Beleid informatiebeveiliging en

Stichting VCO Harderwijk-Hierden
HARDERWIJK

Datum: 16 maart 2026

Inhoudsopgave

Inhoudsopgave **2**

1 IBP Beleid **4**
1.1 Introductie 4

2 Bestuur **6**
2.1 Strategie & visie 6
2.2 Inzicht in het informatielandschap 7
2.3 Onafhankelijke toetsing 8

3 Organisatie **10**
3.1 Organisatie 10
3.2 Eigenaarschap en verantwoordelijkheid 10
3.3 Rollen en eigenaarschap 11

4 Risicomanagement **13**
4.1 Risicomanagement 13

5 Personeelsbeheer **15**
5.1 Personeelsbeheer 15
5.2 IBP binnen werving en selectie 15
5.3 Training digitale vaardigheden 15
5.4 Beperking risico’s ICT-medewerkers 16
5.5 Personele wijzigingen 16
5.6 Bewustwording 17

6 Configuratiemanagement **18**
6.1 Configuratiemanagement 18

7 Incident- & problemmanagement **19**
7.1 Incident- & problemmanagement 19
7.2 Incidentmanagement 19
7.3 Problemmanagement 20

8 Wijzigingenbeheer **21**
8.1 Wijzigingenbeheer 21

9 Inkoop en ingebruikname van software **23**
9.1 Inkoop en ingebruikname van software 23

10 Datamanagement **25**
10.1 Datamanagement 25
10.2 Databeheer en verwijdering van hardware 25
10.3 Gegevensuitwisseling 26
10.4 Procesmanagement en gegevensverwerking 27

11 Identity- & Accessmanagement **29**
11.1 Identity- & Accessmanagement 29

12 Securitymanagement **32**
12.1 Securitymanagement 32
12.2 Basisbeveiliging ICT 32
12.3 Gedragscode IBP 34
12.4 Bewaking en toetsing van de ICT-beveiliging 34

12.5 ICT-infrastructuur 35
12.6 Cryptografische sleutels 36

13 Fysieke beveiliging 37
13.1 Fysieke beveiliging 37
13.2 Fysieke beveiligingsmaatregelen 37
13.3 Beheer van fysieke toegangsrechten 37
13.4 Cameratoezicht 38

14 ICT-operatie 39
14.1 ICT-operatie 39

15 Bedrijfscontinuïteitsmanagement 41
15.1 Bedrijfscontinuïteitsmanagement 41
15.2 Bedrijfscontinuïteitsplan 41
15.3 Technische en organisatorische maatregelen voor BCM 41

16 Ketenbeheer 43
16.1 Ketenbeheer 43

17 Bijlagen 45
17.1 Bijlagen 45

18 IBP-processen 46
18.1 IBP-processen 46
18.2 Operationele processen in kaart 46
18.3 Register van verwerkingen 46
18.4 (pre-)DPIA 48
18.5 Privacy by Design & Default 49
18.6 Datavernietiging op applicatieniveau 49
18.7 Toetsing gegevensverstrekking aan derden 50

19 Organisatorische inbedding 52
19.1 Organisatorische inbedding 52
19.2 Functionaris Gegevensbescherming 52
19.3 Medezeggenschapsraad 53

20 Rechten van betrokkenen 54
20.1 Rechten van betrokkenen 54
20.2 Afhandeling rechten van betrokkenen 54
20.3 Informatieplicht 55
20.4 Toestemming 55
20.5 Geautomatiseerde besluitvorming/profilering 57

21 Verantwoording 59
21.1 Verantwoording 59

1 IBP Beleid

1.1 Introductie

In een wereld die steeds verder digitaliseert, is het beschermen van informatie en privacy van essentieel belang. Het beheren van de (digitale) informatievoorziening binnen VCO brengt steeds meer belangrijke verantwoordelijkheden met zich mee met betrekking tot veiligheid. Elke handeling kan invloed hebben op de veiligheid van onderwijsprocessen en de vertrouwelijkheid van gegevens.

Als VCO vinden wij dat de veiligheid en privacybescherming van onze leerlingen en medewerkers voorop moet staan. De veiligheid die met technische middelen kan worden bereikt is echter begrensd en dient ook bij stichting Voor Christelijk Onderwijs Harderwijk-Hierden (hierna: VCO) te worden ondersteund door passend beheer en procedures. Hoewel er door de ontwikkeling binnen de ICT nieuwe beveiligingsrisico's zijn geïntroduceerd, blijkt bij beveiligingsincidenten vaak de mens de meest kwetsbare schakel.

In het Normenkader Informatiebeveiliging & Privacy (IBP) voor het funderend onderwijs (FO) staan de eisen beschreven waaraan VCO moet voldoen. Met dit IBP-beleid geven wij als VCO invulling aan dit normenkader en beschrijven wij de wijze waarop wij als VCO de informatiebeveiliging en privacy borgen. Dit document zal samen met de technische beveiligingsmaatregelen, het privacy- en veiligheidsbeleid en de procedures een adequaat niveau van beveiliging voor VCO opleveren.

Ons IBP-beleid richt zich niet alleen op de technische aspecten van informatiebeveiliging, maar ook op de organisatorische maatregelen die bijdragen aan het creëren van een veilige en betrouwbare leer- en werkomgeving. Hierbij is de betrokkenheid van alle medewerkers, leerlingen, ouders, leveranciers en andere belanghebbenden van cruciaal belang.

Bestuurlijke vaststelling, communicatie en evaluatie

Het beleid informatiebeveiliging en privacy (IBP) is vastgesteld door het College van Bestuur van Stichting VCO Harderwijk-Hierden en vormt het kader voor alle organisatorische en technische maatregelen op het gebied van informatiebeveiliging en privacy.

Het IBP-beleid is beschikbaar voor medewerkers en wordt actief onder de aandacht gebracht via interne communicatiekanalen, het privacy- en veiligheidsplan en het bewustwordingsprogramma IBP.

De uitvoering en effectiviteit van het IBP-beleid worden periodiek geëvalueerd. Deze evaluatie vindt onder andere plaats via audits, het Jaarplan IBP en de bespreking van auditresultaten en actieplannen met het College van Bestuur. Op basis hiervan kan het beleid waar nodig worden aangepast of aangescherpt.

Wettelijke en reglementaire kaders

Het juridisch kader voor dit IBP-beleid wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet UAVG. Daarnaast kunnen uit andere wet- en regelgeving verplichtingen of instructies voortvloeien voor de verwerking van persoonsgegevens. Voor VCO is op dit gebied onder andere de volgende wetgeving van belang:

- Wet op het primair onderwijs;
- Wet onderwijstoezicht;
- Archiefwet en Archiefbesluit;
- Leerplichtwet;
- Wet medezeggenschap op scholen;
- Arbeidsregelgeving en CAO;
- Belastingwetgeving;
- Telecommunicatiewet en e-privacy wetgeving.

Indien een (mogelijke) strijdigheid tussen dit beleid en de AVG en/of gerelateerde wet- en regelgeving bestaat, dan moet voorafgaand aan een verwerking overlegd worden met de Privacy Officer.

Als onderwijssector hebben we afgesproken om toe te werken naar één normenkader om aan de minimale vereisten te voldoen voor digitaal veilig onderwijs. Dit is het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs'. Dit normenkader beschrijft de regels, principes en

standaarden op het gebied van informatiebeveiliging en privacy waaraan VCO moet voldoen voor een digitale veilige schoolomgeving.

Ter invulling van de AVG en de bescherming van persoonsgegevens heeft het bestuur het Privacyreglement VCO vastgesteld. Dit reglement is leidend voor de wijze waarop VCO invulling geeft aan de privacybeginselen (art. 5 AVG) zoals rechtmatigheid, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid. Het Privacyreglement wordt periodiek geëvalueerd en is beschikbaar voor alle belanghebbenden.

2 Bestuur

2.1 Strategie & visie

Om VCO digitaal veilig te houden, is een duidelijke strategie en visie op informatiebeveiliging en privacy (IBP) noodzakelijk. Hiermee borgen we de continuïteit van het lesgeven en de werking en veiligheid van essentiële informatiesystemen.

Binnen VCO is de bescherming van (gevoelige) informatie en persoonsgegevens van zowel leerlingen, ouders als medewerkers van groot belang. Het doel van informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen.

IBP speelt een belangrijke rol bij het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van data. Deze drie kwaliteitsaspecten worden als volgt gedefinieerd:

• Beschikbaarheid gaat over de mate waarin informatie op de juiste momenten beschikbaar is.

• Vertrouwelijkheid gaat over de mate waarin toegang tot informatie beperkt is tot diegenen die daartoe bevoegd zijn.

• Integriteit gaat over de mate waarin informatie correct geregistreerd wordt en zonder fouten is.

Een betrouwbare informatievoorziening is van essentieel belang voor kwalitatief goed en hoogwaardig onderwijs binnen VCO. Ouders, medewerkers, leerlingen en alle andere belangstellenden verwachten daarnaast dat er zorgvuldig wordt omgegaan met privacygevoelige informatie.

Visie
IBP is niet alleen een technische aangelegenheid, maar een integraal onderdeel van de dagelijkse bedrijfsvoering binnen VCO. IBP is een continue verantwoordelijkheid van alle medewerkers, leerlingen, ouders en leveranciers. Dit vereist een cultuur waarin het bewustzijn van risico’s is ingebed in alle lagen van VCO.

De wijze waarop we IBP hebben ingericht, is gefocust op een praktische, risico-gebaseerde aanpak waarbij het normenkader IBP leidend is. We willen veilig en betrouwbaar onderwijs bieden. Onze focus ligt op het implementeren van volgens de wet- en regelgeving passende technische en organisatorische maatregelen, in lijn met onze risicobereidheid. IBP is belangrijke pijler, maatregelen moeten waar mogelijk praktisch uitvoerbaar en kosten-efficiënt zijn, zodat we de continuïteit van het onderwijs kunnen waarborgen.

Strategie

Onze strategie voor IBP is gericht op het realiseren van de kernprincipes uit onze visie: IBP moet effectief, praktisch en kosten efficiënt zijn, waarbij we altijd oog houden voor de onderwijskundige doelen en wet- en regelgeving.

Onze doelstellingen ten aanzien van IBP zijn als volgt:

1. Voldoen aan de relevante wettelijke vereisten
VCO hanteert het normenkader IBP als leidraad voor de ontwikkeling, implementatie en controle van onze informatiebeveiligings- en privacy maatregelen. Het normenkader helpt ons om te voldoen aan de wettelijke eisen, zoals de AVG, en biedt een praktische aanpak die aansluit bij de specifieke behoeften van het primair onderwijs.
Ieder jaar stellen we een Jaarplan IBP op (B:GO.03 - Jaarplan IBP), waarin alle activiteiten rondom IBP en ook de implementatie concreet vorm krijgen. Het jaarplan IBP wordt aan het eind van het jaar geëvalueerd, in de vorm van een Jaarplan IBP rapport (E:GO.03 – Jaarplan IBP rapport), hieruit volgen de behaalde resultaten en een advies voor het komende jaar.

2. Risico-gebaseerde aanpak
Onze strategie komt voort uit een risico-gebaseerde aanpak waarbij de focus ligt op de bescherming van de meest kritieke informatie en (persoons)gegevens en systemen. VCO is zich ervan bewust dat risico’s niet te voorkomen zijn en streeft ernaar om de grootste risico’s te beperken en beheersbaar te maken. Beheersmaatregelen worden toegepast op deze kritieke informatie en (persoons)gegevens en systemen binnen onze organisatie. We hebben een overzicht van bedrijfskritische applicaties

opgesteld (D.GO.02 - Overzicht bedrijfskritische applicaties). Indien hierbij sprake is van een hoog risicoverwerking op persoonsgegevens wordt er een privacytoets (DPIA) uitgevoerd.

3. Bewustwording en training
Informatiebeveiliging en privacy is een verantwoordelijkheid van iedereen binnen VCO. Daarom zetten we in op bewustwording en training. Een goed geïnformeerde en alerte organisatie vormt de eerste verdedigingslinie tegen bedreigingen. Het bewustwordingsprogramma (B:HR.06 - Bewustwordingsprogramma) in combinatie met de jaarlijkse aandacht IBP op schoolniveau (D:GO.02 - Jaarlijkse aandacht IBP op schoolniveau), vormen hiervoor onze basis.

4. Beveiliging van digitale en fysieke omgevingen
We richten ons op de beveiliging van informatie in zowel digitale als fysieke omgevingen, met een focus op praktische en eenvoudig toepasbare maatregelen. Dit omvat zowel technische als organisatorische maatregelen die zorgen voor een veilige werkomgeving.

5. Incidentenbeheer en continuïteit
Beveiligingsincidenten of datalekken kunnen ondanks voorzorgsmaatregelen altijd optreden. Het is daarom van belang dat VCO snel en adequaat kan reageren, zodat de schade beperkt blijft en het onderwijsproces zo min mogelijk wordt verstoord.

6. Kostenbeheersing en efficiëntie
Maatregelen om informatiebeveiliging en privacy te waarborgen moeten uitvoerbaar en betaalbaar blijven. We richten ons op, in volgens de wet- en regelgeving gestelde, passende technische en organisatorische maatregelen. Met oplossingen die effectief zijn zonder de organisatie onevenredig te belasten qua (financiële) middelen.

7. Verankering in de organisatie
Het succes van onze IBP-strategie hangt af van de verankering binnen heel VCO. IBP is dus niet slechts een verantwoordelijkheid van onze ICT-afdeling en -leveranciers, het is onderdeel van het dagelijks handelen en de cultuur van de VCO.

Roadmap

De IBP-roadmap en het Jaarplan IBP worden vastgesteld door het College van Bestuur en vormen de basis voor de planning, prioritering en uitvoering van IBP-maatregelen. Hierin worden ook de benodigde middelen, investeringen en verantwoordelijkheden vastgelegd.

De uit de roadmap en het Jaarplan IBP voortvloeiende maatregelen en procedures worden binnen de organisatie gecommuniceerd naar medewerkers en relevante stakeholders, zodat zij op de hoogte zijn van hun rol en verantwoordelijkheden bij de uitvoering van het IBP-beleid.

Vaststelling en communicatie
De strategie en visie op informatiebeveiliging en privacy (IBP) zijn vastgesteld door het College van Bestuur van Stichting VCO Harderwijk-Hierden. Het College van Bestuur draagt zorg voor de periodieke herbevestiging van deze strategie en visie, onder andere in samenhang met het Jaarplan IBP en de IBP-roadmap.

