicoafweging per applicatie of en hoelang de logging bewaard moet worden en of er aanvullende eisen voor de logging zijn.
2. Zorg ervoor dat een logregel minimaal informatie over de gebeurtenis of handeling bevat, welke gebruiker deze uitvoert, vanaf welk apparaat dit gebeurt, het resultaat van de actie en een datum en tijdstip van de handeling.
3. Leg ook activiteiten van systeembeheerders vast.
4. Zorg voor waarborgen die verhinderen dat de logging gewijzigd kan worden. Eventuele wijzigingen in logging of pogingen tot het verwijderen van logging moeten vastgelegd worden in de logging zelf.
5. Controleer de logging periodiek om ongebruikelijke activiteiten te ontdekken. Grotere organisaties kunnen hiervoor bijvoorbeeld een SIEM inzetten. Deze voert automatische controle uit en gaat na of de logging correct gebeurt.
6. Zorg ervoor dat it een overzicht heeft van alle logbestanden binnen de organisatie.

## **Referentie naar andere normen en kaders**

ISO A8.15, A8.16

Certificeringsschema ROSA:

Integriteit van de gegevens/Onweerlegbaarheid

Integriteit van de toepassing/Onweerlegbaarheid

Vertrouwelijkheid/Logging

## **Link naar relevante P normen**

### **SM.05 Testen, inspectie en toezicht beveiliging**

#### **Norm**

Implementatie van it-beveiliging wordt proactief getest en bewaakt. It-beveiliging wordt regelmatig getoetst om ervoor te zorgen dat de door de organisatie goedgekeurde baseline voor informatiebeveiliging wordt gehandhaafd. Een log- en bewakingsfunctie maakt vroegtijdige preventie en detectie mogelijk en daardoor tijdige rapportage van ongebruikelijke en/of abnormale activiteiten.

#### **Waarom is dit nodig?**

Testen, inspectie en monitoring helpen je om tijdig ongebruikelijke en abnormale activiteiten te detecteren en aan te pakken.

#### **1 - Ad hoc**

1 – Ad hoc

- a) De implementatie van it-beveiliging wordt ad hoc getest.
- b) Er zijn geen procedures of beleid.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is een procedure met richtlijnen voor het testen van beveiligingsmaatregelen, maar deze focust vooral op het testen van units of componenten.



- b) Penetratietesten of social engineeringoefeningen worden adhoc uitgevoerd.
- c) Toezicht op ongebruikelijke of abnormale activiteiten vindt plaats door de logs achteraf te checken.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a) Er zijn procedures en beleid voor het scannen, testen en beheren van it-beveiliging gedefinieerd en ingevoerd. Deze zijn goedgekeurd door het schoolbestuur.
- b) Er is een beveiligingsbaseline ingevoerd voor alle it-componenten die essentieel zijn voor bedrijfsvoering.
- c) Penetratietesten en social engineeringtesten worden gepland en periodiek uitgevoerd.
- d) Er is een log- en controlefunctie ingericht voor vroegtijdige preventie en/of detectie en tijdige melding van ongewone en/of abnormale activiteiten. Er wordt extra aandacht besteed aan cybersecuritydreigingen.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Alle it-componenten, netwerkkaparaatuur, diensten en applicaties zijn geïnventariseerd. Elke component heeft een beveiligingsrisicorating gekregen en wordt volgens die rating gescand of getest.
- b) Alle it-componenten die essentieel zijn voor bedrijfsvoering worden (automatisch) opgenomen in de CMDB en realtime gecontroleerd op beveiligingsincidenten volgens de behoeften van de school.
- c) Red-teamingoefeningen worden gepland en periodiek uitgevoerd.
- d) Het proces van securitytesten, -surveillance en -monitoring wordt periodiek geëvalueerd.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a) Het testen van it-beveiliging is opgenomen in de projectmanagement- en software-ontwikkelingsmethodieken, zodat beveiliging gegarandeerd meegenomen wordt in ontwerp-, ontwikkelings- en testeisen. Zo wordt het risico dat nieuwe of veranderende systemen kwetsbaarheden introduceren zoveel mogelijk beperkt.
- b) Dreigingen op het gebied van cybersecurity worden voortdurend in de gaten gehouden door geautomatiseerde detectie- en responsetechnologie (bijvoorbeeld SIEM).

### **Aan de slag**

1. Zorg ervoor dat beveiligingsbaselines zijn ingericht. Hierover vind je meer informatie in norm SM.01 Beveiligingsbaselines.
2. Stel vast hoe vaak en op welke wijze de informatiebeveiliging getest wordt.
3. Organiseer ten minste eens per twee jaar een penetratietest binnen een kritiek systeem van de organisatie en voer (geautomatiseerde) kwetsbaarheidsanalyses uit.
4. Schakel log- en controlefuncties (zoals IDS/IPS) in op gebruikte devices, (cloud)accounts, netwerkkaparaatuur, en (cloud)software op basis van actuele dreigingen. Zorg dat meldingen opgevolgd worden. Het kan effectiever zijn om deze meldingen centraal te verzamelen en af te (laten) handelen.

### **Referentie naar andere normen en kaders**

ISO A5.25, A5.35, A5.36, A8.8, A8.15, A8.16, A8.19, A8.29, A8.34

Certificeringsschema ROSA:

Vertrouwelijkheid/Omggaan met kwetsbaarheden

## **Link naar relevante P normen**

### **SM.06 Patchmanagement**

#### **Norm**

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 het Cyber Security Incident Response Team (CSIRT) en/of leveranciers.

#### **Waarom is dit nodig?**

Als je patches of beveiligingsoplossingen niet of te laat installeert, kan dat ertoe leiden dat kwaadwillende personen bekende kwetsbaarheden misbruiken om ongeautoriseerde toegang tot de it-infrastructuur van je school te verkrijgen.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen beleid voor patchmanagement.
- b) Individuele risicoanalyse voor kwetsbaarheden en patches.
- c) Ad-hocinstallatie van patches en beveiligingsfixes.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is een informeel beleid voor patchmanagement.
- b) Risico's op kwetsbaarheden en installatie van patches en fixes worden gemanaged maar niet gedocumenteerd.
- c) Patches worden vaak ingevoerd met onvoldoende oog voor informatiebeveiliging.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er is een formeel vastgelegd beleid voor patchmanagement.
- b) Patchmanagement is op organisatieniveau ingevoerd en gedocumenteerd, in lijn met changemanagement.
- c) Patches worden in de basis overgenomen in samenwerking met CSIRT.
- d) It-medewerkers checken handmatig de patchlevels van besturingssystemen, databases en applicaties.

#### **4 - Beheerst**

4 – Beheerst

- a) De effectiviteit van patchmanagement wordt regelmatig geëvalueerd. Deze evaluaties worden gedocumenteerd en verbeteringen worden bepaald.
- b) Patchmanagement wordt meer benaderd op basis van risico's dan vanuit compliance.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Er zijn automatische controles op patchlevels en alerts voor it-medewerkers (maar geen automatische installatie van patches).
- b) Rapportages worden automatisch gegenereerd voor het schoolbestuur of de schoolleiding.

#### **Aan de slag**

1. Stel een procedure voor patchmanagement op.
2. Stel de patchmanagementprocedure vast.

3. Controleer regelmatig op patchlevels en leg dit vast.
4. Software van derden (zoals SaaS, operating system of libraries) moet actief onderhouden zijn en mag niet End-of-Support zijn.

### **Referentie naar andere normen en kaders**

ISO A8.8, A8.19

Certificeringsschema ROSA: Beschikbaarheid/Onderhoud  
Integriteit van de toepassing/Controle integriteit  
Vertrouwelijkheid/Omggaan met kwetsbaarheden

### **Link naar relevante P normen**

## **SM.07 Threat- en vulnerabilitymanagement**

### **Norm**

Er is een proces voor threat- en vulnerabilitymanagement ingevoerd om bedreigingen te identificeren en kwetsbaarheden tijdig te detecteren en te verhelpen. Het gaat hierbij om kwetsbaarheden die kunnen leiden tot een verslechtering van de prestaties van of een aanval op bedrijfsmiddelen. Welke aanvalsvectoren cybercriminelen gebruiken, wordt ook beschouwd en er worden maatregelen genomen om blootstelling te verminderen.

### **Waarom is dit nodig?**

Threat- en vulnerabilitymanagement helpt om bedreigingen en kwetsbaarheden in beeld te brengen. Zo krijg je inzicht in de manieren waarop de systemen van de school kunnen worden aangevallen.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen proces voor threat- en vulnerabilitymanagement.
- b) Er wordt niet geautomatiseerd op kwetsbaarheden gescand.
- c) Vrijwel alles wordt handmatig gedaan, systeem voor systeem.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is een eenvoudig en informeel threat- en vulnerabilitymanagementproces ingevoerd.
- b) Er is een vulnerabilityscanner, idealiter voor zowel web- als netwerkvectoren, die tevens scant op incorrecte configuratie van apparatuur.
- c) Scanning gebeurt ad hoc.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er is een formeel vastgelegd proces voor threat- en vulnerabilitymanagement ingevoerd inclusief samenwerking met CERT, gedreven vanuit compliance en bekende risico's.
- b) Er is een tool voor het beoordelen van kwetsbaarheden, waarschijnlijk gevoed met scans vanuit verschillende bronnen.

### **4 - Beheerst**

4 – Beheerst

- a) Threat- en vulnerabilitymanagement en patching zijn ingevoerd als onderdeel van een ecosysteem en niet

als losse entiteit.

- b) Er is een geavanceerd en grondig proces ingevoerd voor het valideren van kwetsbaarheden. Dit proces maakt gebruik van penetratietesten.
- c) Het red-teamconcept is ingevoerd voor formele penetratietesten.
- d) Er wordt periodiek gerapporteerd over threat- en vulnerabilitymanagement.
- e) Het threat- en vulnerabilitymanagementproces wordt periodiek geëvalueerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) De afdelingen it-beveiliging en it-operations implementeren processen om gezamenlijk de lifecycle van kwetsbaarheden te managen.
- b) Het ingevoerde proces is cruciaal voor closed-loop threat- en vulnerabilitymanagement, van bedreigingsidentificatie tot herstel en validatie.
- c) Data voor threat- en vulnerabilitymanagement is geïntegreerd met alle andere aspecten van it-beveiliging en operations, om near realtime aanpassingen in securitymanagement en netwerk- en datacentermanagement mogelijk te maken.
- d) Indicatoren richten zich op het verbeteren van beveiliging, in plaats van enkel het rapporteren van kwetsbaarheden.

### **Aan de slag**

1. Stel een procedure op voor threat- en vulnerabilitymanagement.
2. Stel een tool beschikbaar in de organisatie voor vulnerabilityscanning en zet deze regelmatig in. Leg de resultaten vast.

## **Referentie naar andere normen en kaders**

ISO A5.7, A8.7, A8.8

Certificeringsschema ROSA:

Vertrouwelijkheid/Omggaan met kwetsbaarheden

## **Link naar relevante P normen**

## **SM.08 Beschikbaarheid en bescherming infrastructuur**

### **Norm**

Interne beheers-, beveiligings- en auditmaatregelen worden ingevoerd tijdens configuratie, integratie en onderhoud van hardware en infrastructuursoftware met het doel 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 is dit nodig?**

Door de it-infrastructuur te beveiligen wordt de beschikbaarheid en integriteit gewaarborgd. Hierdoor ontstaat een digitaal veilige omgeving voor leerlingen en medewerkers.

## **1 - Ad hoc**

### **1 – Ad hoc**

- a) Er is geen proces gedefinieerd voor de bescherming en beschikbaarheid van infrastructuurcomponenten.
- b) Het belang van it-infrastructuur wordt onderkend, maar er is geen consistente totaalaanpak.
- c) Er is geen aparte testomgeving voor it-infrastructuur.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Infrastructuurbescherming en -beschikbaarheid wordt ondersteund door enkele (formele) procedures en het belang van it-infrastructuur is duidelijk.
- b) Voor enkele omgevingen is een aparte testomgeving voor it-infrastructuur.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

- e) Er is een helder gedefinieerd en door iedereen begrepen proces voor de bescherming en beschikbaarheid van de it-infrastructuur.
- f) De procesbeschrijving is in lijn met de vereisten van de school en goedgekeurd door het bestuur.
- g) De verantwoordelijkheden voor het gebruik van gevoelige componenten van de infrastructuur zijn gedefinieerd en begrepen door de ontwikkelaars van infrastructuurcomponenten en degenen die ze implementeren.
- h) Het testen betreft onder meer de functionaliteit, beveiliging, beschikbaarheid en integriteit, en eventueel andere aanbevelingen van de leverancier.
- i) Test- en productieomgevingen van de it-infrastructuur zijn van elkaar gescheiden.
- j) Alle applicatiesoftware wordt voor installatie getest in een gescheiden maar vergelijkbare omgeving van productie. De installatie van software met een licentie wordt gedaan volgens richtlijnen van de leverancier.

## **4 - Beheerst**

### **4 – Beheerst**

- a) Onderhoud van gevoelige it-infrastructuurcomponenten wordt gelogd en regelmatig geëvalueerd door verantwoordelijk management.
- b) Van alle infrastructuurdata en -software wordt een back-up gemaakt vóór het uitvoeren van installatie- of onderhoudstaken.
- c) De implementatie en uitvoering van relevante procedures worden periodiek geëvalueerd en gedocumenteerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) De bescherming en beschikbaarheid van de infrastructuur is proactief afgeleid van de eisen binnen de organisatie voor beveiliging en beschikbaarheid.
- b) De infrastructuurcomponenten worden voortdurend bewaakt door geautomatiseerde detectie- en responsetechnologie, bijvoorbeeld SIEM, als integraal onderdeel van de infrastructuur.

## **Aan de slag**

1. Beschrijf op welke wijze bescherming en beschikbaarheid van de it-infrastructuur plaatsvindt. Laat dit vaststellen door het schoolbestuur.
2. Leg voor elk onderdeel van de it-infrastructuur vast wie wijzigingen in de componenten mag en kan aanbrengen. Deze persoon zorgt ervoor dat kennis over de componenten up-to-date is. Bijvoorbeeld door het volgen van trainingen of het lezen van alle door de leverancier gepubliceerde informatie.
3. Scheid altijd test- en productieomgevingen van elkaar. Test software altijd eerst in de testomgeving voordat deze geïnstalleerd wordt op productie.
4. Pas bij installatie van software met een licentie de richtlijnen van de leverancier toe.

## **Referentie naar andere normen en kaders**

ISO A5.8, A8.14, A8.31

Certificeringsschema ROSA:  
Beschikbaarheid/Ontwerp  
Beschikbaarheid/Capaciteit Beheer  
Beschikbaarheid/Testen  
Beschikbaarheid/Scheiden omgevingen

### **Link naar relevante P normen**

## **SM.09 Onderhoud van de infrastructuur**

### **Norm**

Een strategie of plan voor het onderhoud aan de infrastructuur is ontwikkeld en borgt dat wijzigingen worden beheerd in overeenstemming met de changemanagementprocedure van de organisatie. Hieronder vallen ook periodieke beoordelingen van organisatiebehoeften, patchmanagement, upgradestrategieën, risico's, beoordeling van kwetsbaarheden en beveiligingseisen.

### **Waarom is dit nodig?**

Om risico's voor de bedrijfsvoering zoveel mogelijk te beperken, is het belangrijk dat de it-infrastructuur van je school in goede staat verkeert. Planmatig onderhoud draagt bij aan het voorkomen van verstoringen in de bedrijfsvoering van je school en daardoor dus het geven van onderwijs.

### **1 - Ad hoc**

#### **1 – Ad hoc**

- a) Er is geen proces gedefinieerd voor het onderhoud van de infrastructuur.
- b) Wijzigingen aan de infrastructuur voor nieuwe applicaties worden gedaan zonder formele strategie of totaalplan.
- c) Onderhoud wordt uitgevoerd op basis van incidenten en korte termijnplanning.

### **2 - Herhaalbaar**

#### **2 – Herhaalbaar**

- a) Er is een informeel proces voor onderhoud van infrastructuur ingevoerd.
- b) Onderhoud van it-infrastructuur is niet gebaseerd op een gedefinieerde strategie en houdt geen rekening met organisatiebehoeften.
- c) Enkele onderhoudsactiviteiten worden gepland en/of gecoördineerd.
- d) Documentatie voor essentiële systeemsoftware wordt onderhouden.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a) Er is een duidelijk, gedefinieerd en begrepen proces voor het onderhoud van de it-infrastructuur.
- b) De procesomschrijving is in lijn met changemanagement en goedgekeurd door het schoolbestuur.
- c) Het proces ondersteunt de behoeften van essentiële businessapplicaties, is in lijn met it- en businessstrategieën en wordt consequent toegepast.
- d) Onderhoud wordt gepland, ingeroosterd en gecoördineerd.
- e) De documentatie voor systeemsoftware wordt onderhouden en periodiek geactualiseerd met leveranciersdocumentatie voor alle systemen.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Het onderhoudsproces van technische infrastructuur wordt consequent toegepast op alle it-componenten en focust zich op hergebruik.
- b) Het proces is goed georganiseerd en proactief.

- c) De it-infrastructuur ondersteunt de businessapplicaties adequaat.
- d) De effectiviteit van de infrastructurele onderhoudsprocedures wordt periodiek geëvalueerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Het onderhoudsproces voor technische infrastructuur is proactief en in lijn met essentiële businessapplicaties en technische architectuur.
- b) Er wordt regelmatig onderzoek gedaan naar de relevante organisatiebehoeften, patchmanagement, upgrade-strategieën, risico's, beoordeling van kwetsbaarheden en beveiligingseisen.
- c) Er worden good practices gebruikt voor technische oplossingen, en de organisatie is op de hoogte van de nieuwste platformontwikkelingen en managementtools.
- d) Kosten worden bespaard door infrastructuurcomponenten te standaardiseren en automatisering toe te passen.

### **Aan de slag**

1. Neem het onderhoud van de it-infrastructuur op in het proces voor changemanagement. Zie voor meer informatie norm CH.01 Normen en procedures voor wijzigingen.
2. Stel een maintenanc>window op, zodat onderhoud alleen op vooraf vastgestelde momenten plaatsvindt.
3. Houd een overzicht bij van al het onderhoud en plan dit in binnen het maintenanc>window.
4. Update systeemdokumentatie na wijzigingen.