De strategie en visie op IBP worden actief gecommuniceerd binnen de organisatie en richting relevante externe partijen. Medewerkers worden geïnformeerd via beleidsdocumenten, bewustwordingsactiviteiten en jaarlijkse aandacht voor IBP op school- en organisatieniveau. Leveranciers en contractpartners worden geïnformeerd via contractuele afspraken, verwerkersovereenkomsten en relevante beleidsdocumentatie, zodat zij hun werkzaamheden in overeenstemming uitvoeren met de IBP-strategie van VCO.

2.2 Inzicht in het informatielandschap

Het beheer en gebruik van informatie binnen het primair onderwijs speelt een belangrijke rol bij het waarborgen van een effectieve, veilige en transparante leeromgeving. Inzicht in en beheer van de informatiestromen ondersteunt VCO om snel en adequaat in te spelen op veranderingen en externe dreigingen. Inzicht in het informatielandschap, laat zien hoe gegevens binnen VCO worden verwerkt en verbonden zijn, wat essentieel is voor het nemen van juiste beveiligingsmaatregelen.

Om organisatiebreed inzicht te behouden in de AVG-naleving, vindt er een continue stroom van

informatie plaats naar de Privacy Officer. Deze informatie wordt geput uit de centrale registers (zoals het verwerkingsregister en het datalekregister) die doorlopend worden geactualiseerd op basis van incidentmeldingen, nieuwe software-aanvragen en DPIA-uitkomsten vanuit de scholen. De Privacy Officer aggregeert deze informatie periodiek tot een sturingsbeeld voor de bestuursorganen.

Doelstellingen

- Inzicht te verkrijgen in de verwerking van informatie en persoonsgegevens en samenhang tussen processen en systemen binnen VCO.
- Tijdig en effectief in te spelen op wijzigingen in wet- en regelgeving of dreigingen van buitenaf.
- De juiste beveiligingsmaatregelen te nemen om onze (persoons)gegevens te beschermen.
- Te voldoen aan de doelstellingen van VCO, regelgeving en wettelijke vereisten, zoals de AVG.

Uitgangspunten

- Er is inzicht in zowel de huidige als de gewenste situatie voor het informatielandschap. Dit inzicht geeft een duidelijk overzicht van de huidige informatiebewaarplaatsen en -stromen en de gewenste situatie (streefbeeld), wat helpt bij het plannen en sturen van veranderingen.
- Eens twee jaar wordt het streefbeeld voor het informatielandschap door het schoolbestuur vastgesteld.
- Het plan om het streefbeeld te implementeren is in een migratieplan (B:GO.04 - Informatiemodel migratieplan) uitgewerkt en opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Het streefbeeld is in overeenstemming met de organisatiebrede doelstellingen van VCO, inclusief naleving van wettelijke voorschriften, zoals de AVG en de organisatorische verantwoordelijkheden.
- Het informatielandschap is visueel in kaart gebracht in een informatiemodel (D:GO.04 - Informatiemodel).
- Beheer van het informatiemodel wordt uitgevoerd onder verantwoording van het College van Bestuur en vindt plaats volgens een vastgesteld proces (C:GO.04 - Informatiemodel wijzigingsproces).
- Het Informatiemodel wordt gebruikt om beslissingen te nemen wanneer er wijzigingen zijn in het informatielandschap, zoals nieuwe applicaties of veranderingen in wet- en regelgeving. Zo wordt getoetst wat de gewenste oplossingsrichting is. Dit helpt VCO om gecontroleerd en veilig te veranderen, waarbij risico’s worden geminimaliseerd en naleving van wet- en regelgeving wordt gewaarborgd. Het gebruik van het informatiemodel is verwerkt in het changemanagementproces (C:CH.01 - Changemanagementproces).
- VCO hanteert een actuele architectuurbaseline voor haar IT-landschap. Voor de inrichting van de Microsoft-omgeving (tenant) wordt de vigerende industrie-baseline als 'SOLL'-architectuur gehanteerd. Deze baseline is gericht op maximale veiligheid en naleving van wettelijke voorschriften. Het bestuur keurt de gehanteerde architectuurkaders periodiek goed als onderdeel van het IT-jaarplan.

2.3 Onafhankelijke toetsing

Onafhankelijke toetsing (audit) van de informatievoorziening en ICT binnen het onderwijs is cruciaal om te garanderen dat VCO voldoet aan wet- en regelgeving. Deze audits, uitgevoerd door interne of externe auditors, bieden inzicht in afwijkingen tussen de dagelijkse praktijk en de norm en het vastgestelde beleid/procedure. Een goed opgesteld auditplan, helpt het schoolbestuur om afwijkingen te signaleren en daarmee risico’s te mitigeren, door de juiste maatregelen te treffen. We toetsen minimaal eens per drie jaar het volledige normenkader.

Doelstellingen

- Afwijkingen tussen de normen, de dagelijkse praktijk en het vastgestelde beleid/procedures signaleren.
- De naleving van wet- en regelgeving, beleidsnormen en interne procedures te waarborgen.
- De prestaties van de informatievoorziening en ICT-processen te verbeteren door middel van correctieve maatregelen.
- Een veilige, efficiënte en betrouwbare ICT-omgeving te creëren binnen VCO.

Uitgangspunten

- De auditcommissie stelt een auditplan op en het schoolbestuur keurt dit goed. Eisen voor audits en andere controleactiviteiten worden zorgvuldig gepland en goedgekeurd door de Privacy Officer van VCO om het risico op verstoring van bedrijfsprocessen te minimaliseren.
- Het auditplan (B:GO.05 - Auditplan Normenkader) beschrijft welke onderdelen van de informatievoorziening en ICT wanneer worden getoetst en door wie (interne of externe auditor).
- De richtlijn is dat het gehele normenkader ten minste eens per drie jaar wordt getoetst, zodat VCO regelmatig beoordeelt of beleid/processen voldoen aan alle normen.
- Informatiesystemen van VCO worden bovendien voortdurend gecontroleerd op naleving van de implementatie van beveiligingsnormen, in nauwe samenwerking met onze ICT-partner Serve IT. Naast een continue monitoring vindt er jaarlijks een zogenaamde APK plaats waarbij alle systemen doorgelicht worden.
- Na afloop van elke audit worden de resultaten vastgelegd in een auditrapport (E:GO.05 - Auditrapport Normenkader). Vervolgens wordt een actieplan (B:GO.05 - Auditactieplan Normenkader) opgesteld om de nodige verbeteringen door te voeren. Het actieplan omvat concrete maatregelen om afwijkingen op te lossen.
- De auditcommissie en de uitvoerende functionarissen bespreken de auditresultaten met het schoolbestuur. Het moment dat de auditresultaten worden besproken is opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP). Hierbij wordt het eerder opgestelde actieplan beoordeeld en vastgesteld om te waarborgen dat alle bevindingen binnen de gestelde termijn worden opgelost.
- De implementatie en uitvoering van de functiescheiding, zoals vastgelegd in de Autorisatiematrix, worden periodiek getoetst als onderdeel van de interne auditfunctie
- Bij de uitvoering van interne en externe audits wordt gebruikgemaakt van vastgestelde auditinstrumenten, waaronder checklists en werkdocumenten die zijn gebaseerd op het Normenkader Informatiebeveiliging en Privacy.
- De ingevulde checklists en onderliggende auditdocumentatie vormen onderdeel van het auditdossier en zijn beschikbaar voor verificatie en opvolging. De resultaten van de audits, inclusief bevindingen en verbetermaatregelen, worden gerapporteerd aan het College van Bestuur en besproken binnen de auditcommissie.

3 Organisatie

3.1 Organisatie

Het belang van effectieve besluitvorming en functiescheiding in het kader van informatiebeveiliging binnen VCO staan aan de basis voor digitale veiligheid. Heldere rolverdeling, verantwoordelijkheid en eigenaarschap zorgen voor goed afgewogen keuzes en dragen daarmee bij aan de bescherming van systemen en processen tegen bedreigingen.

Kennisoverdracht en het onderhouden van documentatie, trainingen en implementatiematerialen vinden centraal plaats. Bij wijzigingen in beleid, processen of systemen worden relevante documenten geactualiseerd en actief gecommuniceerd. Bij personeelswisselingen en functiewijzigingen wordt benodigde kennis overgedragen en, waar nodig, aanvullende instructie of training verzorgd. De actualiteit van documentatie en ondersteunende materialen wordt periodiek beoordeeld binnen de PDCA-cyclus.

3.2 Eigenaarschap en verantwoordelijkheid

Het belang van effectieve besluitvorming en functiescheiding in het kader van informatiebeveiliging binnen VCO staan aan de basis voor digitale veiligheid. Heldere rolverdeling, verantwoordelijkheid en eigenaarschap zorgen voor goed afgewogen keuzes en dragen daarmee bij aan de bescherming van systemen en processen tegen bedreigingen.

Door rollen, verantwoordelijkheden en eigenaarschap formeel toe te wijzen en te verankeren binnen VCO, ontstaat er een duidelijke structuur die bijdraagt aan effectieve besluitvorming en een betrouwbaar beheer van informatiebeveiliging. Dit zorgt ervoor dat iedereen binnen VCO weet wat er van hen wordt verwacht en welke rol zij spelen in het waarborgen van een veilige (digitale) omgeving. Daarnaast stelt deze aanpak VCO in staat om belangen zorgvuldig af te wegen bij het nemen van beslissingen over informatiebeveiliging.

De algehele beheercyclus (zowel vaststelling als implementatie, controle en bijstelling) van het informatiebeveiligingsproces valt onder de eindverantwoordelijkheid van de bestuurder van VCO. De bestuurder is samen met de Privacy Officer verantwoordelijk voor een duidelijk te volgen IBP beleid. Het Managementteam (MT) stelt, in samenspraak met de Privacy Officer, het gewenste niveau van informatiebeveiliging vast voor VCO.

De bestuurder bekrachtigt met de vaststelling van dit beleid de formele aansprakelijkheid voor het beheersen van de informatierisico’s en het naleven van de wet- en regelgeving, conform de strategie en organisatiedoelstellingen van VCO

Doelstelling

Het doel van eigenaarschap en verantwoordelijkheid is een duidelijke structuur te creëren voor het effectief managen van informatiebeveiligingsrisico’s en het waarborgen van informatiebeveiliging en privacy.

Uitgangspunten

- De uitvoering van het informatiebeveiligingsproces is belegd binnen de afdeling Bedrijfsvoering & Organisatie van VCO. Activiteiten voor informatiebeveiliging worden gecoördineerd door de Privacy Officer van VCO, die rechtstreeks aan de bestuurder rapporteert.
- De Privacy Officer draagt de verantwoordelijkheid over het ontwikkelen van het informatiebeveiligingsbeleid en -plan, de uitvoering van de risicoanalyse, de implementatie van het beveiligingsplan, het evalueren van de documentatie en de naleving van het beleid.
- De bestuurder is eindverantwoordelijk voor privacy binnen de organisatie en is als enige bevoegd om restrisico’s te accepteren die overblijven na het treffen van maatregelen (bijvoorbeeld uit een DPIA).
- Schooldirecteuren en stafmanagers zijn verantwoordelijk voor de naleving van het privacybeleid binnen hun eigen school.
- De IBP'er is gemandateerd om (pre-)DPIA’s te initiëren en te coördineren. De uitkomsten en geadviseerde maatregelen worden ter besluitvorming voorgelegd aan het bestuur.

Ten aanzien van de periodieke IBP-verslaglegging gelden de volgende verantwoordelijkheden:

- Privacy Officer: Is verantwoordelijk voor de inhoudelijke samenstelling van het organisatieverslag en het verzamelen van de benodigde data
- College van Bestuur: Is verantwoordelijk voor de definitieve vaststelling van het verslag en de verspreiding hiervan naar de Raad van Toezicht en de GMR
- Functionaris Gegevensbescherming: Is verantwoordelijk voor het onafhankelijk toetsen van het verslag en het adviseren van het bestuur hierover."

De leden van het IBP-team zijn:

- Bovenschoolse ICT'er
- Privacy Officer
- Functionaris Gegevensbescherming

Onder verantwoording van:

- College van Bestuur

Onder toezicht van:

- Functionaris Gegevensbescherming

VCO heeft een Functionaris Gegevensbescherming aangesteld. De FG houdt intern toezicht op de naleving van de AVG en adviseert het bestuur en de organisatie. De FG voert zijn taken onafhankelijk uit en ontvangt hierover geen instructies van het bestuur of anderen en heeft geen andere taken die kunnen leiden tot belangenverstrengeling. De FG rapporteert rechtstreeks aan het College van Bestuur over de stand van zaken rondom privacy.

Betrokkenheid: De FG wordt tijdig betrokken bij alle plannen die impact hebben op privacy, zoals bij de start van nieuwe projecten of de aanschaf van systemen (DPIA's).
Alle rollen op het gebied van het managen van informatiebeveiligingsrisico's zijn vastgesteld en toegewezen op normniveau, dit wordt uitgewerkt in het overzicht van rollen (D:OR.01 - Overzicht van rollen op normniveau).

Om de continuïteit en relevantie van het IBP-beleid te waarborgen, worden alle rollen, verantwoordelijkheden en de toewijzing van het eigenaarschap van informatierisico's jaarlijks geëvalueerd door de Privacy Officer en ter bespreking voorgelegd aan het bestuur.

Medezeggenschap

De GMR vertegenwoordigt het personeel, de ouders en de leerlingen op stichtingsniveau. In het kader van IBP heeft de GMR de volgende positie:

- Instemmingsrecht: Conform het Medezeggenschapsstatuut en de WMS heeft de GMR instemmingsrecht op de vaststelling of wijziging van het IBP-beleid en het Privacyreglement.
- Informatierecht: Het College van Bestuur informeert de GMR proactief over de algemene staat van informatiebeveiliging en de omgang met persoonsgegevens binnen de stichting.
- Verantwoording: De GMR ontvangt jaarlijks een samengevoegde rapportage over de naleving van het IBP-beleid, waarin de belangrijkste trends op het gebied van incidenten, verzoeken van betrokkenen en verbetermaatregelen worden gedeeld.

Hiermee fungeert de GMR als kritische gesprekspartner voor het bestuur en waarborgt zij de balans tussen de onderwijsambities en de bescherming van de persoonlijke levenssfeer van de VCO-gemeenschap

3.3 Rollen en eigenaarschap

VCO hanteert het principe van functiescheiding als een fundamentele beheersmaatregel. Dit is een expliciete strategie om te voorkomen dat individuele medewerkers in staat zijn essentiële processen te schaden of frauduleuze handelingen te verrichten, en verkleint daarmee de kans op onbedoelde fouten. Dit beleid richt zich op het afstemmen van autorisaties op basis van functies en rollen en het beperken van toegang tot gegevens en systemen op basis van de noodzaak voor het uitvoeren van dagelijkse werkzaamheden. De scheiding van rollen en verantwoordelijkheden is formeel vastgesteld

door het bestuur. Dit principe wordt operationeel geborgd door de Autorisatiematrix.

Doelstelling

Het doel van functiescheiding is VCO te beschermen tegen risico’s die voortvloeien uit nalatig gebruik of opzettelijk misbruik van systemen.

Uitgangspunten

- Niemand bij VCO mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen.
- Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd wordt als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
- Er is een overzicht opgesteld (D:OR.02 – Functiescheidingsoverzicht) waarin combinaties van taken en autorisaties (rechtenstructuur) zijn opgenomen die aan één medewerker mogen worden toegekend. Dit overzicht zorgt ervoor dat ongeoorloofde combinaties van uitvoerende en controlerende taken worden vermeden.
- Indien deze taken niet gescheiden kunnen worden, wordt er apart toezicht georganiseerd (C:OR.02 - Toezichtproces op afwijkingen functiescheiding) om misbruik of nalatigheid te voorkomen.
- Dit geldt ook voor technisch beheerders die geen toegang mogen hebben tot de data van het informatiesysteem dat zij beheren. Deze afwijkingen worden vastgelegd binnen het functiescheidingsoverzicht (D:OR.02 – Functiescheidingsoverzicht).

4 Risicomanagement

4.1 Risicomanagement

Het bestuur van Stichting VCO Harderwijk-Hierden stelt vast dat informatiebeveiliging en privacy randvoorwaardelijk zijn voor het realiseren van goed onderwijs. De risicobereidheid is als volgt geformuleerd: VCO accepteert uitsluitend die risico's op het gebied van informatiebeveiliging en privacy die geen wezenlijke impact hebben op de continuïteit van het onderwijs, de bescherming van persoonsgegevens, de reputatie van de organisatie en het vertrouwen van ouders en leerlingen. Risico's die kunnen leiden tot schending van wettelijke verplichtingen, verlies van vertrouwelijke gegevens of langdurige verstoring van het primaire proces worden niet geaccepteerd en dienen te worden gemitigeerd tot een aanvaardbaar restrisico. Acceptatie van restrisico's vindt uitsluitend plaats na expliciete bestuurlijke afweging en vastlegging. De risicobereidheid wordt jaarlijks geëvalueerd en indien nodig bijgesteld in het kader van de PDCA-cyclus.

IBP-risico's worden periodiek geclassificeerd, geprioriteerd en besproken in het managementteam, op basis van dezelfde methodiek als andere strategische risico's. De status van IBP-risico's, de voortgang van beheersmaatregelen en de acceptatie van restrisico's worden opgenomen in de kwartaalrapportages en het jaarplan. Hiermee is geborgd dat IBP-risico's structureel worden meegenomen in de bestuurlijke afwegingen en dat eigenaarschap en opvolging zijn belegd.

Doelstelling

Het doel van risicomanagement is om te zorgen dat informatiebeveiligingsrisico's op een gestructureerde manier worden beheerst.

Uitgangspunten

Het startpunt voor risicomanagement op het gebied van informatiebeveiliging binnen VCO bestaat uit vijf identificatie pijlers:

1. Het Normenkader IBP is de basis voor informatierisicomanagement binnen VCO en wordt gezien als zelfstandig onderdeel binnen het kader van informatiebeveiliging en privacy. Als VCO functioneren we minimaal op het vereiste volwassenheidsniveau 3 op en zorgen we ervoor dat we hieraan blijven voldoen.
2. DPIA's worden gezien als een belangrijk onderdeel van onze risicobeheersing. DPIA's worden tijdig en op de juiste verwerkingen en applicaties uitgevoerd zodat we informatiebeveiligingsrisico's identificeren en beheersbaar kunnen maken. Als VCO volgen we de vastgestelde beheersmaatregelen vanuit de DPIA's op.
3. Door de ICT-sector uitgevoerde risicoanalyses/ dreigingsbeelden, zoals het 'Dreigingsbeeld funderend onderwijs'.
4. De verantwoordelijkheid voor het identificeren van de strategische risico's ligt bij het schoolbestuur en voor de tactische en operationele risico's bij de schooldirecteuren, leidinggevenden van de stafafdelingen, proceseigenaren en systeemeigenaren. Hieronder vallen ook risico's vanuit fysieke beveiliging.
5. Door VCO zelf vastgelegde incidenten (datalekken/beveiligingsincidenten) en problemen.

We voeren risicomanagement uit in de volgende vijf stappen:

1. Identificeren van de risico's (zie vorige stap)

2. Uitvoeren van de risicoanalyse
   Risicobereidheid: De risicobereidheid van VCO is leidend. Risico's met een mogelijke impact op de privacy van leerlingen en medewerkers worden minimaal geaccepteerd.

3. Bepalen van de beheersmaatregelen
   Vermijden: Het proces aanpassen zodat het risico niet meer bestaat.
   Mitigeren: Maatregelen treffen om kans of impact te verlagen.
   Overdragen: Risico delen (bijv. verzekeren of contractueel beleggen).
   Accepteren: Formeel accepteren van een restrisico door het bestuur

4. Implementeren van de beheersmaatregelen
5. Monitoring en evaluatie van de geïmplementeerde beheersmaatregelen

Bij het uitvoeren van de bovengenoemde vijf stappen van risicomanagement, erkennen we als VCO een aantal randvoorwaarden die bepalen hoe we omgaan met de risico's. Deze randvoorwaarden zijn:
1. Risicobereidheid/risicoprofiel
2. Eigenaarschap
3. Dataclassificatie

Het bovenstaande beleid is uitgewerkt in het risicomanagementproces (C:RM.02 – Risicomanagementproces). Daarnaast leggen we risico's vast in een risicoanalyse (D:RM.02 - Risicoanalyse) en stellen we een risico actieplan op (B:RM.03 - Risico actieplan) om beheersmaatregelen vast te stellen, implementeren en evalueren. De status van risico's (E:RM.02 – (rest)Risico rapport) wordt periodiek gerapporteerd aan het schoolbestuur.

5 Personeelsbeheer

5.1 Personeelsbeheer

Personeelsbeheer richt zich op de medewerkers binnen VCO. Specifieke aandacht is er voor medewerkers die op basis van hun werkzaamheden over passende competenties dienen te beschikken voor een ICT-rol en overige rollen. Personeelsbeheer omvat de gehele cyclus van werving, doorstroming en uitdiensttreding, evenals het delen en behouden van kennis over IBP.

Competenties op het gebied van IBP worden regelmatig getoetst, waar nodig wordt er actie genomen om de competenties op het noodzakelijke niveau te krijgen. Bij functiewijzigingen, zoals het aangaan van een dienstverband elders, worden direct maatregelen getroffen voor kennisoverdracht en herverdeling van verantwoordelijkheden om risico's te minimaliseren en de continuïteit van functies te waarborgen. Er is aandacht voor instructies aan medewerkers en technische ondersteuning. We hebben een bewustwordingsprogramma om medewerkers te informeren over hun verantwoordelijkheden met betrekking tot IBP.

5.2 IBP binnen werving en selectie

IBP binnen werving en selectie zorgt ervoor dat VCO beschikt over gekwalificeerde en gescreende ICT-medewerkers op het gebied van het veilig werken met vertrouwelijke gegevens.

Doelstellingen

- Gekwalificeerde ICT-medewerkers aantrekken die bijdragen aan een veilige en competente werkomgeving.
- Voorzien in uitgangspunten voor de selectie en screening van medewerkers en externen.

Uitgangspunten

- • De rollen en verantwoordelijkheden van medewerkers en externe gebruikers ten aanzien van beveiliging zijn vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van VCO.
- Het wervingsproces voor ICT-medewerkers (C:HR.01 - Wervingsproces ICT personeel (HR-proces)) is gedocumenteerd en wordt onderhouden in overeenstemming met het algemene personeelsbeleid.
- Bij het werven van (ICT-)medewerkers wordt aandacht besteed aan de specifieke kwalificaties en vaardigheden die nodig zijn voor de functie.
- Er zijn maatregelen ingevoerd om ervoor te zorgen dat de geworven ICT-medewerkers beschikken over de juiste competenties op het gebied van informatiebeveiliging en privacy.
- Screening (Verklaring Omtrent het Gedrag - VOG) maakt onderdeel uit van het wervingsproces en wordt uitgevoerd volgens de wettelijke voorschriften. Bij de aanstelling worden de gegevens die de medewerker heeft verstrekt over zijn arbeidsverleden en scholing geverifieerd. De VOG wordt herhaald volgens de voorschriften.
- Als onderdeel van de contractuele verplichting behoren medewerkers en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van VCO ten aanzien van informatiebeveiliging zijn vastgelegd.

5.3 Training digitale vaardigheden

In een snel veranderende digitale wereld is het essentieel dat al onze medewerkers over de juiste kennis en vaardigheden (blijven) beschikken om hun taken veilig en effectief uit te voeren. Door gerichte training, opleiding en kennisoverdracht te stimuleren, bevorderen we de continuïteit en de prestaties van medewerkers en waarborgen we een veilige en efficiënte werkomgeving.

Doelstelling
Het doel van het trainen van digitale vaardigheden is ervoor te zorgen dat onze medewerkers, over de juiste competenties beschikken om hun taken effectief en veilig uit te voeren binnen de gedigitaliseerde werkomgeving.

Uitgangspunten

- Er is een proces voor training ingevoerd (C:HR.02 - Trainingsproces ICT'ers en gebruikers) dat (nieuwe) medewerkers ondersteunt bij het ontwikkelen en bijhouden van de benodigde vaardigheden op het gebied van digitale vaardigheden. Dit proces is goedgekeurd door het schoolbestuur en wordt minimaal eens per jaar uitgevoerd.
- Medewerkers hebben toegang tot individuele persoonlijke ontwikkelplannen, waarin hun opleidings- en ontwikkelingsbehoeften zijn vastgelegd (B:HR.02 - Persoonlijk ontwikkelingsplan (HR-proces)). Dit draagt bij aan de voortdurende verbetering van vaardigheden, waarbij ook de focus gelegd kan worden op informatiebeveiliging, privacy en digitale vaardigheden.
- VCO zorgt voor de benodigde gebruikersondersteuning bij ICT-applicaties, zodat eindgebruikers de systemen efficiënt kunnen gebruiken en incidenten snel worden opgelost (C:HR.05 - ICT gebruikersondersteuningsproces). In dit proces is een opdeling gemaakt tussen ondersteuning door onze organisatie en door externe leveranciers.
- We houden beheerdocumentatie (D:HR.05 – De ICT beheerdocumentatie) bij om kennisoverdracht te waarborgen en om ervoor te zorgen dat systemen consistent en effectief worden beheerd en onderhouden. Er is met ICT en de externe ICT-leverancier een beheerdocumentatieproces afgesproken (C:HR.05 - ICT beheerdocumentatieproces) om te beschrijven hoe beheerdocumentatie wordt opgesteld, onderhouden en opgeslagen.

5.4 Beperking risico’s ICT-medewerkers

Om de continuïteit van het onderwijs te waarborgen, is het cruciaal dat VCO voor sleutelfuncties/-posities niet afhankelijk is van één medewerker. Daarom beschrijven we de maatregelen voor opvolgingsplanning, functierotatie en het aanwijzen van back-ups, zodat kritieke functies bij vertrek of langdurige afwezigheid van sleutelfiguren kunnen worden overgenomen.

Doelstelling
Het doel van ICT-personeelsrisico’s is risicobeperking van afhankelijkheid van specifieke medewerkers in sleutelfuncties/-posities om de continuïteit het onderwijs binnen VCO te waarborgen.

Uitgangspunten

- Het ICT-personeelsplan (B:HR.03 - ICT-personeelsplan) wordt door het schoolbestuur vastgesteld en bevat onderwerpen die de continuïteit van VCO waarborgen.

5.5 Personele wijzigingen

Wanneer een medewerker van functie verandert of het dienstverband eindigt worden beveiligingsrisico's beperkt en indien noodzakelijk maatregelen genomen om de continuïteit van de werkzaamheden te waarborgen.

Doelstelling
Het doel van personele wijzigingen is om bij functiewijzigingen en beëindiging van dienstverbanden gestructureerd alle noodzakelijke acties te ondernemen om continuïteit te garanderen en informatiebeveiligingsrisico’s te beperken.

Uitgangspunten

- Bij functiewijziging of beëindiging van een dienstverband worden kennis en verantwoordelijkheden van de vertrekkende medewerker tijdig overgedragen aan een aangewezen opvolger of collega binnen VCO. Dit proces is vastgelegd in het personeelswijzigingsproces (C:HR.04 - Personeelswijzigingsproces (HR-proces)).
- De toegangsrechten van de medewerker worden onmiddellijk herzien en zo nodig ingetrokken bij functiewijzigingen of beëindiging van het dienstverband. Dit voorkomt ongeautoriseerde toegang tot vertrouwelijke informatie en systemen.
- HR zorgt voor een checklist met de benodigde stappen voor de afhandeling van functiewijzigingen en beëindigingen. Deze checklist is opgenomen in het personeelswijzigingsproces (C:HR.04 - Personeelswijzigingsproces (HR-proces)). Voor het vertrek van de medewerker verifieert HR bij de verantwoordelijke manager of alle noodzakelijke acties correct zijn uitgevoerd.
- Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van VCO die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.

5.6 Bewustwording

Het juist handelen van medewerkers vormt de eerste verdedigingslinie tegen informatiebeveiligingsrisico’s en datalekken. Een bewustwordingsprogramma is daarom van groot belang om alle gebruikers binnen VCO, waaronder medewerkers, leerlingen en externen, bewust te maken van hun verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy. Door de betrokkenen te informeren over risico's en gedragsrichtlijnen helpt het bewustwordingsprogramma informatiebeveiligingsrisico’s te beperken. De bewustwordingsactiviteiten zijn opgenomen in het jaarplan IBP.

Om te voldoen aan het normenkader informatiebeveiliging en privacy en om de bewustwording en kennis van privacywetgeving onder medewerkers structureel te borgen, wordt deelname aan de e-learning Privacy Wijs en het behalen van de bijbehorende toets verplicht gesteld voor alle medewerkers van Stichting VCO Harderwijk-Hierden. Iedere medewerker dient jaarlijks de training te volgen en de toets met goed gevolg af te ronden. De voortgang en resultaten worden gemonitord via het centrale dashboard. Niet-naleving wordt opgevolgd door de directie, in samenwerking met de IBP’er. Deze verplichting is vastgesteld door het College van Bestuur, na instemming van de GMR, en wordt jaarlijks geëvalueerd en waar nodig bijgesteld.

Doelstelling
Het doel van bewustwording is medewerkers, leerlingen, leveranciers en andere betrokkenen binnen VCO te informeren, te trainen en te motiveren om op een veilige en verantwoorde manier om te gaan met informatie en persoonsgegevens.