### **Referentie naar andere normen en kaders**

ISO 8.1, A7.13, A8.8, A8.32

Certificeringsschema ROSA:

Beschikbaarheid/Ontwerp

Beschikbaarheid/Onderhoud

### **Link naar relevante P normen**

## **SM.10 Cryptografisch sleutelmanagement**

### **Norm**

Er zijn beleid en procedures voor het genereren, veranderen, intrekken, vernietigen, verspreiden, certificeren, opslaan, invoeren, gebruik en de archivering van cryptografische sleutels om de sleutels te beschermen tegen aanpassing en ongeautoriseerde toegang.

### **Waarom is dit nodig?**

Cryptografie (versleuteling) wordt gebruikt om gegevens over te dragen die niet leesbaar zijn voor andere partijen. Cryptografische sleutels worden gebruikt om versleutelde gegevens weer leesbaar te maken. Zo bescherm je de vertrouwelijkheid, authenticiteit en integriteit van informatie. Goed beheer van de sleutels voorkomt dat informatie in verkeerde handen komt. Daarmee beperk je het risico op diefstal, corruptie en onjuist of ongeautoriseerd gebruik van informatie.

## **1 - Ad hoc**

### **1 – Ad hoc**

- a) Er is geen beleid of procedure voor key lifecycle management.

## **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er zijn informeel beleid en procedures voor key lifecycle management.

## **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er zijn formeel vastgelegd beleid en procedures voor key lifecycle management.
- b) Beschermende maatregelen zijn ingevoerd om informatie veilig met elkaar te kunnen delen, bijvoorbeeld door toepassing van encryptie.
- c) De vertrouwelijkheid en integriteit van private keys wordt afgedwongen.

## **4 - Beheerst**

4 – Beheerst

- a) De effectiviteit van de procedures voor cryptografisch sleutelmanagement wordt periodiek geëvalueerd.

## **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Op basis van de periodieke assessments worden de procedures voor het beheer van cryptografische sleutels geëvalueerd en verbeterd. Tekortkomingen worden gerapporteerd aan het schoolbestuur of de schoolleiding.

## **Aan de slag**

1. Maakt een schoolbestuur gebruik van cryptografische sleutels bij encryptie (of de ondertekening van documenten)? Stel dan beleid op voor sleutelmanagement en pas het toe.

## **Referentie naar andere normen en kaders**

ISO A8.24

Certificeringsschema ROSA:

Vertrouwelijkheid/Transport en fysieke opslag

## **Link naar relevante P normen**

### **SM.11 Netwerkbeveiliging**

#### **Norm**

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 is dit nodig?**

Netwerkbeveiliging helpt bij het tegengaan van bedreigingen van buitenaf. Als je beveiligingstechnieken toepast met gebruik van best practices, verklein je het risico op diefstal, corruptie en onjuist of ongeautoriseerd gebruik van informatie.

## **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen netwerkbeveiligingsbeleid.



- b) Er zijn geen procedures of richtlijnen.
- c) Ad-hocrisicoanalyse en het gebruik van maatregelen door individuen.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er is een informeel netwerkbeveiligingsbeleid.
- b) Er worden procedures voor implementatie van netwerkbeveiliging gevolgd, maar deze zijn niet formeel vastgesteld.
- c) Best practices worden gebruikt, maar niet op een gestructureerde manier.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

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

## **4 - Beheerst**

### **4 – Beheerst**

- a) De relevante procedures worden periodiek geëvalueerd op actualiteit en uitvoering. De uitkomsten hiervan worden gedocumenteerd.
- b) Op basis van deze evaluaties worden verbeteringen doorgevoerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Op basis van het periodieke assessment worden de procedures geëvalueerd en verbeterd. Tekortkomingen worden gerapporteerd aan het schoolbestuur of de schoolleiding.

## **Aan de slag**

1. Stel vast welk beleid, procedures en richtlijnen voor de organisatie van toepassing zijn. Leg dit vast in de beveiligingsbaselines. Zie voor meer informatie norm SM.01 Beveiligingsbaselines.
2. Zorg dat er bij transport van gevoelige data zoals grote hoeveelheden persoonsgegevens over een niet-vertrouwd netwerk versleuteling plaatsvindt.
3. Pas netwerksegmentatie toe om verspreiding van malware en virussen te kunnen beperken.

## **Referentie naar andere normen en kaders**

ISO A8.20, A8.21, A8.22

Certificeringsschema ROSA:

Beschikbaarheid/Capaciteit Beheer

Vertrouwelijkheid/Netwerk toegang

Vertrouwelijkheid/Transport en fysieke opslag

## **Link naar relevante P normen**

### **SM.12 Beheersing van malware-aanvallen**

#### **Norm**

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

#### **Waarom is dit nodig?**

Door de juiste maatregelen tegen malware te treffen beperk je het risico hierop. Mocht er toch een inbreuk plaatsvinden? Dan verminder je met een goede beheersing de gevolgschade.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen beleid voor het voorkomen van malware.
- b) Er is geen (volledig) geautomatiseerde anti-malwaresoftware.
- c) Er zijn geen (volledig) up-to-date virusdefinities.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is anti-malwarebeleid, maar dit is niet formeel vastgelegd.
- b) Er is antivirussoftware in gebruik.
- c) De virusdefinities zijn up-to-date.
- d) De meeste inkomende e-mails worden gefilterd op malware.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

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

#### **4 - Beheerst**

4 – Beheerst

- a) De effectiviteit van het distributieproces, de gebruikelijke evaluatie van nieuwe bedreigingen en het filteren van de e-mails wordt periodiek geëvalueerd.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) De periodieke assessments worden gebruikt om het beheersen van malwareaanvallen te evalueren en te verbeteren.
- b) Tekortkomingen worden aan het schoolbestuur of de schoolleiding gerapporteerd.

## **Aan de slag**

1. Neem in de beveiligingsbaselines op welke anti-malwaremaatregelen technisch genomen worden. Zie voor meer informatie over beveiligingsbaselines norm SM.01 Beveiligingsbaselines.
2. Neem in de activiteiten voor bewustwording rondom informatiebeveiliging van medewerkers én leerlingen malware expliciet op.
3. Scan en filter e-mail - zowel inkomend als uitgaand - op spam en malware.

## **Referentie naar andere normen en kaders**

ISO A8.1, A8.7, A8.12, A8.19, A8.26

Certificeringsschema ROSA:

Integriteit van de toepassing/Controle integriteit

## **Link naar relevante P normen**

### **SM.13 Bescherming van beveiligingstechnologie**

#### **Norm**

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

#### **Waarom is dit nodig?**

Door technologie bestand te maken tegen manipulatie en documenten hierover niet openbaar te maken, maak je het kwaadwillenden moeilijker om systemen te compromitteren.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er zijn geen specifieke maatregelen getroffen om aan beveiliging gerelateerde technologie te beschermen.
- b) Reguliere documentatie en beveiligingsdocumentatie worden op dezelfde manier opgeslagen.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er zijn beleid en procedures opgesteld om de gevolgen van een inbreuk in de beveiliging te beperken. Deze bevatten specifiek beheersmaatregelen voor configuratiemanagement, applicatietoegang, databeveiliging en fysieke beveiligingseisen.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Beveiligingsfuncties zijn ontworpen om wachtwoordregels te ondersteunen, zoals minimumlengte, soort karakters, geldigheidsduur en voorkomen van hergebruik.
- b) Toegang is geautoriseerd en op de juiste wijze goedgekeurd.

#### **4 - Beheerst**

4 – Beheerst

- a) Het toekennen en goedkeuren van toegang, mislukte toegangspogingen, geblokkeerde toegang en geautoriseerde toegang tot gevoelige bestanden of data worden geregistreerd.

## 5 - Continu verbeteren

### 5 – Continu verbeteren

- a) Veiligheidsrapportage wordt door het systeem gegenereerd en gebruikt om (kwaadaardig) binnendringen via kwetsbaarheden van het netwerk te voorkomen.
- b) De maatregelen zijn onderdeel van een jaarlijkse managementreview van veiligheidsvoorzieningen voor fysieke en logische toegang tot bestanden en data.

### Aan de slag

1. Pas alle beveiligingsmaatregelen die er zijn voor andere applicaties ook toe op technologie die beveiliging moet borgen. Zo wordt inbreuk op beveiligingstechnologie zo moeilijk mogelijk gemaakt.
2. Maak documentatie over beveiliging niet openbaar. Pas bij opslag en verzenden van deze documentatie de maatregelen toe die gelden bij een hoog vertrouwelijke classificatie.