Uitgangspunten

- Het bewustwordingsprogramma (B:HR.06 - Bewustwordingsprogramma) wordt VCO-breed uitgevoerd en richt zich op alle medewerkers, leerlingen, leveranciers en andere betrokkenen.
- Het bewustwordingsprogramma wordt jaarlijks vastgesteld en opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Alle medewerkers van VCO worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van VCO, voor zover relevant voor hun functie.
- Tijdens de inwerkperiode van nieuwe medewerkers worden informatiebeveiliging en privacy nadrukkelijk besproken. Periodiek wordt voor alle nieuwe medewerkers een verplichte IBP-training gegeven (D:HR.06 - IBP-training nieuwe medewerkers), de planning hiervan is opgenomen in het onboardingsproces van nieuwe medewerkers (C:HR.06 - Onboardingsproces nieuwe medewerkers (HR-proces)).
- Leerlingen worden betrokken bij het bewustwordingsprogramma wanneer zij gebruikmaken van digitale middelen binnen VCO. Informatiebeveiligingsrisico's worden op passende wijze uitgelegd zodat ook zij hun verantwoordelijkheid begrijpen en bijdragen aan een veilige digitale omgeving.
- Het bewustwordingsprogramma wordt jaarlijks geëvalueerd en indien nodig aangepast om te blijven voldoen aan de veranderende eisen en risico's op het gebied van informatiebeveiliging en privacy. De evaluatie van het bewustwordingsprogramma is opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).

6 Configuratiemanagement

6.1 Configuratiemanagement

Het effectief beheer van ICT-componenten binnen VCO hangt sterk af van configuratiemanagement. Dit proces is gericht op het documenteren van details zoals hardware, software (waaronder versienummers), updates, instellingen en hoe systemen met elkaar verbonden zijn. Deze informatie is vastgelegd in een centrale configuratiemanagementdatabase (CMDB) voor een volledig en actueel overzicht van de ICT-omgeving. Het beheer van fysieke digitale bedrijfsmiddelen speelt hierin een belangrijke rol, omdat dit dragers zijn van bedrijfs- en persoonsgevoelige informatie.

Doelstellingen

- Een volledig inzicht in alle ICT-componenten en hun configuraties, om het beheer van de ICT-omgeving van VCO te ondersteunen.
- Alle wijzigingen aan systemen en diensten vast leggen en analyseren om de impact en beveiligingsrisico’s te kunnen beoordelen en minimaliseren.
- Fysieke bedrijfsmiddelen registreren en beheren, zodat we overzicht hebben van alle hardware en informatiebeveiligingsrisico’s beperkt blijven.

Uitgangspunten

- Er is in overleg met onze ICT-leverancier een proces opgesteld (C:CO.01 – Configuratiemanagementproces) om alle configuratie-items (hardware, software, netwerkcomponenten, etc.) en hun kenmerken (zoals versienummers, licenties en instellingen) te identificeren, te beheren en te onderhouden.
- Het configuratiemanagementproces is volledig afgestemd op Change-, Incident- en Problemmanagement (zie hoofdstuk 7 resp. 6).
- Alle middelen en wijzigingen in middelen (hardware en software) worden door onze ICT-leverancier gemonitord en vastgelegd in een centrale opslag (D:CO.02 - De CMDB). De CMDB bevat alle relevante informatie inclusief onderlinge relaties tussen systemen en configuratiebaselines. Waar mogelijk wordt door onze ICT-leverancier automatisering ingezet om wijzigingen in apparatuur en software te detecteren, vast te leggen en te monitoren. Dit vergemakkelijkt het bijhouden van de CMDB en reduceert de kans op menselijke fouten. Alle fysieke bedrijfsmiddelen worden waar mogelijk voorzien van een unieke, traceerbare labeling bij aanschaf en registratie, conform de richtlijnen van de afdeling Bedrijfsvoering.
- Bij inkoop van fysieke digitale bedrijfsmiddelen, zoals laptops, digiborden en netwerkapparatuur, worden deze geregistreerd. De registratie van fysieke digitale bedrijfsmiddelen is vastgelegd in het bedrijfsmiddelen registratieproces (C:CO.01 - Digitale bedrijfsmiddelen registratieproces (Inkoopproces)).
- Het configuratiemanagementproces (C:CO.01) is gedocumenteerd, gestandaardiseerd en gecommuniceerd naar alle relevante medewerkers, inclusief de ICT-leverancier.
- Er is een formeel proces ingevoerd voor het complete beheer van licenties. Dit proces waarborgt dat VCO voldoet aan alle licentievoorwaarden en omvat de registratie van de gehele licentiecyclus (aanschaf, toewijzing, archivering en verlopen licenties).
- De contractbeheerder en de proceseigenaar CM voeren minimaal eens per jaar een evaluatie uit op de naleving van de licentiecyclus. De bevindingen worden opgenomen in de rapportage aan het management om te waarborgen dat de organisatie niet over- of onder-gelicentieerd is

7 Incident- & problemmanagement

7.1 Incident- & problemmanagement

Beveiliging is een cruciaal onderdeel van privacybescherming: zonder afdoende technische en organisatorische maatregelen is het risico op datalekken, ongeautoriseerde toegang en andere schendingen te groot. Het normenkader koppelt beveiliging expliciet aan privacy (niet alleen aan informatieveiligheid) om ervoor te zorgen dat persoonsgegevens adequaat worden beschermd.

Incidentmanagement richt zich op het snel en effectief verhelpen van verstoringen en veiligheidsincidenten om de continuïteit van ICT-diensten, en daardoor het onderwijs, te waarborgen. Wanneer het een incident met grote impact betreft of een incident dat zich vaker voordoet, wordt problemmanagement toegepast, waarbij diepgaand onderzoek plaatsvindt om de oorzaak te identificeren en structurele oplossingen te implementeren.

7.2 Incidentmanagement

Incidentmanagement richt zich op het snel en effectief verhelpen van verstoringen en veiligheidsincidenten in de ICT-omgeving, inclusief (cyber)beveiligingsincidenten. Als een incident de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verstoort, spreken we van een inbreuk op de informatiebeveiliging of een (cyber)beveiligingsincident. Binnen incidentmanagement stellen we procedures vast die ervoor zorgen dat incidenten tijdig worden geïdentificeerd, geanalyseerd, geregistreerd en afgehandeld, met een helder escalatieproces voor incidenten die niet direct opgelost kunnen worden.

De operationele uitvoering van de respons op grootschalige of kritieke cyberbeveiligingsincidenten is gedocumenteerd in het 'Stappenplan cybercriminaliteit'. Dit plan omvat de procedures voor preparatie, detectie, isolatie en herstel, inclusief contactpersonen en noodcommunicatiemiddelen. Het plan wordt jaarlijks geoefend en periodiek geëvalueerd.

Doelstellingen

- Incidenten afhandelen volgens het door VCO formeel vastgestelde incidentmanagementproces om doeltreffend en ordelijk te reageren op incidenten.
- Het detecteren, herkenbaar vastleggen en afhandelen van incidenten. Belangrijk hierbij is dat medewerkers, leerlingen en externen een incident of inbreuk op de informatiebeveiliging herkennen en ook melden als het zich voordoet.
- Leren van incidenten. Incidenten worden daarom geëvalueerd, zodat de procedures en beheersmaatregelen kunnen worden bijgesteld.
- Een gestructureerd proces opzetten om incidenten en potentiële datalekken snel te herkennen, juist te classificeren (niet elk incident is direct een datalek) en adequaat af te handelen om schade te beperken.

Uitgangspunten

- VCO heeft een centraal meldpunt, dat bekend is bij alle betrokkenen (medewerkers, leerlingen en externen).
- We hebben een incidentmanagementproces, in samenwerking met onze ICT-leverancier, opgesteld (C:IM.01 – Incidentmanagementproces) waarin we alle vereisten vanuit het normenkader hebben opgenomen, zoals rollen en verantwoordelijkheden, monitoring en training.
- Alle medewerkers, leerlingen en externe gebruikers van informatiesystemen en diensten van VCO zijn verplicht om alle waargenomen of verdachte zwakke plekken of incidenten direct te registreren en te rapporteren bij het centrale meldpunt, ten behoeve van proactieve probleemidentificatie
- Incidenten van de categorie beveiligingsincident en datalek worden door VCO geregistreerd in een incidentenregister (D:IM.01 – Incidentregister).
- Periodiek stellen we een rapport op (E:IM.01 – Incidentrapport) dat we bespreken met het schoolbestuur, het bespreken van dit rapport is opgenomen in de Jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Er zijn verantwoordelijkheden en procedures vastgesteld om een snelle, doeltreffende en

ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen. Informatiebeveiligingsgebeurtenissen worden zo snel mogelijk via de juiste leidinggevende niveaus gerapporteerd.
- Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure. Datalekken worden binnen 72 uur gemeld aan de Autoriteit Persoonsgegevens.
- Incidenten van de categorie beveiligingsincident en datalek worden vastgelegd in een systeem. Vermissing of diefstal van apparatuur of media die gegevens van VCO bevatten wordt altijd aangemerkt als informatiebeveiligingsincident.
- Rollen, verantwoordelijkheden en escalaties zijn vastgelegd, zodat de afhandeling efficiënt en consistent verloopt.

7.3 Problemmanagement

Problemmanagement richt zich op het identificeren en beheersen van onderliggende oorzaken van incidenten met een grote impact dan wel terugkerend karakter in de ICT-omgeving, waardoor het aantal en de impact van beveiligingsincidenten en datalekken worden verminderd. Waar incidentmanagement zich richt op het zo snel mogelijk herstellen van verstoringen, gaat problemmanagement een stap verder door proactief en reactief de oorzaken van structurele ICT-fouten te analyseren en blijvende oplossingen te ontwikkelen.

Doelstellingen

- Problemen bij de bron aan pakken, wat de continuïteit en stabiliteit van de ICT-diensten ten goede komt en de kans op herhaalde beveiligingsincidenten verkleint.
- Problemen afhandelen volgens het door VCO formeel vastgestelde problemmanagementproces voor een doeltreffende afhandeling van deze problemen.
- Het detecteren, herkenbaar vastleggen en afhandelen van problemen. Belangrijk hierbij is dat de vertaling van incident naar probleem op de juiste wijze gemaakt kan worden.

Uitgangspunten

- VCO heeft in samenwerking met onze ICT-leverancier een problemmanagementproces opgesteld (C:IM.04 – Problemmanagementproces) waarin we alle vereisten vanuit het normenkader hebben opgenomen, zoals rollen en verantwoordelijkheden, identificatie en analyse.
- Problemen worden geregistreerd in een problemenregister (D:IM.04 – Problemregister).
- Eens per half jaar stellen we een rapport op (E:IM.04 - Problemrapport) dat we bespreken met het schoolbestuur, het bespreken van dit rapport is opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Het problemmanagementproces is continu en zowel reactief als proactief. Proactieve probleemidentificatie vindt plaats door middel van systematische analyse van:
  1) trends uit het incidentenregister,
  2) externe bronnen (zoals leveranciersrapportages, Kennisnet en CERT-waarschuwingen), 3) periodieke risicoanalyses.
  Dit waarborgt dat structurele fouten worden opgespoord en geminimaliseerd voordat zij tot incidenten leiden.

8 Wijzigingenbeheer

8.1 Wijzigingenbeheer

Wijzigingenbeheer, ook bekend als changemanagement, omvat het gestructureerd doorvoeren van wijzigingen in de ICT-systemen van de organisatie. Dit proces is essentieel voor het behouden van veilige en stabiele ICT en het waarborgen van de continuïteit van onderwijs- en ondersteunende processen.
Wijzigingen aan informatiesystemen en ICT-infrastructuur worden gecontroleerd getest en geaccepteerd voordat deze in productie worden genomen. Afhankelijk van de aard van de wijziging en de impact op de organisatie vindt het testen plaats binnen de eigen organisatie of bij de betreffende leverancier.

Voor wijzigingen met impact op beschikbaarheid, integriteit of vertrouwelijkheid van informatie wordt vooraf bepaald welke test- en acceptatiecriteria van toepassing zijn. Acceptatie van de wijziging vindt plaats door de daartoe bevoegde functionaris of proceseigenaar.

De overdracht van een geaccepteerde wijziging naar de productieomgeving vindt gecontroleerd plaats volgens het vastgestelde wijzigingsbeheerproces. Hierbij wordt geborgd dat uitsluitend geaccepteerde wijzigingen worden doorgevoerd en dat de continuïteit en veiligheid van de informatievoorziening behouden blijven.

Doelstellingen
Het doel van wijzigingenbeheer is:

- Voorkomen van verstoringen in onderwijs- en ondersteunende processen door wijzigingen op een gestructureerde en gecontroleerde wijze door te voeren.
- Beschermen van de ICT-systemen tegen ongeoorloofde wijzigingen en risico’s door wijzigingen zorgvuldig te beoordelen, categoriseren en testen voordat deze wordt doorgevoerd.
- Wijzigingen afhandelen volgens het door VCO formeel vastgestelde changemanagementproces voor het aanvragen, beoordelen, autoriseren en testen van wijzigingen om de betrouwbaarheid van de ICT-systemen en databeveiliging te versterken.
- Inrichten van een versnelde wijzigingsroute bij noodsituaties zodat kritieke wijzigingen snel, maar beheerst kunnen worden doorgevoerd en achteraf geëvalueerd.
- Gebruik van een representatieve en beveiligde testomgeving om wijzigingen vooraf te testen en het effect op de productieomgeving te evalueren, zodat de continuïteit en betrouwbaarheid worden gewaarborgd.

Uitgangspunten

- VCO heeft in samenwerking met onze ICT-leverancier een proces voor wijzigingenbeheer opgesteld (C:CH.01 - Changemanagementproces) waarin we de vereisten vanuit het normenkader en de samenwerking met onze ICT-leverancier nader hebben uitgewerkt.
- In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan het administreren van significante wijzigingen en de goedkeuringsprocedure.
- Instellingen van informatiebeveiligingsfuncties (bijvoorbeeld security software) op het koppelvlak tussen vertrouwde en niet-vertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.
- Binnen het changemanagementproces zijn categorieën van wijzigingen bepaald. Wijzigingen van de categorie 2 (Middel) en 3 (Groot) worden geregistreerd in een changesregister (D:CH.01 – Changeregister). Wijzigingen in de categorie 1 (Klein) worden geregistreerd als incident.
- Het wijzigingsbeheerproces (C:CH.01), inclusief de procedure voor noodwijzigingen, is formeel vastgesteld door het Bestuur, gedocumenteerd en gecommuniceerd naar alle betrokken medewerkers en de ICT-leverancier. Dit waarborgt dat alle wijzigingen op een gestandaardiseerde wijze worden behandeld
- VCO heeft voor de centrale digitale werkomgeving (zoals de cloudomgeving) geen aparte demo- of testomgeving tot haar beschikking. Aangezien het technisch beheer en de implementatie van configuratiewijzigingen zijn belegd bij de externe ICT-dienstverlener, is een eigen testomgeving niet noodzakelijk. De externe ICT-dienstverlener volgt een strikt wijzigingsbeheerproces waarbij alle configuratie-aanpassingen en updates vooraf worden getest en gevalideerd in een

gecontroleerde omgeving, alvorens deze in de productieomgeving van de organisatie worden doorgevoerd. Dit beginsel van gecontroleerde wijzigingen en voorafgaande validatie geldt tevens voor de implementatie en het beheer van alle andere cruciale applicaties en software die de organisatie afneemt van externe leveranciers.

- Voor kritieke systemen wordt, waar nodig, het gebruik van een OTAP-straat (Ontwikkeling, Test, Acceptatie en Productie) gemandateerd om de scheiding en controle van wijzigingen te waarborgen. De testomgeving is beveiligd, staat los van de productieomgeving en de toegangsregels voor de verschillende OTAP-omgevingen zijn strikt gedefinieerd.
- VCO hanteert een formeel beleid voor de overdracht van gewijzigde systemen. Hierbij wordt, waar technisch mogelijk en relevant, gebruikgemaakt van gescheiden omgevingen voor Ontwikkeling, Test, Acceptatie en Productie (OTAP). Elke substantiële wijziging behoeft een formele goedkeuring (sign-off) door de verantwoordelijke systeemeigenaar.

9 Inkoop en ingebruikname van software

9.1 Inkoop en ingebruikname van software

Bij de ontwikkeling, aanschaf en ingebruikname van software hanteert VCO een gestructureerde en risicogebaseerde aanpak. Voor alle nieuwe software en wezenlijke wijzigingen aan bestaande software geldt dat informatiebeveiliging en privacy vanaf het ontwerp en gedurende de gehele levenscyclus worden meegenomen.

Security by design, privacy by design en privacy by default vormen hierbij verplichte uitgangspunten. Indien softwareontwikkeling of -beheer is uitbesteed aan leveranciers, worden deze uitgangspunten geborgd door middel van vastgestelde eisen, contractuele afspraken en toetsing voorafgaand aan ingebruikname.

VCO hanteert een ingericht proces voor servicelevelmanagement om de kwaliteit en continuïteit van IT-diensten te bewaken. Dit proces is gericht op het structureel monitoren, evalueren en bijsturen van afgesproken serviceniveaus.

Servicelevelmanagement is gebaseerd op de vastgestelde Service Level Agreements en is organisatiebreed ingevoerd. Het proces is vastgesteld door het College van Bestuur of de schoolleiding.

De performance van IT-diensten wordt periodiek vastgelegd in een servicelevelrapport. Dit rapport geeft inzicht in de mate waarin afgesproken serviceniveaus worden gerealiseerd.

De uitkomsten van het servicelevelrapport worden, indien nodig, besproken met de IT-serviceprovider. Afwijkingen of verbeterpunten worden opgevolgd binnen het vastgestelde proces voor leveranciers- en contractmanagement.

Voor iedere nieuwe ontwikkeling, aanschaf of significante wijziging van software is voorafgaande goedkeuring vereist van het daartoe bevoegde managementniveau. Deze goedkeuring is gebaseerd op een beoordeling van risico’s, waaronder informatiebeveiliging en privacy.

Voorafgaand aan ingebruikname worden verplichte beveiligingsmijlpalen doorlopen. Deze omvatten in ieder geval een risicobeoordeling, het testen en accepteren van de software en het vastleggen van de gemaakte afwegingen en besluiten. Deze stappen maken integraal onderdeel uit van het besluitvormingsproces en kunnen niet worden omzeild.

Bewustwording op het gebied van informatiebeveiliging en privacy ondersteunt deze aanpak en is beschikbaar voor medewerkers op vrijwillige basis, passend bij hun rol en verantwoordelijkheden.

Leveranciersrisicomanagement

VCO hanteert een ingericht proces voor leveranciersrisicomanagement om risico’s die samenhangen met het uitbesteden van (cloud)diensten te identificeren, te beoordelen en te beheersen. Dit proces is organisatiebreed ingevoerd en vastgesteld door het College van Bestuur of de schoolleiding.

In het leveranciersrisicomanagementproces worden risico’s met betrekking tot de beschikbaarheid, continuïteit, beveiliging en compliance van leveranciers doorlopend geanalyseerd en, waar nodig, beperkt.

Bij het beoordelen van leveranciers wordt onder meer rekening gehouden met contractuele en organisatorische waarborgen, zoals geheimhoudingsafspraken (NDA’s), escrowvoorzieningen, de levensvatbaarheid van leveranciers, naleving van beveiligingseisen, beschikbaarheid van alternatieve leveranciers en afspraken over boetes en beloningen.

Niet-gemitigeerde of geaccepteerde leveranciersrisico’s worden periodiek gerapporteerd aan het College van Bestuur of de schoolleiding.

Contracten met leveranciers voldoen aan geldende wet- en regelgeving, waaronder privacywetgeving. Voorafgaand aan ondertekening wordt getoetst of de levering van diensten voldoet aan wet- en regelgeving en aan het eigen informatiebeveiligingsbeleid.

Interne beheersing bij derden

VCO hanteert een formeel ingericht proces om te borgen dat interne beheersmaatregelen bij externe

dienstverleners effectief worden toegepast. Dit proces is gericht op het beheersen van risico’s die samenhangen met uitbesteding van diensten en maakt onderdeel uit van het leveranciersmanagement.

De status van de interne beheersmaatregelen van externe dienstverleners wordt periodiek beoordeeld. Deze beoordeling richt zich onder meer op naleving van contractuele afspraken, beveiligingseisen en relevante wet- en regelgeving.

Voor het toezicht op externe dienstverleners zijn procedures ingericht om te controleren of contractuele verplichtingen worden nageleefd. Afwijkingen worden vastgelegd en opgevolgd, en waar nodig geëscaleerd binnen het vastgestelde leveranciers- en risicomanagementproces.

Doelstellingen

- De informatiebeveiligings- en privacy risico’s bij de inkoop en ingebruikname van software te beheersen en verminderen.
- Zorgen dat alle software aankopen voldoen aan vastgestelde standaarden voor informatiebeveiliging, privacy by design en data-integriteit.
- Goedkeuring en betrokkenheid van het management te realiseren bij inkoop van software.
- De beschikbaarheid, integriteit (kwaliteit en volledigheid) en vertrouwelijkheid van gegevens tijdens en na dataconversie en/of migratie (naar nieuwe systemen) te waarborgen.

Uitgangspunten

- Voor alle software inkopen volgt VCO het software inkoopproces (C:SD.01 - Software inkoopproces (Inkoopproces)). Dit bevat verplichte risicobeoordelingen (zoals een pre-DPIA en beoordeling van de verwerkersovereenkomst).
- Alle software inkopen moeten voldoen aan de vastgestelde standaarden. Deze standaarden zijn opgenomen in de software inkoopeisen (D:SD.01 - Software inkoopeisen).
- Voor elke software inkoop is goedkeuring vereist zoals beschreven in het software inkoopproces (C:SD.01 - Software inkoopproces (Inkoopproces)).
- Voor elke implementatie wordt een risico- en impactanalyse uitgevoerd en worden beheersmaatregelen vastgesteld. Dit proces is vastgelegd in het software implementatieproces (C:SD.01 - Software implementatieproces). Hierin is ook de naleving van de beveiligingsbaselines opgenomen (D:SM.01 - Security Baselines).
- De methodiek voor de ontwikkeling en aanschaf van software bevat verplichte, niet-te-omzeilen beveiligingsmijlpalen (Security Gates). Deze mijlpalen omvatten in ieder geval een risicobeoordeling (pre-DPIA), beveiligingstests en waar noodzakelijk een broncodebeoordeling. Deze mijlpalen moeten worden gedocumenteerd en goedgekeurd door de systeemeigenaar en de IBP'er alvorens het proces wordt voortgezet. Bij samenwerking met externe partijen stelt de organisatie consequent eisen op het gebied van Privacy by Design en Privacy by Default.
- Er is een procedure vastgesteld om de installatie van programmatuur op productiesystemen te beheersen. Alleen geautoriseerd personeel van Serve IT kan functies en software installeren of activeren.
- Er wordt alleen door de leverancier onderhouden (versie van) software gebruikt.
- Voor elke dataconversie en migratie worden beheersmaatregelen gedefinieerd en goedgekeurd door de proces- en/of systeemeigenaar om de eisen vast te stellen. Dit proces is vastgelegd in het software implementatieproces (C:SD.01 - Software implementatieproces).
- Integriteitscontroles tijdens dataconversie en migratie worden gedocumenteerd en geëvalueerd door de proces- en/of systeemeigenaar. De resultaten van deze controles moeten voldoen aan de eerder vastgestelde eisen voordat de conversie/migratie formeel wordt geaccepteerd. Dit proces is vastgelegd in het software implementatieproces (C:SD.01 - Software implementatieproces).
- Bij wijzigingen in besturingssystemen worden bedrijf kritische toepassingen beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van VCO.

10 Datamanagement

10.1 Datamanagement

Datamanagement is van groot belang voor het waarborgen van de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid (beveiliging) van gegevens binnen VCO. Het schoolbestuur is eindverantwoordelijk, terwijl proces- en systeemeigenaren zorgen voor correct beheer binnen hun domein. Het toewijzen van eigenaarschap en het classificeren van gegevens voor het juiste beschermingsniveau zijn essentieel om risico's zoals datalekken te voorkomen. De systeemeigenaar voert beveiligingsmaatregelen uit op basis van deze classificatie in opdracht van de proceseigenaar (ook wel data-eigenaar).

Het beleid en de procedures voor Datamanagement worden actief en formeel gecommuniceerd naar de gehele organisatie en zijn integraal toegepast op alle bedrijfskritische data en informatiesystemen.

Dataconversie en datamigratie

Bij dataconversies en datamigraties hanteert VCO een gecontroleerde en risicogebaseerde aanpak, gericht op het waarborgen van de juistheid, volledigheid en integriteit van gegevens. Dataconversie en datamigratie worden beschouwd als kritieke momenten binnen het datamanagementproces.

Voorafgaand aan iedere dataconversie of -migratie wordt een risico- en impactanalyse uitgevoerd om te bepalen welke beheersmaatregelen noodzakelijk zijn. Deze analyse vormt de basis voor het ontwerp van de beheersmaatregelen.

Het ontwerp van de beheersmaatregelen voor dataconversie of -migratie wordt vastgelegd en ter goedkeuring voorgelegd aan de verantwoordelijke systeem- of proceseigenaar. De uitvoering vindt uitsluitend plaats na formele aanvaarding van deze maatregelen.

De getroffen beheersmaatregelen zijn erop gericht te waarborgen dat gegevens tijdens en na de dataconversie of -migratie juist, volledig en integer zijn overgezet. Hiertoe worden passende controles uitgevoerd.

De resultaten van de uitgevoerde controles worden vastgelegd en beoordeeld door de verantwoordelijke systeem- of proceseigenaar. De dataconversie of -migratie wordt pas formeel geaccepteerd nadat is vastgesteld dat aan de gestelde eisen is voldaan.

10.2 Databeheer en verwijdering van hardware

Proces- en systeemeigenaren zijn binnen VCO duidelijk toegewezen. Zij hebben de bevoegdheid om beslissingen te nemen over beveiliging, beheer en gebruik van data en ICT-systemen. De proceseigenaren bepalen de classificatie van gegevens en systemen waarna de systeemeigenaren zorgen voor de juiste beveiligingsmaatregelen op basis van deze classificatie.

Wij gebruiken hetzelfde dataclassificatieschema voor heel VCO. Dit helpt bij het toepassen van passende maatregelen zoals toegangscontrole, archivering en versleuteling afgestemd op de gevoeligheid van de (persoons)gegevens. Hiermee kunnen we beter voldoen aan wet- en regelgeving, zoals privacywetgeving, en waarborgen we de bescherming van belangrijke gegevens van VCO en betrokkenen. Ook verkleinen we het risico op datalekken en zorgen we voor veilige opslag, verwerking en verwijdering van gegevens in lijn met de doelstellingen van onze organisatie.

Doelstelling
Het doel van databeheer is het waarborgen van de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid (beveiliging) van (persoons)gegevens binnen VCO.

Uitgangspunten

- We stellen proces- en systeemeigenaren aan en leggen dit vast in een overzicht van proces- en systeemeigenaren (D:DM.01 – Overzicht proces- en systeemeigenaren). De bestuurder is bestuurlijk eindverantwoordelijk; proces- en systeemeigenaren fungeren als data-owners. De Privacy Officer (of FG) ondersteunt, adviseert en rapporteert aan het bestuur."
- We classificeren en bepalen de technische en organisatorische maatregelen op basis van de classificatie en bijbehorende maatregelen vanuit het certificeringsschema ROSA. Deze classificatie en bescherming worden uitgewerkt in het dataclassificatieschema (D:DM.02 -

Dataclassificatieschema).
- We hebben richtlijnen voor het opslaan, bewaren en archiveren van data en persoonsgegevens. Deze richtlijnen zijn in overeenstemming met (informatie)beveiligingsbeleid, contractuele afspraken en wet- en regelgeving. Deze zijn uitgewerkt in het dataopslag overzicht (D:DM.04 - Data verwerkingsrichtlijnen), richtlijnen worden indien van toepassing ook opgenomen in de gedragscode medewerkers (D:SM.03 - Gedragscode medewerkers) en het bewustwordingsprogramma (B:HR.06 - Bewustwordingsprogramma).
- Het bewaartermijnenbeleid is formeel vastgesteld en beschrijft de processen voor het tijdig verwijderen of anonimiseren van persoonsgegevens. Waar noodzakelijk zijn specifieke procedures vastgesteld voor het verwijderen van gegevens. Het beleid en het Bewaartermijnenoverzicht worden consequent toegepast.
- We hebben een procedure opgesteld voor dataverwijdering uit applicaties (C:DM.06 - Dataverwijderingsproces voor applicaties).
- Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten, worden beveiligd opgeslagen, tenzij de vertrouwelijke informatie op de mobiele gegevensdrager voldoende versleuteld is.
- Het dataclassificatieschema (D:DM.02) is formeel vastgesteld en goedgekeurd door het Bestuur. De richtlijnen beschrijven nadrukkelijk het eigendom van data en de definities voor elk classificatieniveau
- Er is formeel overeenstemming bereikt met de proceseigenaren over de definitieve dataclassificatie van hun systemen, als basis voor het toepassen van de benodigde beheersmaatregelen

Dataverwijdering hardware
VCO hanteert formele procedures voor het verwijderen en overdragen van data en hardware, met als doel te voldoen aan organisatiedoelstellingen en toepasselijke wet- en regelgeving en om (gevoelige) data en software adequaat te beschermen.
Bij het buiten gebruik stellen, hergebruiken, overdragen of afvoeren van hardware en gegevensdragers wordt geborgd dat aanwezige data op een passende wijze wordt verwijderd, gewist of vernietigd. Dit geldt in het bijzonder voor apparatuur en media waarop vertrouwelijke of gevoelige informatie is opgeslagen.
De wijze van verwijderen of overdracht van data en hardware is afgestemd op de classificatie van de gegevens. Indien noodzakelijk worden gespecialiseerde leveranciers of verwerkers ingezet om veilige verwijdering of vernietiging te waarborgen.
De verantwoordelijkheden voor het initiëren, uitvoeren en controleren van procedures voor het verwijderen en overdragen van data en hardware zijn vastgelegd. De verantwoordelijke systeem- of proceseigenaar ziet toe op correcte uitvoering en naleving van deze procedures.