### Referentie naar andere normen en kaders

ISO A5.15, A5.25, A5.26, A5.28, A5.36, A6.8, A7.2, A7.7, A7.8, A7.12, A8.2, A8.5, A8.8, A8.15, A8.17, A8.18, A8.19, A8.20, A8.21

### Link naar relevante P normen

## 12. Fysieke beveiliging

Bij fysieke beveiliging gaat het om de maatregelen om een pand of specifieke ruimten daarbinnen te beschermen. Ondanks het open karakter van een school, wil je bepaalde ruimtes toch extra beveiligen. Denk hierbij aan ruimtes waarin nog fysieke dossiers staan met gegevens van medewerkers of (oud-)leerlingen. Of de serverruimte die belangrijk is om te beschermen voor de continuïteit van werkprocessen. Dit zijn redenen om maatregelen te nemen. Soms kan een goed slot op de deur al zo'n beheersmaatregel zijn.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Hoofd facilitair, schoolleider

Geraadpleegd: It-verantwoordelijke, managers, adviseur informatiebeveiliging

Geïnformeerd: Medewerkers van de school

## PH.01 Fysieke beveiligingsmaatregelen

### Norm

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

### Waarom is dit nodig?

Door toegang tot ruimten met gevoelige informatie of it-gerelateerde componenten binnen de scholen te autoriseren, registreren en monitoren zorg je ervoor dat onbevoegden geen toegang krijgen tot deze informatie en componenten. Maar ook andere beveiligingsrisico's zoals brand, waterschade en stroomuitval wil je zoveel mogelijk beperken. Mocht het toch voorkomen? Dan moet je voorbereid zijn. Door maatregelen te treffen,

voorkom je dat de integriteit en beschikbaarheid van it-componenten en gegevens in gevaar komen en zorg je er in geval van calamiteiten voor dat je snel kunt schakelen.

## **1 - Ad hoc**

1 – Ad hoc

- a) Er wordt geen fysiek beveiligingsbeleid gehanteerd.
- b) De organisatie kan niet snel diefstal of aanvallen op gebouwen en apparatuur detecteren.
- c) Het beheer van faciliteiten en apparatuur is afhankelijk van de bekwaamheid van enkele individuen.

## **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er zijn beleidskaders voor fysieke beveiliging, maar deze zijn niet volledig en worden niet consequent gehanteerd. Overtreding van regels wordt niet opgemerkt.
- b) Fysieke beveiliging is een informeel proces en standaarden worden niet consequent toegepast binnen de organisatie.

## **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er is een alomvattend op risico's gebaseerd beleid inzake fysieke beveiliging. Dat beleid is gedocumenteerd, gecommuniceerd en wordt ondersteund door (toegangs)systemen voor de bescherming en ondersteuning van medewerkers, leerlingen, leveranciers, bezoekers, et cetera. Het beleid is ook voor incidentrespons en -rapportage.
- b) Het beleid is goedgekeurd door het schoolbestuur of de schoolleiding.
- c) Er zijn effectieve maatregelen genomen om bedreigingen en ongeautoriseerde toegang tot terrein en gebouwen en diefstal van apparatuur te voorkomen, te detecteren en tegen te houden.
- d) 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.
- e) Verantwoordelijkheden en eigenaarschap zijn duidelijk vastgesteld.

## **4 - Beheerst**

4 – Beheerst

- a) Het fysieke beveiligingsbeleid behandelt ook de veiligheid en bescherming van medewerkers en apparatuur wanneer deze niet op locatie zijn. Het beleid schrijft ook voor dat het management toezicht houdt op de effectiviteit van de beheersmaatregelen en het voldoen aan standaarden, en dat er in het risicomanagementproces rekening gehouden wordt met de mogelijkheid tot herstel van faciliteiten en apparatuur.
- b) Voor alle faciliteiten is bepaald welke standaarden van toepassing zijn. Dit betreft onder meer terreinkeuze, bouw, bewaking, veiligheid van medewerkers, mechanica, elektronica en bescherming tegen omgevingsfactoren (zoals brand, blikseminslag en overstroming)
- c) Het voldoen aan het beleid wordt op ad-hocbasis geëvalueerd (door de second line of defense).

## **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Er is een goedgekeurde langetermijnplanning voor de faciliteiten die essentieel zijn voor de ondersteuning van het terrein en de it-omgeving, gebaseerd op het beleid.
- b) Alle faciliteiten zijn geïnventariseerd en geclassificeerd volgens het informatierisicomanagementproces.
- c) Het al dan niet voldoen aan het beveiligingsbeleid wordt periodiek gerapporteerd aan het schoolbestuur of de schoolleiding.
- d) Het beleid wordt jaarlijks geëvalueerd, geactualiseerd en opnieuw goedgekeurd door het schoolbestuur.

## **Aan de slag**

1. Maak fysieke beveiliging onderdeel van het IBP-beleid. Zie voor meer informatie over het opstellen van IBP-beleid norm GO.02 Beleid informatiebeveiliging.
2. Bepaal op basis van een risicoanalyse welke maatregelen genomen moeten worden. Herhaal deze risicoanalyse ten minste elke drie jaar.
3. Maak je gebruik van cameratoezicht? Pas dan de handreiking Cameratoezicht en het modelreglement Cameratoezicht toe.
4. Rapporteer periodiek aan het schoolbestuur over de status van de maatregelen.
5. Neem bij verhuizing of verbouwing de fysieke beveiliging mee in het ontwerp op basis van een risicoanalyse.

## **Referentie naar andere normen en kaders**

ISO A7.1, A7.2, A7.3, A7.4, A7.5, A7.8, A7.9, A7.11, A7.12

Certificeringsschema ROSA:  
Vertrouwelijkheid/Fysieke toegang

## **Link naar relevante P normen**

### **PH.02 Beheer van fysieke toegangsrechten**

#### **Norm**

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

#### **Waarom is dit nodig?**

Medewerkers moeten voor het vervullen van hun functie toegang hebben tot bepaalde ruimtes in de school. Hiervoor geef je toegangsrechten uit. Als medewerkers een andere functie krijgen of de school verlaten, trek je die toegangsrechten in. Dit hou je bij in een overzichtelijke administratie. Zo houd je grip op wie wel toegang heeft tot ruimtes met gevoelige informatie en it-componenten en wie niet. Op deze manier houd je de beveiliging hiervan op orde.

#### **1 - Ad hoc**

##### **1 – Ad hoc**

- a) Er zijn geen procedures vastgelegd voor de administratie van fysieke toegang.
- b) Medewerkers hebben onbeperkt fysieke toegang tot het terrein, de gebouwen en de ruimtes van de organisatie.
- c) Andere procedures voor beheer en bescherming van fysieke it-eigendommen zijn niet of nauwelijks vastgelegd.

#### **2 - Herhaalbaar**

##### **2 – Herhaalbaar**

- a) Er zijn informele procedures om toegang tot specifieke ruimtes te beperken.
- b) Fysieke beveiligingsdoelen zijn niet gebaseerd op formele standaarden of organisatiedoelen.
- c) Onderhoudsprocedures voor de faciliteiten worden niet (goed) vastgelegd en hangen vooral af van de good practices van enkele individuen.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a) Er worden formeel vastgelegde procedures voor de administratie van fysieke toegang toegepast.
- b) Er worden beveiligingsmaatregelen en toegangsbeperkingen toegepast zodat alleen geautoriseerde medewerkers fysieke toegang heeft tot gebouwen, it-kritieke omgevingen of datacenters.
- c) Toegang tot fysieke it-omgevingen (serverruimtes) wordt verleend op basis van functie en verantwoordelijkheden.
- d) Er zijn procedures om de toegangsprofielen up-to-date te houden.
- e) Er is een proces ingevoerd om alle toegangen tot fysieke it-omgevingen te controleren en te bewaken, waarbij alle bezoekers, inclusief leveranciers en onderhoudsmedewerkers, worden geregistreerd.
- f) Verantwoordelijkheden en eigenaarschap zijn duidelijk toegewezen en gecommuniceerd.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Daadwerkelijke toegang en overtredingen van het toegangsbeleid wordt streng gecontroleerd en periodiek bekeken.
- b) Gestandaardiseerde technieken worden toegepast om omgevings- en veiligheidsfactoren voor fysieke beveiliging aan te pakken.
- c) Het management onderzoekt periodiek de doeltreffendheid van de autorisaties en het gebruik van de toe te passen standaarden.
- d) Het management heeft doelen en metrics vastgesteld voor het beheer van fysieke it-omgevingen.
- e) De operationele effectiviteit van de fysieke beveiligingsprocedures wordt periodiek geëvalueerd.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a) Toegangsbeheer wordt voortdurend gecontroleerd.
- b) De omgeving wordt beheerd en bewaakt door gespecialiseerde apparatuur en hardwareruimtes worden op afstand beheerd.
- c) Er worden preventief onderhoudsprogramma's uitgevoerd volgens strikte tijdschema's en gevoelige apparatuur wordt regelmatig getest en gecontroleerd.
- d) Strategieën en standaarden voor faciliteiten zijn volgens it-beschikbaarheidsdoelen en geïntegreerd in continuïteitsplanning en crisismanagement.
- e) De fysieke beveiligingsfaciliteiten worden door het management geëvalueerd en geoptimaliseerd op basis van de vastgestelde doelen en metrics.

### **Aan de slag**

1. Zorg er voor dat kritieke it-ruimtes toegangsbeperkende maatregelen hebben. Maak bij voorkeur gebruik van een toegangssysteem (met pas) en niet alleen van een sleutel.
2. Bepaal met een risicoanalyse welke andere fysieke maatregelen noodzakelijk zijn, zoals een alarmsysteem in de nacht.
3. Maak een overzicht waarin is vastgelegd welke rol/functie toegang krijgt tot kritieke it-ruimtes of datacenters en waarom.
4. Leg de toekenning van nieuwe toegangsrechten schriftelijk vast.
5. Leg vast wie toegang heeft gehad tot kritieke it-ruimtes. Dit kan ook door middel van een toegangssysteem.

## Referentie naar andere normen en kaders

ISO A7.2, A7.6, A7.8, A7.9

Certificeringsschema ROSA:  
Vertrouwelijkheid/Fysieke toegang

## Link naar relevante P normen

# 13. It-operatie

De onderwerpen binnen het domein it-operatie gaan over drie standaard it-beheeractiviteiten, jobprocessing, backup en herstel en capacity- en performancemanagement. In welke mate deze voor jouw school van toepassing zijn, is afhankelijk van welke it-taken de school zelf uitvoert en welke zijn uitbesteed. Je kunt hierbij denken aan het maken van back-ups, het hebben van herstelprocedures en het zorgen voor voldoende servercapaciteit. Dit alles om het geven van onderwijs te garanderen.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur  
Verantwoordelijk voor uitvoering: It-verantwoordelijke, it-leverancier  
Geraadpleegd: Adviseur informatiebeveiliging  
Geïnformeerd: Medewerkers van de school

## OP.01 Jobprocessing

### Norm

De organisatie heeft procedures voor geautomatiseerde jobprocessing. Taakactiviteiten worden gecontroleerd en omvatten het gebruik van interfaces tussen relevante systemen om te bevestigen dat de datatransmissies volledig, nauwkeurig en geldig zijn. En 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 is dit nodig?

Jobprocessing procedures zorgen ervoor dat controle van de automatische activiteiten, zoals back-ups of dagelijkse gegevensuitwisselingen, plaatsvindt en storingen tijdig geïdentificeerd en opgelost kunnen worden. Zo weet je dat als je bij een incident moet terugvallen op een back-up, de informatie op die back-up zo volledig en actueel mogelijk is.

### 1 - Ad hoc

1 – Ad hoc

a) Er zijn geen procedures vastgesteld voor jobprocessing.

### 2 - Herhaalbaar

2 – Herhaalbaar

- a) Er zijn verschillende runbooks voor productietaken beschikbaar en deze beschrijven in het algemeen taken en interfaces voor de meest relevante systemen.
- b) Jobprocessing wordt lokaal (per afdeling) ingevoerd en er is geen correlatie tussen verschillende systemen.
- c) Afwijkingen in (back-up) jobscheduling worden niet centraal geregistreerd (via incidentmanagement).



### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a. Een runbook voor jobscheduling is beschikbaar en afgestemd op de doelstellingen van de school (overeenkomen door systeem- of proceseigenaar).
- b. Het runbook bevat gedetailleerde informatie en instructies.
- c. Jobprocessing en interfacebewaking worden centraal ingevoerd en beheerd, inclusief de correlatie tussen verschillende systemen.
- d. Uitzonderingen of afwijkingen in de jobprocessing worden geregistreerd via het incidentmanagementproces.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Rapportage over jobprocessing maakt deel uit van de rapportage over het servicelevel.
- b) De operationele effectiviteit van jobprocessing wordt periodiek geëvalueerd.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a) Speciale tooling wordt gebruikt om de jobprocessing en de opvolging van daaraan gerelateerde afwijkingen te automatiseren (bijvoorbeeld automatische herstart), afhankelijk van hoe belangrijk de taken zijn.

### **Aan de slag**

- 1. Maak je gebruik van applicaties die data uitwisselen? Maak je zelf back-ups van systemen en heb je dat dus niet bij een leverancier belegd? Zorg dan voor een runbook voor jobscheduling. Hierin staat beschreven welke taak op welke wijze wordt uitgevoerd en wat er gebeurt bij afwijkingen.

### **Referentie naar andere normen en kaders**

ISO A5.37

### **Link naar relevante P normen**

## **OP.02 Procedures voor back-up en herstel**

### **Norm**

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

### **Waarom is dit nodig?**

Als je een strategie hebt voor back-up en herstel en daar procedures opricht en regelmatig test, verminder je daarmee het risico om bij een incident meer data te verliezen dan acceptabel is voor je organisatie. Tegelijk verlaag je de kosten van herstel.

### **1 - Ad hoc**

#### **1 – Ad hoc**

- a) Er zijn geen procedures voor back-up en herstel.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a. Er zijn procedures voor back-up en herstel van systemen, applicaties, data en documentatie.
- b. Het back-upschema en de retentie-eisen zijn niet (volledig) in lijn met de eisen van de organisatie.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

- a) 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.
- b) Beleid en procedures zijn in lijn met organisatiebehoeften en goedgekeurd door het schoolbestuur of de schoolleiding.
- c) De verantwoordelijkheden voor het maken, herstellen en bewaken van back-ups zijn duidelijk toegewezen.
- d) De prioriteit voor dataherstel is gebaseerd op eisen die de organisatie heeft bepaald en procedures voor de continuïteit van it-diensten.

## **4 - Beheerst**

### **4 – Beheerst**

- a) Door middel van het risicomanagementmodel en it-servicecontinuïteitsplan wordt periodiek bepaald welke data essentieel is voor de organisatie.
- b) Er worden periodiek voldoende hersteltesten uitgevoerd om te garanderen dat alle componenten van back-ups effectief en correct hersteld kunnen worden.
- c) De operationele effectiviteit van back-up- en herstelprocedures worden periodiek geëvalueerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) De performance van het back-up- en herstelproces wordt periodiek aan het schoolbestuur of de schoolleiding gerapporteerd en indien nodig worden verbeteringen voorgesteld.
- b) De procedures zijn een belangrijk onderdeel van de disasterrecoveryplanning van de organisatie.
- c) Systemen, applicaties, gegevens en documentatie die door derden worden onderhouden of verwerkt, worden adequaat geback-up of anderszins beveiligd.
- d) Teruggave van back-ups door derden is verplicht en escrow- of deponeringsregelingen worden overwogen.

## **Aan de slag**

1. Bepaal voor alle systemen, applicaties en dataverwerkingen welke eisen er zijn voor back-up- en herstelprocedures. Leg dit vast in een beleidsdocument en in procedures die voldoen aan de eisen.
2. Zorg dat het schoolbestuur of de schoolleiding het beleid en de bijbehorende procedures vaststelt.
3. Neem dataherstel op in het bedrijfscontinuïteitsplan. Zie voor meer informatie norm BC.01 Bedrijfscontinuïteitsplanning.

## **Referentie naar andere normen en kaders**

ISO A8.13, A8.16

Certificeringsschema ROSA:

Beschikbaarheid/Herstel

Integriteit van de gegevens/Backup

## **Link naar relevante P normen**

### **OP.03 Capacity- en performancemanagement**

#### **Norm**

De organisatie heeft procedures ingevoerd 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- en performancemanagement houdt rekening met alle middelen die nodig zijn om de it-service te leveren en met plannen voor korte, middellange en lange termijn businessrequirements, inclusief het voorspellen van toekomstige behoeften op basis van eisen voor werkbelasting, opslag en onvoorziene gebeurtenissen.

#### **Waarom is dit nodig?**

Om aan de behoeften van medewerkers en leerlingen te kunnen blijven voldoen op het gebied van it-capaciteit, is het belangrijk om op deze behoeften te anticiperen. Dat kun je doen door de capaciteit van it-services daarop af te stemmen, bijvoorbeeld op het gebied van bandbreedte of opslagruimte. Capacity- en performancemanagement is van belang om de capaciteit en prestaties van de it-services te monitoren en te beoordelen, zodat je tijdig kunt ingrijpen als je de systemen moet uitbreiden of verbeteren.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen capacity- en performancemanagement ingevoerd.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is een proces en technologie ingevoerd om relatief eenvoudige tracking en handmatige rapportage van raw performance metrics op serverniveau te bewerkstelligen.
- b) Rapportage is handmatig en ad hoc (vooral op basis van incidenten).

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er is een proces en technologie gedefinieerd en ingevoerd om samenhangende tracking en geautomatiseerde rapportage van raw performance metrics op server- of partitionniveau te bewerkstelligen.
- b) 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.

#### **4 - Beheerst**

4 – Beheerst

- a. Er is een proces en technologie voor volledig geautomatiseerde tracking, analyse en rapportage van metrics, sterk gerelateerd aan services van de school.
- b. Naast gegevens over de werkbelasting van systemen en applicaties wordt rekening gehouden met prestatie- en capaciteitsmetrics die sterk samenhangen met business- of servicemetrics (bijvoorbeeld configuratie, kosten, responstijden, enzovoort).
- c. Er vindt periodiek geautomatiseerde, op uitzondering georiënteerde analyse en rapportage plaats.
- d. Het voorspellen van toekomstige behoeften wordt gedaan op basis van periodieke rapportage.
- e. Operationele effectiviteit van de capacity- en performancemanagementprocessen wordt periodiek geëvalueerd.