Doelstelling
Het doel van dataverwijdering hardware is gevoelige gegevens veilig en volledig te verwijderen of het vernietigen van hardware en opslagmedia, zodat deze niet in verkeerde handen kunnen komen.

Uitgangspunt
- VCO heeft in samenwerking met onze ICT-leverancier een proces vastgesteld (C:DM.06 - Dataverwijderingsproces voor hardware) om te waarborgen dat het verwijderen van data, vernietigen of overdragen van hardware volgens de noodzakelijke informatiebeveiligingseisen wordt uitgevoerd.
- Alle apparatuur van VCO die opslagmedia bevat, wordt gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en software zijn verwijderd of veilig zijn overschreven, voordat de apparatuur wordt verwijderd.
- Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij VCO/Serve IT ingeleverd. Serve IT zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is.
- Hergebruik van apparatuur buiten VCO is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode.

10.3 Gegevensuitwisseling

VCO hanteert vastgestelde beleidskaders en procedures om gegevens en software te beschermen en gecontroleerde uitwisseling van gegevens mogelijk te maken. Uitwisseling van gegevens vindt uitsluitend plaats binnen de kaders van het vastgestelde IBP-beleid en de bijbehorende richtlijnen.

Het IBP-beleid is vastgesteld door het College van Bestuur en is organisatiebreed van toepassing. Het vormt het kader voor alle vormen van gegevensuitwisseling binnen en buiten de organisatie.

Bedrijfs- en persoonsgegevens worden geclassificeerd op basis van hun vertrouwelijkheid, integriteit en beschikbaarheid. Deze classificatie is richtinggevend voor de wijze waarop gegevens worden opgeslagen, verwerkt en uitgewisseld.

Gegevens die buiten de organisatie worden uitgewisseld, worden passend beveiligd op basis van hun classificatie. Alle uitgaande e-mailverkeer van VCO wordt standaard versleuteld verzonden, zodat de vertrouwelijkheid van gegevens tijdens transport is geborgd.

Voor essentiële applicaties en gegevensuitwisselingen wordt logging toegepast. Loggegevens worden gebruikt voor monitoring en evaluatie van gegevensuitwisseling. Onjuiste, incomplete of afwijkende gegevensuitwisselingen worden gesignaleerd en opgevolgd om verdere verwerking te voorkomen en passende maatregelen te kunnen nemen.

Doelstellingen

- Zorgdragen voor de veilige uitwisseling van informatie en persoonsgegevens binnen VCO en met externe partijen.
- Minimaliseren van de kans op datalekken of misbruik van informatie.

Uitgangspunten

- We hebben een protocol opgezet voor data-uitwisseling (D:DM.05 - Protocol gegevensuitwisseling). Er zijn formele procedures vastgesteld om de uitwisseling van informatie via alle typen communicatiefaciliteiten te beschermen.
- De regels rondom uitwisseling van gegevens tussen personen is opgenomen in de gedragscode medewerkers (D:SM.03 - Gedragscode medewerkers).
- Er zijn overeenkomsten vastgesteld voor de uitwisseling van informatie en programmatuur tussen VCO en externe partijen. Hierin zijn maatregelen, verantwoordelijkheden en procedures voor incidentmelding beschreven.
- Medewerkers van VCO zijn geïnstrueerd om zodanig om te gaan met (telefoon)gesprekken, e-mail, en mobiele apparatuur dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt.
- Medewerkers zijn geïnstrueerd om geen vertrouwelijke documenten onbeheerd te laten liggen (bij de printer, in een lokaal etc.)
- Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mailberichten naar externe e-mailadressen te voorkomen.
- Informatie die een rol speelt bij elektronische berichtuitwisseling wordt op geschikte wijze beschermd, bijvoorbeeld via een (spam)filter voor e-mail.

10.4 Procesmanagement en gegevensverwerking

Procesmanagement en gegevensverwerking

Het beheer van processen waarin persoonsgegevens worden verwerkt, loopt via een systematische en gestructureerde aanpak.

- Processen met een hoog risico voor betrokkenen zijn formeel beschreven en vastgelegd. Proceseigenaren zijn aangewezen en zijn verantwoordelijk voor de periodieke evaluatie van de procesbeschrijvingen op naleving van de AVG-beginselen
- Het verwerkingsregister (bevat minimaal alle wettelijk vereiste onderdelen. De procedure voor het opzetten en actueel houden van dit register is vastgelegd in de procesbeschrijving opstellen verwerkingsregister.
- Wijzigingen en nieuwe initiatieven worden direct in het register opgenomen. De IBP'er is verantwoordelijk voor de jaarlijkse beoordeling van het register op volledigheid en actualiteit.
- VCO hanteert een vaste en consequente methode, vastgelegd in de Procesbeschrijving Pre-

DPIA, om voor alle nieuwe en sterk gewijzigde verwerkingen het risico te bepalen.

Besluitvorming: Alle DPIA-rapporten worden opgesteld volgens een gestandaardiseerd format. De procedure voor het opvolgen, behandelen of accepteren van risico’s is vastgesteld. Afwijkingen van het advies van de FG worden formeel gedocumenteerd en exclusief door het bestuur geaccepteerd.

11 Identity- & Accessmanagement

11.1 Identity- & Accessmanagement

Binnen VCO waarborgen we met Identity- en Accessmanagement (IAM) een veilige, gecontroleerde toegang tot systemen, applicaties, informatie en persoonsgegevens. Er is een toegangsbeleid vastgesteld, gedocumenteerd en beoordeeld op basis van de eisen van VCO en beveiligingseisen. Door het zorgvuldig inrichten van toegangsrechten en het actief monitoren van gebruikersactiviteiten, verkleinen we het risico op ongeoorloofde toegang en versterken we de bescherming van kritieke gegevens. IAM vormt een structureel onderdeel van ons informatiebeveiligingsproces en ondersteunt de continuïteit van het onderwijs door middel van duidelijke procedures, een autorisatiematrix en een noodtoegangsproces.

Doelstelling
Het doel van Identity- en Accessmanagement is het systematisch vastleggen, beheren en controleren van toegangsrechten.
Medewerkers krijgen uitsluitend toegang tot die systemen en gegevens die noodzakelijk zijn voor hun taken, conform het ‘need-to-know’ en ‘need-to-have’-principe.

Uitgangspunten

- Voor alle applicaties die zijn opgenomen in het overzicht van bedrijf kritische applicaties (D:GO.02), is een autorisatiematrix opgesteld door de proceseigenaar (D:ID.01). Deze matrices koppelen gebruikersrollen aan toegangsrechten op basis van functie.
- Gebruikers worden individueel geïdentificeerd, geauthentiseerd en geautoriseerd. Toegangsrechten worden niet toegekend op groepsniveau, maar altijd aan individuele medewerkers. Toegangsrechten zijn herleidbaar naar personen; rolgebaseerde toekenning is toegestaan mits gecontroleerd en gedocumenteerd in autorisatiematrix.
- Activiteiten van gebruikers zijn herleidbaar via unieke gebruikers-ID’s. Dit maakt het mogelijk om beveiligingsincidenten snel en effectief te analyseren en, indien nodig, te herstellen.
- Alle gebruikersgegevens en toegangsrechten worden beheerd in een centrale, beveiligde gebruikersdatabase (D:ID.02). Dit gebeurt volgens het centrale registratieproces (C:ID.01).
- Periodiek vindt een vergelijking plaats tussen de autorisatiematrix en de actuele gebruikersrechten. Dit gebeurt mnimaal eens per jaar, afhankelijk van de risico-inschatting. Afwijkingen worden direct gecorrigeerd. De procedure is vastgelegd in het (super)user toegangsrechtencontroleproces (C:ID.01).
- Toekennen, wijzigen of intrekken van toegangsrechten verloopt via een vastgesteld proces (C:ID.02). Hierbij is afstemming met de proces- of systeemeigenaar verplicht. Dit proces is gekoppeld aan het personeelswijzigingsproces van HR (C:HR.04).
- Voor de toekenning van toegangsrechten is altijd een formele toestemmingsprocedure vereist waarbij de data- of systeemeigenaar expliciet goedkeuring geeft. Zonder deze goedkeuring worden geen rechten verleend.
- Gebruikersrechten worden actief beheerd; rechten die gedurende een vooraf vastgestelde periode inactief zijn, worden automatisch of handmatig gedetecteerd en tijdig uitgeschakeld om misbruik te voorkomen.
- Superuserrechten worden uitsluitend toegekend volgens het formeel vastgestelde wijzigingsproces (C:ID.02). Hiervoor is goedkeuring van het de bestuurder vereist. Deze rechten zijn niet opgenomen in de reguliere autorisatiematrix, maar worden separaat geregistreerd in de gebruikersdatabase (D:ID.02).
- Het gebruik van superuserrechten wordt gelogd binnen de betreffende applicaties. Bij aanschaf van nieuwe software is logging van superuseractiviteiten opgenomen als verplicht criterium (C:SD.01).
- Voor noodsituaties is een apart noodtoegangsproces ingericht. Dit beschrijft onder welke voorwaarden tijdelijk superuserrechten aan reguliere accounts kunnen worden toegekend (C:ID.02). Evaluatie en logging zijn hier onderdeel van.

Beheer van toegangsrechten van gebruikers
Er zijn formele procedures voor registratie, autorisatie en intrekking van toegangsrechten. Gebruikers

worden vooraf geïdentificeerd; gegevens worden centraal vastgelegd. Functiescheiding en toegangsrechten zijn gebaseerd op risico's (o.a. in ParnasSys en HR2Day). Toegang is persoonsgebonden. Speciale bevoegdheden zijn beperkt tot wat nodig is. Functionele accounts zijn herkenbaar. Toegang wordt aangepast bij functiewijzigingen. Wachtwoordbeheer vindt plaats volgens een formeel proces met Serve IT.

Wachtwoordbeleid:

- Veilige uitgifte na identiteitscontrole
- Initiële en tijdelijke wachtwoorden direct vervangen
- Alleen gebruiker kent wachtwoord
- Minimaal 8 tekens
- Complexiteit:
  moet minimaal 3 van de 4 onderstaande tekens bevatten:
  - Hoofdletter
  - Kleine letter
  - Cijfer
  - Symbool
- Mag niet voorkomen op de 'Global banned password' lijst

Verantwoordelijkheden van gebruikers van VCO
Gebruikers volgen beveiligingsregels, zoals:

- Geen wachtwoorden opschrijven of delen
- Geen voorspelbare wachtwoorden
- Wachtwoord direct wijzigen bij vermoeden van misbruik
- Werkplekken worden vergrendeld bij afwezigheid. Gevoelige documenten worden beveiligd geprint (met pincode). Schermen worden automatisch vergrendeld bij inactiviteit.

Beheer van bijzondere toegangsrechten
Binnen VCO wordt het gebruik van superuserrechten als een bijzonder risico aangemerkt. Superuserrechten worden uitsluitend toegekend indien dit noodzakelijk is voor de uitvoering van taken en wanneer reguliere gebruikersrechten onvoldoende zijn.
Voor het toekennen van superuserrechten is een formele procedure ingericht. Deze procedure omvat de aanvraag, beoordeling, toekenning, vastlegging en intrekking van superuserrechten. De procedure is gedocumenteerd en organisatiebreed gecommuniceerd.
De personen aan wie superuserrechten zijn toegekend en de bijbehorende rechten worden vastgelegd. Toekenning van superuserrechten vindt uitsluitend plaats na goedkeuring door of namens het College van Bestuur, waarbij mandaatverlening mogelijk is.
Het gebruik van superuserrechten wordt gelogd. Deze loggegevens worden periodiek geëvalueerd om misbruik of ongeoorloofd gebruik te signaleren. Bevindingen worden opgevolgd conform het incidentmanagementproces.

Noodprocedure (emergency access)
Voor situaties waarin reguliere toegangsprocedures onvoldoende zijn om een incident of ernstige verstoring te verhelpen, hanteert VCO een formele noodprocedure. Deze noodprocedure is bedoeld voor uitzonderlijke situaties en wordt uitsluitend ingezet wanneer directe ingrepen noodzakelijk zijn om de continuïteit, beveiliging of beschikbaarheid van systemen en gegevens te waarborgen.
De noodprocedure beschrijft onder welke omstandigheden noodtoegang mag worden gebruikt, wie bevoegd is om deze noodtoegang te activeren en hoe dit wordt vastgelegd. De noodprocedure is gedocumenteerd en organisatiebreed gecommuniceerd.
Elk gebruik van de noodprocedure wordt geregistreerd. Hierbij wordt vastgelegd wie de noodprocedure heeft gebruikt, wanneer dit heeft plaatsgevonden en met welk doel.

Het gebruik van de noodprocedure wordt altijd geëvalueerd. Deze evaluatie omvat tevens de uitgevoerde handelingen met superuserrechten en eventuele wijzigingen van noodwachtwoorden. De evaluatie wordt vastgelegd en, indien nodig, leiden de bevindingen tot verbetermaatregelen of aanvullende beheersmaatregelen.

Toegangsbeheersing voor netwerken
Toegang wordt alleen verleend aan geautoriseerde gebruikers. Netwerkgebruik is vastgelegd in beleid. Alleen noodzakelijke netwerkdiensten zijn toegankelijk. Authenticatie voor externe toegang is vereist. Apparatuur moet geauthentiseerd zijn; BYOD-apparaten worden niet in het netwerk van VCO opgenomen. Serve IT beheert toegang tot diagnosepoorten. Niet-benodigde netwerkdiensten worden afgesloten. Informatiediensten zijn logisch gescheiden. Netwerkroutering voorkomt ongewenste datastromen en controleert bron- en bestemmingsadressen.