## 5 - Continu verbeteren

### 5 – Continu verbeteren

a) Belangrijke onderdelen van de infrastructuur en het applicatielandschap worden geanalyseerd om toekomstige behoeften te voorspellen. Dit wordt gestructureerd uitgevoerd om prestatie- en continuïteitsplanning te ondersteunen.

#### Aan de slag

1. Beheer je it in huis? Monitor dan actief of er voldoende capaciteit beschikbaar is in de vorm van bijvoorbeeld servercapaciteit of opslagcapaciteit. Monitor ook of de performance van de it voldoet.
2. Onderneem actie bij afwijkingen.

#### Referentie naar andere normen en kaders

ISO A8.6, A8.14

Certificeringsschema ROSA:

Beschikbaarheid/Capaciteit Beheer

Beschikbaarheid/Testen

Beschikbaarheid/Monitoring

#### Link naar relevante P normen

## 14. Bedrijfscontinuïteits-management

Bedrijfscontinuïteitsmanagement gaat over het voorbereid zijn op grote verstoringen. In het onderwijs betekent dit dat bekeken moet worden welke zaken nodig zijn om het primaire proces – het verzorgen van onderwijs – door te kunnen laten gaan. Daarnaast moet je in kaart brengen welke grote calamiteiten denkbaar zijn. Zo bestaat er voor elke school een risico op een ransomwareaanval, maar hoeft niet elke school rekening te houden met het gevaar van een overstroming of ontsporing van een chloortrein. Op basis van deze informatie kun je bepalen hoe continuïteits- en herstelplannen van je school eruit moeten zien.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Hoofd bedrijfsvoering, IBP-verantwoordelijke, risicomanager, it-verantwoordelijke

Geraadpleegd: Management, adviseur informatiebeveiliging

Geïnformeerd: Medewerkers van de school

### BC.01 Bedrijfscontinuïteitsplanning

#### Norm

Business- en it-continuïteitsplannen dienen ontworpen te zijn 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 en alternatieve verwerkings- en herstelmogelijkheden in alle kritieke it-services. De plannen omvatten ook gebruiksrichtlijnen, rollen en verantwoordelijkheden, procedures, communicatieprocessen en de testmethode.

#### Waarom is dit nodig?

Bedrijfs- en it-continuïteitsplannen geven je kaders om tijdens een grote storing de juiste dingen te doen. Ze helpen je om adequaat te handelen, zodat je de gevolgen van de storing beperkt kunt houden. Het is dus belangrijk om deze plannen te hebben.

## **1 - Ad hoc**

### **1 – Ad hoc**

- a) Er is geen bedrijfsgericht it-continuïteitsplan.
- b) De it-organisatie heeft een beperkt en algemeen herstelplan voor het netwerk en de systemen.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) It- (en uiteindelijk bedrijfs)continuïteitsplannen worden ontwikkeld op basis van een informeel (en beknopt) framework. Deze plannen zijn niet compleet en gebaseerd op een risico gerelateerd begrip van potentiële bedrijfseffecten.
- b) In het geval van een grote onderbreking kunnen betrokken belangrijke processen en systemen wellicht worden hersteld, maar herstelactiviteiten zullen waarschijnlijk ontoereikend zijn.
- c) Als kritieke programma's en data verloren gaat en/of belangrijke medewerkers vertrekken, kunnen belangrijke businessprocessen gedurende een langere periode niet uitgevoerd worden.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

- a) Bedrijfs- en it-continuïteitsplannen zijn gedefinieerd, geïntegreerd en goedgekeurd door het schoolbestuur of de schoolleiding.
- b) De organisatie heeft een bedrijfsimpactanalyse uitgevoerd, op basis waarvan recoverytimedoelen zijn bepaald en volledig gedocumenteerde it-herstelplannen en bedrijfs- continuïteitsplannen zijn opgesteld om deze doelen te bereiken.
- c) De plannen betreffen gebruikershandleidingen, rollen, verantwoordelijkheden, crisismanagement, communicatieprocessen en de testmethode.
- d) Dankzij deze plannen kan de organisatie waarschijnlijk belangrijke operationele processen voortzetten in het geval van een grote onderbreking.

## **4 - Beheerst**

### **4 – Beheerst**

- a) De continuïteitsplannen bevatten een roulerend schema van tabletop en live simulatietesten van de continuïteits- en crisismanagementplannen, waarin verbeteringen zijn doorgevoerd op basis van de resultaten van eerdere tests.
- b) Tekortkomingen bij de uitvoering van bedrijfscontinuïteitsplannen worden gerapporteerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) Bedrijfscontinuïteitsplannen en gerelateerde processen worden periodiek geëvalueerd.
- b) Zowel tekortkomingen in (de effectiviteit of efficiëntie van) de continuïteitsplannen als verbeteringen worden gerapporteerd aan het schoolbestuur of schoolleiding.

## **Aan de slag**

1. Stel een bedrijfscontinuïteitsplan op en laat het vaststellen door het schoolbestuur.
2. Maak gebruik van de handreiking Bedrijfscontinuïteitsmanagement (BCM). Hierin staat een praktische aanpak voor BCM beschreven. Je kunt hierbij denken aan het uitvoeren van een bedrijfsimpactanalyse (BIA) of het bepalen van herstelstrategie en -aanpak. Hierbij kun je gebruikmaken van het template Bedrijfscontinuïteitsplan. Dan geef je invulling aan alle aspecten van de norm.

## **Referentie naar andere normen en kaders**

ISO A5.5, A5.6, A5.29, A5.30

Certificeringsschema ROSA:  
Beschikbaarheid/Herstel

## **Link naar relevante P normen**

### **BC.02 Testen van disaster recovery**

#### **Norm**

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

#### **Waarom is dit nodig?**

Als je de bedrijfs- en it-continuïteitsplannen test, kom je erachter of ze voldoen of dat ze tekortschieten. Indien nodig kun je de plannen dan verbeteren. Test je de plannen niet, dan loop je het gevaar dat ze niet werken op het moment dat je ze nodig hebt.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Het testen van it-continuïteitsplannen wordt niet of ad hoc uitgevoerd.
- b) Er is een geïsoleerde testbenadering voor sommige kritieke applicaties en enkele eenvoudige hersteltests voor infrastructuurcomponenten.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Het it-continuïteitsplan wordt regelmatig getest (eenmaal per jaar).
- b) Er is een beperkte consolidatie van individuele hersteltestmethoden voor kritieke toepassingen. Het testen gebeurt meestal via geïsoleerde testen op individuele applicaties en onderliggende infrastructuur.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Bedrijfs- en it-continuïteitsplannen worden getest via goedgekeurde, geïntegreerde test-/herstelscenario's.
- b) 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.
- c) Er is voorzien in een gedegen voorbereiding, documentatie, rapportage van de testresultaten en, afhankelijk van de resultaten, uitvoering van een actieplan.

#### **4 - Beheerst**

4 – Beheerst

- a) Geïntegreerde bedrijfscontinuïteitstests worden uitgevoerd voor het volledige bedrijfskritische applicatie- en infrastructuurlandschap. Dat wil zeggen een volledige failovertest inclusief het herstel van bedrijfsspecifieke activiteiten en werkplekken.
- b) Bewezen hersteltools zijn aanwezig voor alle applicaties, en infrastructuurcomponenten, applicaties en services voor alle lagen zijn ondergebracht.

- c) Er zijn succesvolle tests op meerdere niveaus voor applicaties en infrastructuurcomponenten.
- d) De testplannen voor bedrijfs- en it-continuïteit worden periodiek herzien.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) De organisatie slaagt standaard voor haar BC/DR-tests zonder grote tekortkomingen of uitzonderingen omdat haar procedures en capaciteiten over de duur van een paar jaar zijn gefinetuned.
- b) Periodieke rapporten over de geteste effectiviteit van de continuïteitsplannen worden naar het schoolbestuur of de schoolleiding gestuurd.

### **Aan de slag**

1. Test voor kritische applicaties periodiek of de continuïteitsplannen werken.
2. Documenteer de tests zorgvuldig, zodat de resultaten waar nodig leiden tot verbeteracties.

## **Referentie naar andere normen en kaders**

ISO A5.29, A5.30

Certificeringsschema ROSA:  
Beschikbaarheid/Herstel

## **Link naar relevante P normen**

### **BC.03 Offsite back-upopslag**

#### **Norm**

Alle kritieke back-upmedia, documentatie en andere it-resources die nodig zijn in het kader van it-herstellen en bedrijfscontinuïteitsplannen worden offsite opgeslagen. De inhoud van back-upopslag wordt bepaald in samenspraak met de eigenaren van bedrijfsprocessen en it-medewerkers. 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 gearcheeerde gegevens is gewaarborgd en gearcheeerde gegevens worden periodiek getest en verversd.

#### **Waarom is dit nodig?**

Back-ups en andere it-resources die op een andere locatie dan de school zijn opgeslagen kun je inzetten op het moment dat de it-infrastructuur van de school fysiek beschadigd is.

### **1 - Ad hoc**

#### **1 – Ad hoc**

- a) Back-upmedia worden niet, of slechts gedeeltelijk, offsite opgeslagen.
- b) Er worden geen extra maatregelen genomen om verlies van data te voorkomen in geval van nood bij het primaire datacenter.