Toegangsbeveiliging voor besturingssystemen
Toegang verloopt via beveiligde inlogprocedures; bij kritische systemen is 2-factor authenticatie vereist. Foutieve inlogpogingen leiden tot tijdelijke blokkering. Elke gebruiker heeft een unieke ID. Authenticatie vindt plaats op basis van wachtwoord (minimaal) en alleen na verificatie van identiteit.

- Wachtwoordbeheer:
- Interactief en gecontroleerd op kwaliteit
- Initieel wachtwoord moet direct worden gewijzigd
- Zelf wijzigen vereist her-authenticatie en bevestiging
- Gebruik van systeemtools die beveiliging kunnen omzeilen is beperkt en valt onder Serve IT.

Toegangsbeheersing voor toepassingen en informatie
Toegang is beperkt conform toegangsbeleid. Extern gebruik vereist 2-factor authenticatie. Voor het beheer van kritische apparaten gebruikt Serve IT ook 2-factor authenticatie. Gevoelige systemen worden geïsoleerd in aparte omgevingen.

Draagbare computers
Draagbare apparaten zijn beveiligd tegen risico’s. Waar mogelijk wordt geen data lokaal opgeslagen. Printen in onveilige omgevingen vereist risicobeoordeling. Anti-malware blijft actueel. Bij verlies of diefstal wordt verbinding met centrale systemen geblokkeerd. Procedures zijn vastgelegd in de bruikleenovereenkomst.

Ontwikkelaars met toegang tot de productie omgeving
Medewerkers van VCO schrijven geen software welk gebruikt wordt binnen de stichting.
Mocht dit wel gaan gebeuren, dan zal hier beleid voor vastgesteld worden om de strikte scheiding van taken in de softwarelevenscyclus te waarborgen.
Onze IT leverancier voegt beleidsregels toe aan onze omgeving. Medewerkers die betrokken zijn bij de ontwikkeling van de beleidsregels, hebben geen schrijftoegang tot de productieomgeving. Het vrijgeven van software naar de productieomgeving mag uitsluitend worden uitgevoerd door speciaal geautoriseerde, onafhankelijke rollen die op hun beurt geen schrijftoegang hebben tot de ontwikkel- en testomgevingen.

12 Securitymanagement

12.1 Securitymanagement

Securitymanagement richt zich op de technische aspecten van informatiebeveiliging, waarbij risico’s met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zoveel mogelijk worden geïdentificeerd en gemitigeerd. Dit omvat onder andere het aanpakken van dreigingen en kwetsbaarheden, bescherming tegen malware, en het waarborgen van veilige informatieverwerking op mobiele apparaten.

Essentiële onderdelen van securitymanagement voor VCO zijn het implementeren van sterke authenticatiemechanismen, het correct beveiligen van mobiele apparaten en het loggen van alle systeemactiviteiten. Regelmatige beveiligingstests, zoals penetratietesten, tijdige installatie van software-updates en patches, en aandacht voor nieuwe dreigingen en kwetsbaarheden zijn eveneens cruciaal. Daarnaast is het essentieel om de ICT-infrastructuur te beschermen en te onderhouden. Cryptografische sleutels (beveiligingssleutels) moeten zorgvuldig worden beheerd bij versleuteling, netwerken moeten voorzien zijn van adequate beveiliging (zoals firewalls), en beveiligingstechnologieën dienen goed beschermd te blijven tegen bedreigingen.

De verantwoordelijkheid voor het opzetten van securitymanagement toegewezen aan de ICT-verantwoordelijke. Dit zijn de privacy officer in samenwerking met Serve IT. De ICT-verantwoordelijke voert de beveiligingsnormen uit. Sommige aspecten van securitymanagement zijn uitbesteed aan externe leveranciers, waarbij toezicht wordt gehouden via leveranciersmanagement.

De Functionaris Gegevensbescherming (FG) en de Interne Auditfunctie dragen zorg voor de periodieke, onafhankelijke toetsing op de naleving van het IBP-beleid en de vastgestelde Security Baselines

12.2 Basisbeveiliging ICT

VCO hanteert een gestructureerde aanpak voor het testen, inspecteren en het houden van toezicht op de beveiliging van systemen en netwerken. Deze aanpak is gericht op het tijdig identificeren van kwetsbaarheden en het beheersen van risico’s voor informatiebeveiliging en continuïteit.

Voor essentiële IT-componenten is een beveiligingsbaseline vastgesteld. Deze baseline beschrijft de minimale beveiligingseisen waaraan systemen en netwerken moeten voldoen en vormt het uitgangspunt voor beheer, monitoring en toetsing.

Beveiligingsmaatregelen worden periodiek getoetst door middel van controles, inspecties en testen. Waar passend worden penetratietesten en social-engineeringtesten gepland en uitgevoerd, rekening houdend met risico’s, impact en proportionaliteit.

Het testen en toezicht op informatiebeveiliging maken onderdeel uit van de reguliere beheercyclus en worden uitgevoerd binnen de kaders van het vastgestelde IBP-beleid. De uitkomsten worden vastgelegd en betrokken bij evaluaties en verbetermaatregelen.

Netwerkbeveiliging

VCO hanteert een vastgesteld netwerkbeveiligingsbeleid om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en systemen te waarborgen. Dit beleid omvat procedures, richtlijnen en documentatie voor het beheer en de beveiliging van essentiële netwerkcomponenten en wordt organisatiebreed toegepast.

Binnen de netwerkbeveiliging worden passende beveiligingstechnieken ingezet voor toegangsautorisatie, het beheersen van informatiestromen en het scheiden van netwerken en netwerkzones. Deze maatregelen zijn gericht op het beperken van ongeautoriseerde toegang en het voorkomen van ongewenste datastromen.

Bij het transport van gevoelige gegevens over niet-vertrouwde netwerken worden passende beveiligingsmaatregelen getroffen, waaronder versleuteling, om gegevens tijdens overdracht te beschermen.

De netwerkbeveiligingsmaatregelen worden periodiek beoordeeld en onderhouden als onderdeel van het reguliere beheer- en beveiligingsproces.

Doelstellingen

- Beperken van het risico van ongeoorloofde toegang tot ICT-middelen.
- Vaststellen en handhaven van beveiligingsbaselines om een consistente implementatie van beveiligingsmaatregelen te garanderen.
- Bevorderen van veilige toegang, gebruik en beheer van ICT-middelen, inclusief mobiele apparaten en thuiswerkfaciliteiten.
- Bedreigingen van malware zo veel mogelijk afweren en beheersen in geval van inbreuk.
- Tijdig signaleren van zwakheden in systemen en het nemen van bijbehorende maatregelen.

Uitgangspunten

- Als VCO hebben wij met onze ICT-leverancier beveiligingsbaselines (D:SM.01 - Security baselines) gedefinieerd. Deze zijn formeel goedgekeurd door de bestuurder en gedeeld met de ICT-afdeling en verantwoordelijken bij onze ICT-leverancier. Deze beveiligingsbaselines worden in ieder geval toegepast op onze bedrijf kritische applicaties (D:GO.01 - Overzicht van bedrijf kritische applicaties).
- De naleving van de beveiligingsbaselines controleert VCO is samenwerking met Serve IT periodiek een per half jaar door middel van het beveiligingsbaseline controle proces (C:SM.01 - Security baseline controle proces), waarbij de resultaten en eventuele afwijkingen worden beoordeeld en gedocumenteerd in een register (D:SM.01 - Security baseline register). Dit register wordt periodiek besproken met het schoolbestuur. Dit moment is opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Als er tijdens de beoordeling een afwijking als risico wordt gezien, wordt deze opgenomen in de risicoanalyse (D:RM.02 - Risicoanalyse) en worden passende maatregelen vastgesteld.
- Nieuwe ICT-infrastructuurcomponenten voldoen bij implementatie aan de beveiligingsbaselines. Bij de implementatie van software wordt hiervoor gebruik gemaakt van het software implementatieproces (C:SD.01 - Software implementatieproces), bij implementatie van hardware wordt hiervoor gebruik gemaakt van het hardware implementatieproces (C:SM.01 - Hardware implementatieproces).
- Bij alle ICT-projecten en projectmanagementprocessen wordt de implementatie van de vastgestelde beveiligingsbaselines standaard afgedwongen. Projecten kunnen niet worden afgerond (decharge) zonder validatie dat aan de baseline is voldaan.
- De mate waarin de organisatie voldoet aan de beveiligingsbaselines wordt periodiek gerapporteerd aan het schoolbestuur en de schoolleiding
- Tweefactorauthenticatie (2FA) is verplicht voor kritieke systemen en niet-vertrouwde omgevingen, tenzij anders vastgelegd na een risicoanalyse en goedkeuring van de bestuurder.
- Onze mobiele apparaten (laptops, Chromebooks, tablets, smartphones, etc.) worden beveiligd met Mobile Device Management (MDM), versleuteling en anti-malwaresoftware. Welk type MDM en antivirus software wordt toegepast per device is uitgewerkt in een overzicht (D:SM.03 - MDM en Antivirus software per device overzicht).
- Onze anti-malwaresoftware wordt centraal beheerd en up-to-date gehouden. E-mails worden gescand op malware en spam. Bewustwording rondom antivirus en -malware is opgenomen in ons Security awareness programma (B:HR.06 - Security awareness programma).
- Wij staan het werken op onbeheerde/privé devices wel toe. Indien er gewerkt wordt op een onbeheerd/privé device, dient de gedragscode ICT (D: SM.03 - Gedragscode medewerkers) voor onbeheerde devices strikt nageleefd te worden.
- Het afdrukken van bedrijfsgegevens of persoonsgegevens in niet-vertrouwde omgevingen (zoals thuiswerkplekken) is uitsluitend toegestaan nadat hiervoor een specifieke risicobeoordeling is uitgevoerd waaruit blijkt dat de vertrouwelijkheid gewaarborgd is.
- Gegevensopslag op onbeheerde/privé devices is niet toegestaan (zero footprint), dit is opgenomen in onze gedragscode ICT (D: SM.03 - Gedragscode medewerkers).
- Bij verlies of diefstal van apparaten wordt toegang tot centrale systemen onmiddellijk afgesloten nadat een melding is gedaan binnen de organisatie via het meldingsproces in de gedragscode ICT (D: SM.03 - Gedragscode medewerkers).
- Wij hebben een proces voor patchmanagement (C:SM.06 - Patchmanagement (controle) proces) waarin naast geautomatiseerde processen ook periodiek door IT-medewerkers handmatige controles worden uitgevoerd op de patchlevels van besturingssystemen, databases en

applicaties om de werking van het proces te verifiëren.
- Netwerkbeveiliging omvat segmentatie, toegangsbeheer en versleuteling van gevoelige gegevens. Netwerksegmentatie en inbraakdetectie wordt toegepast om verspreiding van malware te voorkomen. Het beheer van ons netwerk, samen met onze ICT-leverancier, is in een proces vastgelegd (C:SM.11 - Netwerkbeveiligingsbeheerproces).
- Onze beveiligingsdocumentatie wordt behandeld als vertrouwelijk en niet openbaar gemaakt.
- Onze beveiligingstechnologie is bestand gemaakt tegen manipulatie en ondersteunt robuuste wachtwoordregels.

12.3 Gedragscode IBP

De medewerkers en leerlingen van VCO vormen de eerste verdedigingslinie als het gaat om IBP. Hun gedrag, alertheid en naleving van afspraken zijn van doorslaggevend belang bij het voorkomen van beveiligingsincidenten en het beschermen van gevoelige informatie en persoonsgegevens. Daarom richt onze gedragscode zich niet alleen op het gebruik van ICT-middelen, maar ook op het versterken van het bewustzijn en de verantwoordelijkheid van iedere medewerker in het veilig omgaan met digitale middelen en gegevens.

Doelstellingen

- Voldoen aan wettelijke en organisatorische verplichtingen.
- Een werkklimaat waarin ICT op een constructieve, veilige en ethische manier wordt ingezet.
- Praktische richtlijnen gebruiken voor het dagelijks handelen van medewerkers.
- Bevorderen van bewustwording, waarbij het waarborgen van informatiebeveiliging en bescherming van (persoons)gegevens en professionaliteit centraal staan.

Uitgangspunten

- VCO heeft een gedragscode ICT opgesteld voor medewerkers (D: SM.03 - Gedragscode ICT medewerkers).
- VCO heeft een gedragscode ICT opgesteld voor leerlingen (D: SM.03 - Gedragscode ICT leerlingen).

12.4 Bewaking en toetsing van de ICT-beveiliging

Bewaking en toetsing van de ICT-beveiliging (logging), is het geautomatiseerd bijhouden van gegevens over gebeurtenissen en handelingen binnen een systeem die hebben plaatsgevonden. Logging is een essentieel proces binnen informatiebeveiliging en ondersteunt VCO bij het bewaken van de beschikbaarheid, integriteit en vertrouwelijkheid van systemen, databases en netwerkcomponenten. Het helpt bij het detecteren van ongepaste of ongebruikelijke activiteiten en draagt bij aan de uitvoering van corrigerende maatregelen.

Patchmanagement

VCO hanteert een formeel vastgesteld beleid voor patchmanagement om de beveiliging, stabiliteit en continuïteit van systemen en applicaties te waarborgen. Patchmanagement is een integraal onderdeel van het beheer van IT-systemen en draagt bij aan het tijdig verminderen van kwetsbaarheden.

Het patchmanagementproces is organisatiebreed ingevoerd en sluit aan op het vastgestelde wijzigingsbeheer. Het toepassen van patches vindt plaats volgens vastgestelde procedures, inclusief beoordeling van impact en risico’s, testen waar nodig en vastlegging van uitgevoerde wijzigingen.

Voor het identificeren en prioriteren van beveiligingspatches wordt gebruikgemaakt van relevante externe informatiebronnen over kwetsbaarheden en dreigingen, waaronder meldingen van leveranciers en andere gezaghebbende bronnen.

De status van patches en updates van essentiële systemen en applicaties wordt periodiek gecontroleerd om vast te stellen dat systemen actueel en adequaat beveiligd zijn. Bevindingen worden opgevolgd binnen het beheer- en wijzigingsproces.

Doelstellingen

- Het (vroegtijdig) detecteren van ongepaste of ongebruikelijke activiteiten binnen systemen, databases en netwerkcomponenten.

- Het identificeren van kwetsbaarheden binnen de ICT-omgeving.