### **2 - Herhaalbaar**

#### **2 – Herhaalbaar**

- a. De organisatie heeft een beknopte inventarisatie gedaan van kritieke media die offsite opgeslagen moeten worden.

- b. De inhoud van back-ups wordt bepaald in onderling overleg tussen proceseigenaren en it-medewerkers.
- c. Er zijn maatregelen genomen om offsite back-upopslag van kritieke media te garanderen.

### **3 - Bepaald (streefniveau)**

#### **3 – Bepaald**

- a. Er is een gedetailleerd overzicht van alle kritieke back-upmedia die offsite opgeslagen dienen te worden. Het overzicht is vastgesteld door het schoolbestuur of de schoolleiding.
- b. Aan het management worden duidelijke beschrijvingen van de noodzakelijke dataopslagbeheersmaatregelen gegeven over de offsite opslagfaciliteit, inclusief transport, herstelinstructies, labels en voorraadlijsten van back-upmedia.
- c. De offsiteregeling is in lijn met de vereisten voor bedrijfscontinuïteit en wordt periodiek geëvalueerd.

### **4 - Beheerst**

#### **4 – Beheerst**

- a) Het beheer van de offsiteopslagfaciliteiten handelt op basis van dataclassificatiebeleid en de procedures voor mediaopslag van de organisatie.
- b) Het it-management evalueert periodiek de offsitefaciliteiten, in het bijzonder inhoud, beveiliging en bescherming tegen omgevingsfactoren.
- c) Back-updata wordt regelmatig getest en hersteld om de kwaliteit van de data te waarborgen.
- d) De compatibiliteit van hardware en software betrokken bij het herstel van gearhiveerde data wordt periodiek getest.

### **5 - Continu verbeteren**

#### **5 – Continu verbeteren**

- a. De offsitefaciliteiten worden voortdurend verbeterd.
- b. Mirroring van kritieke media door middel van cloudoplossingen wordt toegepast wanneer realtime back-ups van kritieke media nodig zijn.

### **Aan de slag**

1. Stel op basis van de continuïteitseisen vast welke back-ups hoe vaak gemaakt moeten worden en welke daarvan op een andere locatie opgeslagen moeten worden. Leg dit overzicht voor aan het schoolbestuur en stel het vast.
2. Maak duidelijke afspraken over de manier waarop de data worden opgeslagen.
3. Bekijk jaarlijks of de off-site backup nog passend is bij de eisen van de organisatie.

### **Referentie naar andere normen en kaders**

ISO A8.13

Certificeringsschema ROSA:  
Integriteit van de gegevens/Backup

### **Link naar relevante P normen**

## **BC.04 Datareplicatie**

### **Norm**

Datareplicatie is opgezet tussen de productiefaciliteit van de organisatie en de disasterrecoveryfaciliteit, zodat kritieke financiële en operationele gegevens op korte termijn beschikbaar zijn. Replicatiestatus wordt gemonitord als onderdeel van het bewakingsproces voor systeemtaken.



## **Waarom is dit nodig?**

Als je datareplicatie goed hebt georganiseerd, heb je tijdens een incident gegevens tijdig beschikbaar.

### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen mogelijkheid tot datareplicatie.

### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) In geval van nood kan er datareplicatie plaatsvinden door middel van (extern opgeslagen) back-ups.
- b) De organisatie accepteert het verlies van data tussen de laatste back-up en het moment van het incident.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er is een datareplicatieproces ingevoerd in de faciliteiten voor productie- en disasterrecovery van de organisatie.
- b) De organisatie heeft inzicht in welke financiële en operationele data essentieel zijn en dus gerepliceerd moeten worden. Dit is goedgekeurd door het schoolbestuur of de schoolleiding.
- c) In het geval van een incident zijn data op korte termijn beschikbaar.

### **4 - Beheerst**

4 – Beheerst

- a) Er wordt toegezien op de status van replicatie, als onderdeel van het systemjobsmonitoringproces.
- b) De kwaliteit van datareplicatie wordt minstens jaarlijks (gedeeltelijk) getoetst.

### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Er vinden wekelijks geautomatiseerde gedeeltelijke datareplicatietesten plaats.
- b) Volledig herstel door middel van gerepliceerde data is een integraal onderdeel van jaarlijkse calamiteiten- en hersteltesten.

## **Aan de slag**

1. Geeft de businessimpactanalyse daartoe aanleiding? Dan worden gegevens realtime gerepliceerd naar een herstelfaciliteit. Dit zal voor scholen niet vaak aan de orde zijn, omdat kritieke systemen van scholen – bijvoorbeeld leerlingenadministratie of financiële boekhouding – veelal zijn uitbesteed. Stel deze eis in dat geval aan je leverancier.

## **Referentie naar andere normen en kaders**

ISO A8.14

Certificeringsschema ROSA:

Beschikbaarheid/Ontwerp

Beschikbaarheid/Herstel

## **Link naar relevante P normen**

### **BC.05 Crisismanagement**

#### **Norm**

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 is dit nodig?**

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

#### **1 - Ad hoc**

1 – Ad hoc

a) Er zijn geen crisismanagementplannen of -procedures.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

a) Er is een proces voor crisismanagement, maar deze is slechts gedeeltelijk ingevoerd.

b) Er is een crisismanagementteam, maar de verantwoordelijkheden, taken en benodigde acties zijn informeel en ad hoc.

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

a) 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.

b) Alle betrokkenen zijn op de hoogte van hun verantwoordelijkheden tijdens een crisis.

c) Er zijn periodiek crisisoefeningen voor crisismanagementteams.

#### **4 - Beheerst**

4 – Beheerst

a) Er zijn specifieke herstelscenario's gedefinieerd, waarbij voor elk scenario is bepaald hoe wordt omgegaan met de media en wat gecommuniceerd wordt.

b) Periodiek vindt een algehele oefening van het crisismanagement plaats om het hele proces, inclusief rampverklaring en escalatieprocedures, te valideren.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

a) Er worden verbeteringen bepaald en ingevoerd op basis van de oefeningen van het crisismanagementteam.

b) Resultaten en verbeteringen worden gerapporteerd aan het schoolbestuur en de schoolleiding.

#### **Aan de slag**

1. Maak het crisismanagementplan onderdeel van het bedrijfscontinuïteitsplan. Zie voor meer informatie norm BC.01 Bedrijfscontinuïteitsplanning.

2. Houd jaarlijks een crisisoefening voor het crisismanagementteam.

## Referentie naar andere normen en kaders

ISO A5.29, A5.30

## Link naar relevante P normen

# 15. Ketenbeheer

Ketenbeheer gaat over het hebben van controle op de uitbestede it-diensten. Zeker binnen de onderwijssector worden veel Software as a Service-oplossingen (SaaS-oplossingen) gebruikt. Dit biedt voordelen, want de grotere organisaties die hierin gespecialiseerd zijn hebben veelal een hoger beveiligingsniveau dan een individuele school zelf zou kunnen bereiken. Tegelijkertijd betekent het ook dat de school er minder directe controle over heeft. Daarom is het van groot belang dat je goede afspraken maakt met leveranciers over de minimale beveiligingsvereisten.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Hoofd inkoop, IBP-verantwoordelijke

Geraadpleegd: Adviseur informatiebeveiliging, it-verantwoordelijke

Geïnformeerd: Medewerkers van de school

## SC.01 Service Level Agreement

### Norm

It-services die aan de organisatie worden geleverd, worden gedefinieerd in het contract en in de bijhorende Service Level Agreement (SLA). Er zijn maatregelen genomen om ervoor te zorgen dat diensten voldoen aan de huidige en toekomstige behoeften van de organisatie.

### Waarom is dit nodig?

Een SLA, ook wel dienstverleningsovereenkomst genoemd, zorgt voor duidelijke afspraken tussen de school en de leverancier van het product over onder andere het onderhoud en de ondersteuning van een it-component. Met de SLA kun je de leverancier aanspreken als zijn dienstverlening niet voldoet aan de afspraken.

### 1 - Ad hoc

1 – Ad hoc

a) Er is geen contract met bijbehorend Service Level Agreement (SLA).

### 2 - Herhaalbaar

2 – Herhaalbaar

a) Er zijn enkele afspraken gemaakt over servicelevels.

b) Er zijn geen afspraken gemaakt over periodieke rapportage over geleverde diensten.

### 3 - Bepaald (streefniveau)

3 – Bepaald

a) Servicelevels van it-diensten zijn gebaseerd op business requirements.

b) De SLA bevat afspraken over periodieke rapportage van geleverde diensten en performance.

c) De gedefinieerde serviceniveaus zijn gedocumenteerd in een SLA en formeel goedgekeurd door het schoolbestuur of de schoolleiding en de it-serviceprovider.

#### **4 - Beheerst**

4 – Beheerst

- a) In de SLA zijn specifieke afspraken opgenomen over informatiebeveiliging.
- b) Afspraken over het beëindigen van diensten (bijvoorbeeld exitclausule, escrow, dataoverdracht/-vernietiging) zijn onderdeel van de SLA.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

- a) Criteria voor beveiligingsincidenten zijn gedefinieerd en beveiligingsincidenten worden separaat inzichtelijk gemaakt, naast incidenten veroorzaakt door gebreken of defecten.

#### **Aan de slag**

1. Bepaal voorafgaand aan een offerteaanvraag of aanbesteding wat de eisen zijn die gesteld worden aan de dienst en de leverancier. Denk hierbij bijvoorbeeld aan waar data opgeslagen moet worden, back-upeisen, beschikbaarheidsniveaus en certificering voor kwaliteit en informatiebeveiliging.
2. Stel bij het contracteren van een dienstverlener een SLA op.
3. Zorg dat de SLA wordt goedgekeurd door het schoolbestuur.

#### **Referentie naar andere normen en kaders**

ISO 8.1, A5.19, A5.20, A5.21, A5.22, A8.30

#### **Link naar relevante P normen**

### **SC.02 Servicelevelmanagement**

#### **Norm**

Business requirements en de manier waarop it-services en serviceniveaus bedrijfsprocessen ondersteunen, worden periodiek geanalyseerd. Nagegaan wordt of overeengekomen serviceniveaus worden gehaald. Afwijkingen worden besproken met leveranciers.

#### **Waarom is dit nodig?**

Als je de SLA's goed beheert, heb je snel in de gaten wanneer de prestaties van een leverancier afwijken van wat er is afgesproken. Je kunt een leverancier daar dan op aanspreken zodat zij hun prestaties kunnen verbeteren. Dit komt ten goede aan de prestaties van de school.

#### **1 - Ad hoc**

1 – Ad hoc

- a) Er is geen proces voor servicelevelmanagement.

#### **2 - Herhaalbaar**

2 – Herhaalbaar

- a) Er is een proces voor servicelevelmanagement gedefinieerd, maar beheer en rapportage van servicelevels zijn niet formeel vastgelegd en/of organisatiebreed ingevoerd..

#### **3 - Bepaald (streefniveau)**

3 – Bepaald

- a) Er is een proces voor servicelevelmanagement gedefinieerd, ingevoerd en goedgekeurd door het schoolbestuur

of de schoolleiding.

b) De performance van de services worden periodiek gerapporteerd in een servicelevelrapport (SLR), en indien nodig besproken met de leverancier.

#### **4 - Beheerst**

4 – Beheerst

a) De requirements voor service-onderdelen worden periodiek vergeleken met de daadwerkelijke prestaties van de geleverde onderdelen. Wanneer deze niet voldoen aan de formele SLA-levels/-requirements wordt actie ondernomen.

b) De operationele effectiviteit van het servicelevelmanagementproces wordt minstens één keer per jaar geëvalueerd. Indien nodig worden verbeteringen aangebracht.

#### **5 - Continu verbeteren**

5 – Continu verbeteren

a) Veranderende business requirements worden bekeken in de context van het huidige serviceportfolio om eventuele behoefte aan nieuwe of verbeterde services en servicelevelmogelijkheden te identificeren

#### **Aan de slag**

1. Neem servicelevelmanagement op in het leveranciersmanagementproces.
2. Spreek in de SLA af dat er periodiek een rapportage wordt ontvangen. Hoe vaak dat gebeurt hangt af van hoe kritiek het systeem voor je organisatie is. Dit kan maandelijks, maar ook elk kwartaal. Beoordeel deze rapportages en bespreek afwijkingen volgens het leveranciersmanagementproces met de proceseigenaar en indien nodig met de leverancier.

#### **Referentie naar andere normen en kaders**

ISO 8.1, A5.19, A5.20, A5.21, A5.22, A8.30

#### **Link naar relevante P normen**

### **SC.03 Leveranciersrisicomanagement**

#### **Norm**

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. Leveranciersrisicomanagement neemt aspecten in overweging als niet-openbaarmakingsovereenkomsten (non-disclosure agreements, NDA's), escrowcontracten, voortdurende levensvatbaarheid van de leverancier, conformiteit met beveiligingseisen, alternatieve leveranciers, boetes en beloningen, enzovoort.

#### **Waarom is dit nodig?**

Leveranciersrisicomanagement zorgt ervoor dat risico's met betrekking tot leveranciers beheerd worden. Op basis van deze risico's kunnen eisen aan leveranciers gesteld worden tijdens de aanbestedingsfase. Voorbeelden hiervan zijn levensvatbaarheid van de leverancier, naleving van beveiligingseisen en de beschikbaarheid van de dienst/applicatie.

## **1 - Ad hoc**

### **1 – Ad hoc**

- a) Er is geen proces voor leveranciersrisicomanagement.
- b) Contracten en/of SLA's worden getekend zonder een gedegen risicoanalyse van de externe partij.

## **2 - Herhaalbaar**

### **2 – Herhaalbaar**

- a) Er is een proces voor risicomanagement van leveranciers gedefinieerd, maar dit is slechts gedeeltelijk ingevoerd.
- b) Voor cloudcomputing wordt een checklist gebruikt voor een snelle analyse van de provider.
- c) De geïdentificeerde risico's worden zelden gedocumenteerd en/of gerapporteerd.

## **3 - Bepaald (streefniveau)**

### **3 – Bepaald**

- a. Er is een proces voor leveranciersrisicomanagement gedefinieerd, ingevoerd en vastgesteld door het schoolbestuur of de schoolleiding.
- b. Risico's betreffende het vermogen van de leverancier om effectief en veilig (cloud)diensten te leveren worden voortdurend geanalyseerd en beperkt.
- c. In het proces voor leveranciersrisicomanagement wordt rekening gehouden met non-disclosure agreements (NDA's), escrowcontracten, levensvatbaarheid van leveranciers, compliance met beveiligingseisen, alternatieve leveranciers, boetes en beloningen, et cetera.
- d. Over niet-gemitigeerde of geaccepteerde risico's wordt periodiek aan het schoolbestuur of de schoolleiding gerapporteerd.
- e. Contracten zijn volgens algemene bedrijfsstandaarden en voldoen aan wet- en regelgeving (bijvoorbeeld dataprivacy).
- f. Voordat de contracten worden ondertekend wordt een toetsing verkregen, die aantoont dat de levering van diensten voldoet aan wet- en regelgeving en aan het eigen (beveiligings)beleid.

## **4 - Beheerst**

### **4 – Beheerst**

- a) De operationele effectiviteit van het proces voor leveranciersrisicomanagement wordt jaarlijks geëvalueerd. Eventuele verbeteringen worden aangebracht en geëvalueerd.
- b) Als onderdeel van het proces voor leveranciersrisicomanagement worden interne beheersmaatregelen, zoals beveiligingsmaatregelen, bij de externe partij of provider regelmatig geëvalueerd.

## **5 - Continu verbeteren**

### **5 – Continu verbeteren**

- a) De risico's met betrekking tot het vermogen van de leverancier om effectieve dienstverlening op een veilige en efficiënte manier voort te zetten, worden voortdurend onderzocht en beperkt.

## **Aan de slag**

1. Neem leveranciersrisicomanagement op in het leveranciersmanagementproces.
2. Bespreek risico's die niet gemitigeerd of geaccepteerd worden met het schoolbestuur of de schoolleiding

## **Referentie naar andere normen en kaders**

ISO 8.1, A5.14, A5.19, A5.20, A5.21, A5.22, A5.23

## **Link naar relevante P normen**

RB.04, SW.02

## **SC.04 Interne beheersing bij derden**

### **Norm**

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 is dit nodig?**

Het is voor je school belangrijk dat externe dienstverleners intern hun zaken goed op orde hebben en dat ze voldoen aan wet- en regelgeving en de afspraken die in het contract staan. Immers, als zij hun zaken niet goed geregeld hebben, levert dat risico's op voor de beschikbaarheid, integriteit, vertrouwelijkheid van de it-diensten en -componenten die zij leveren.

### **1 - Ad hoc**

1 – Ad hoc

a) Interne beheersing van externe partijen wordt niet geëvalueerd.

### **2 - Herhaalbaar**

2 – Herhaalbaar

a) Er zijn enkele procedures gedefinieerd voor adequate interne beheersing door externe partijen.

### **3 - Bepaald (streefniveau)**

3 – Bepaald

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

### **4 - Beheerst**

4 – Beheerst

- a. Er zijn procedures om te garanderen dat externe dienstverleners zich aan wet- en regelgeving houden (bijvoorbeeld dataprivacy).
- b. Verdere inzicht in deze toetsing wordt ook verkregen en opgevolgd door:
  - a. Een extern audit rapport (bijvoorbeeld SOC2, ISAE3402/SSAE16 of TPM);
  - b. Te steunen op een intern audit rapport van de serviceprovider (nadat de bekwaamheid van interne audit gevalideerd is);
  - c. Door gebruikmaking van de 'recht op audit' clausule.

### **5 - Continu verbeteren**

5 – Continu verbeteren

- a. Geautomatiseerde tooling en/of uitgebreide servicelevel rapporten bieden de organisatie maandelijks inzicht in de ontwikkeling van interne beheersmaatregelen van externe partijen.

### **Aan de slag**

1. Neem toetsing van interne beheersmaatregelen van leveranciers op in het leveranciersmanagementproces.

## **Referentie naar andere normen en kaders**

ISO 8.1, A5.20, A5.21, A5.22, A5.36

## **Link naar relevante P normen**