Uitgangspunten

- Loggingseisen, het proces en toegepaste technieken zijn gedocumenteerd in ons formeel goedgekeurde Logging proces (C:SM.04 - Logging proces).
- We stellen de bewaartermijnen voor logging vast in lijn met wettelijke en organisatorische vereisten.
- Om alle genomen maatregelen te testen voeren wij, in samenwerking met onze ICT-leverancier, testen uit die de doorgevoerde ICT-beveiliging binnen onze organisatie controleren. Deze testen zijn uitgewerkt in ons audit & controleplan ICT- beveiliging (B: SM.05 - Audit & Controleplan ICT-beveiliging).
- Om bedreigingen, kwetsbaarheden en aanvalsvectoren zo snel mogelijk te identificeren heeft VCO, in samenwerking met onze ICT-leverancier, een ‘threat & vulnerability’ management proces ingericht (C:SM.07 - Threat & Vulnerability management proces). De ICT-leverancier gebruikt hiervoor o.a. tools voor penetratietesten en kwetsbaarheidsscans, welke betrouwbare bronnen zoals SchoolCERT-adviezen meenemen in de beoordeling.
- Wij voeren ook social enigineeringtesten uit in de vorm van bijvoorbeeld mystery guests en/of phishingmail campagnes. Deze organisatiebrede testen zijn opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Alle risico’s die vanuit threat & vulnerability management, penetratietesten, social engineeringtesten, beveiligingstesten en logging analyses volgen, worden opgenomen in de organisatiebrede IBP risicoanalyse (D:RM.02 - Risicoanalyse).
- Wij controleren periodiek de kwaliteit van onze logging. Incorrecte, onvolledige of gebrekkige logging wordt als incident gedocumenteerd, geanalyseerd en opgevolgd met corrigerende maatregelen om de traceerbaarheid te herstellen.

12.5 ICT-infrastructuur

Een veilige en betrouwbare ICT-infrastructuur is onmisbaar voor de continuïteit van ons onderwijs en de ondersteuning van leerlingen en medewerkers. VCO richt zich op het invoeren en waarborgen van interne beheers-, beveiligings- en auditmaatregelen tijdens de configuratie, integratie en het onderhoud van hardware en infrastructuursoftware. Door verantwoordelijkheden helder te definiëren, processen zorgvuldig te beheren en een strategisch onderhoudsplan te hanteren wordt de beschikbaarheid, integriteit en vertrouwelijkheid van de infrastructuur geborgd.

VCO hanteert een duidelijk gedefinieerd en organisatiebreed toegepast proces voor het onderhoud van de IT-infrastructuur. Dit proces is gericht op het waarborgen van de beschikbaarheid, betrouwbaarheid en beveiliging van systemen en netwerken die essentieel zijn voor de bedrijfsvoering.

Het onderhoudsproces is afgestemd op het vastgestelde wijzigingsbeheer. Onderhoudswerkzaamheden die impact hebben op de werking of beschikbaarheid van systemen worden uitgevoerd binnen de kaders van het wijzigingsbeheer en zijn onderdeel van de reguliere beheercyclus. Dit beleid is vastgesteld door het College van Bestuur.

Bij het plannen en uitvoeren van onderhoud wordt rekening gehouden met de behoeften van essentiële businessapplicaties en met de geldende IT- en organisatiedoelstellingen. Onderhoudswerkzaamheden dragen bij aan het ondersteunen van continuïteit en de strategische doelstellingen van de organisatie.

Onderhoudswerkzaamheden worden gepland, ingeroosterd en gecoördineerd om verstoringen te beperken en de beschikbaarheid van systemen te waarborgen.

Documentatie van systeemsoftware en infrastructuur wordt onderhouden en periodiek geactualiseerd, waarbij gebruik wordt gemaakt van actuele leveranciersdocumentatie en beheergegevens.

Doelstellingen

- Het beschermen van de beschikbaarheid, integriteit, vertrouwelijkheid en veiligheid van de ICT-infrastructuur en al haar componenten.
- Het opzetten van een onderhoudsstrategie dat risico’s minimaliseert.
- Zorgen dat de beveiliging in lijn is met de behoeften van VCO.

Uitgangspunten

- Het proces voor bescherming en beschikbaarheid van de ICT-infrastructuur (C:SM.08 - Beschikbaarheid en bescherming van ICT-infrastructuur proces) is samen met onze ICT-leverancier helder gedefinieerd, goedgekeurd door het schoolbestuur en breed bekendgemaakt.
- Er is een onderhoudsstrategie (C:SM.09 - Onderhoud ICT-infrastructuurproces) ontwikkeld voor onze ICT-infrastructuur die risico’s minimaliseert en de continuïteit van de ICT-omgeving ondersteunt.
- De systeemdocumentatie van onze infrastructuur wordt structureel onderhouden en periodiek geactualiseerd, waarbij wijzigingen en updates vanuit leveranciersdocumentatie consistent worden verwerkt voor alle systemen
- De scheiding van test- en productieomgevingen van de IT-infrastructuur is contractueel geborgd via de Service Level Agreement (SLA) met onze ICT-leverancier. De leverancier is verantwoordelijk voor het strikt gescheiden houden van de Ontwikkel-, Test-, Acceptatie- en Productieomgeving (OTAP) en het alleen installeren van geteste applicatiesoftware in de productieomgeving.

12.6 Cryptografische sleutels

Cryptografie (het versleutelen van gegevens) speelt een belangrijke rol in het beschermen van informatie en (persoons)gegevens binnen VCO. Door gegevens te versleutelen wordt voorkomen dat onbevoegde partijen toegang krijgen tot gevoelige informatie. Cryptografische sleutels zijn essentieel voor het versleutelen en ontsleutelen van gegevens en vormen daarmee de kern van een veilige digitale communicatie-infrastructuur.

Doelstelling
Het doel van cryptografische sleutels is het beheer ervan zorgvuldig te organiseren en risico's op ongeoorloofde toegang en aanpassingen van (persoons)gegevens te beperken.

Uitgangspunten

- Als VCO maken wij geen gebruik van cryptografische sleutels in eigen beheer, alle versleutelde communicatie is uitbesteed aan derde partijen die dit binnen hun eigen omgeving georganiseerd hebben.
- Wij volgen het proces (C:SM.10 - Cryptografische sleutel beheerproces) van de aanbieder 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. Wij toetsen of dit proces voldoet aan gestelde veiligheidsnormen.
- De geldigheidsduur van sleutels wordt bepaald aan de hand van de beoogde toepassing.

13 Fysieke beveiliging

13.1 Fysieke beveiliging

Fysieke beveiliging in het kader van IBP gaat over de bescherming van gebouwen en specifieke ruimtes binnen de scholen. Omdat onze scholen een open karakter hebben is het essentieel om gevoelige of kritieke ruimtes extra te beveiligen. Dit geldt onder andere voor ruimtes waar fysieke dossiers van medewerkers en (oud-)leerlingen worden bewaard en voor de server-, printer-, modem- of patchruimtes of ruimte(s) waar cameratoezicht wordt uitgevoerd. Door het invoeren van passende maatregelen kan de veiligheid van (persoons)gegevens en de continuïteit van bedrijfsprocessen worden gewaarborgd.

Dit beleid is alomvattend en op risico’s gebaseerd en wordt ondersteund door fysieke en technische toegangscontrolesystemen om de bescherming van medewerkers, leerlingen, leveranciers en bezoekers te garanderen. Het beleid omvat ook de richtlijnen voor incidentrespons en -rapportage met betrekking tot fysieke beveiligingsincidenten.

13.2 Fysieke beveiligingsmaatregelen

VCO heeft fysieke beveiligingsmaatregelen ingevoerd voor ruimtes met gevoelige informatie of ICT-componenten. Deze maatregelen beperken risico’s zoals onbevoegde toegang, diefstal, brand, waterschade en stroomuitval. Zodat de beschikbaarheid en integriteit van ICT-componenten en gegevens gewaarborgd worden en er snel gereageerd kan worden bij incidenten.

Doelstellingen

- Het voorkomen, detecteren en beperken van (de effecten van) risico's zoals diefstal, onbevoegde toegang en calamiteiten (brand, waterschade, stroomuitval etc.).
- Het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van ICT-componenten en gevoelige informatie en/of persoonsgegevens.
- Het ondersteunen van een veilige leer- en werkomgeving voor alle betrokkenen binnen VCO.

Uitgangspunten

- We voeren periodiek risicoanalyses (D:RM.02 - Risicoanalyses) uit en deze zijn onderdeel van het VCO-brede risicomanagement.
- Op basis van de risicoanalyse nemen we effectieve maatregelen om bedreigingen zoals diefstal, brand, waterschade en vandalisme te voorkomen en nemen deze op in de risicoanalyses (D:RM.02 - Risicoanalyses).
- De basis voor de fysieke beveiliging wordt gevormd door het beleid fysieke toegangsrechten, goedgekeurd door het Bestuur, dat de uitgangspunten biedt voor alle genomen technische en organisatorische maatregelen. Dit beleid is uitgewerkt in het fysieke beveiligingsreglement (D:PH.01 - Fysieke beveiligingsreglement), hierin zijn de verantwoordelijkheden en eigenaarschap voor fysieke beveiliging gedefinieerd.
- Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst, welke jaarlijks wordt gecontroleerd.
- De status van fysieke beveiligingsmaatregelen (E:RM.02 – (rest)Risico rapport) wordt periodiek gerapporteerd aan de bestuurder.
- De (school)gebouwen bieden voldoende weerstand bij inbraak en vandalisme. Er zijn toegangsbeveiligingen (barrières zoals muren, afsluitbare deuren) aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.
- Fysieke beveiligingsmaatregelen zijn passend voor de organisatie en worden actief meegewogen vanaf de eerste fase van een eventuele verhuizing of verbouwing, waarbij rekening wordt gehouden met ontwerp- en certificeringseisen voor zonering en controle.

13.3 Beheer van fysieke toegangsrechten

De fysieke toegang tot kritieke ICT-ruimtes binnen VCO hebben we vastgelegd in richtlijnen voor toegangsbeheer, beveiligingsmaatregelen en monitoring om risico’s te minimaliseren en de continuïteit van ICT-processen te garanderen.

Doelstellingen

- Effectief beperken van risico's zoals onbevoegde toegang, misbruik of calamiteiten effectief te beperken.
- De fysieke toegang tot kritieke ICT-ruimtes strikt reguleren en bewaken, zodat alleen geautoriseerde personen toegang krijgen op basis van hun functie.
- Toegangsadministratie en -controle waarborgen door middel van formele procedures en technische beveiligingsmaatregelen.
- Naast het effectief beperken van risico's, richt dit beheer zich op het waarborgen van de formele procedures voor de administratie van fysieke toegangsprofielen en het periodiek controleren van de toegangsrechten om te garanderen dat deze up-to-date zijn.

Uitgangspunten

Als VCO zien wij de volgende ruimtes als kritieke ICT-ruimte of beveiligingsobject:

- Ruimte(s) waar zich ICT-apparatuur bevindt: laptops, servers, patchkasten, camerasystemen, modems, switches, meterkast, alarminstallatie, brandmeldinstallatie en printer.
- Ruimte(s) waar persoonsgegevens van leerlingen en/of medewerkers of andere gevoelige informatie (zoals financiële gegevens) worden bewaard.
- Kast(en) in lokalen waar persoonsgegevens van leerlingen en/of medewerkers worden bewaard.
- Per locatie is er een overzicht van de genoemde ruimtes, deze gebruiken we als basis voor alle fysieke beveiligingsprocessen en -registers.
- Toegang tot ruimtes met gevoelige informatie en/of persoonsgegevens of ICT-componenten worden geregistreerd volgens het registratie fysieke toegangsproces (C:PH.02 - Registratie fysieke toegangsproces). De registratie van alle toegang tot ICT-kritieke ruimtes, inclusief die van bezoekers en leveranciers, wordt geregistreerd in het toegang tot ICT-kritieke ruimte/beveiligingsobjecten register (D:PH.02 - Toegang tot ICT-kritieke ruimte/beveiligingsobjecten register).
- Er is een formeel proces ingevoerd om alle toegangen tot fysieke IT-omgevingen te controleren en te bewaken, waarbij alle bezoekers, inclusief leveranciers en onderhoudsmedewerkers, worden geregistreerd in het logboek.
- Het proces voor het verlenen, wijzigen en intrekken van toegangsrechten hebben we vastgelegd (C:PH.02 - Toekennen en intrekken fysieke toegangsrechten proces). Toekenning en intrekking van (nieuwe) toegangsrechten wordt schriftelijk geadministreerd in het fysieke toegangsrechtenregister (D:PH.02 - Fysieke toegangsrechten register).
- Toegang wordt verleend via beveiligingsmaatregelen die zijn vastgesteld op basis van de risicoanalyse (D:RM.02 - Risicoanalyses).
- Aanvullende fysieke beveiligingsmaatregelen, worden op basis van een risicoanalyse (PH.01) ingevoerd.

13.4 Cameratoezicht

VCO zet cameratoezicht in om de veiligheid van leerlingen, medewerkers, bezoekers en eigendommen te waarborgen. Het kan een effectieve manier bieden om ongewenst gedrag te voorkomen (preventie) en incidenten zorgvuldig te registreren (afhandeling). Tegelijkertijd is het belangrijk om zorgvuldig om te gaan met de privacy van alle betrokkenen.

Doelstelling
Het doel van cameratoezicht is om de veiligheid van leerlingen, medewerkers, bezoekers en eigendommen te waarborgen. En dit toe te passen het conform de geldende wet- en regelgeving (zoals de AVG). Het toepassen van cameratoezicht vraagt noodzakelijke technische en organisatorische maatregelen.

Uitgangspunten

- Voordat cameratoezicht wordt ingezet heeft VCO een DPIA uitgevoerd om te bepalen of cameratoezicht is toegestaan.
- Voor de ingebruikname van cameratoezicht stellen we als organisatie een cameratoezichtreglement op (D:PH.01 - Cameratoezicht reglement), dat invulling geeft aan de te treffen technische en organisatorische maatregelen.

14 ICT-operatie

14.1 ICT-operatie

ICT-operatie omvat standaard ICT-beheeractiviteiten, namelijk: Jobprocessing en back-up & herstel. De ICT-beheeractiviteiten zijn van belang om het onderwijs te (blijven) ondersteunen.

De prestaties en capaciteit van de ICT-infrastructuur worden continu bewaakt. Op basis van geautomatiseerde rapportages wordt gestuurd op beschikbaarheid en toekomstige capaciteitsbehoeften, zodat de onderwijscontinuïteit niet in het geding komt.

Doelstellingen

- Het veilig en gecontroleerd uitvoeren van geautomatiseerde jobprocessing en data-uitwisselingen.
- Het waarborgen van de beschikbaarheid en integriteit van back-ups om dataverlies bij incidenten te minimaliseren.

Uitgangspunten

- Geautomatiseerde jobprocessing wordt door onze ICT-leverancier uitgevoerd op basis van een formeel runbook afgestemd met systeem- of proceseigenaren. Alle runbooks worden op één plek bewaard en opgenomen in het overzicht van job scheduling (D:OP.01 - Overzicht van job scheduling).
- Afwijkingen of storingen in jobprocessing worden actief gemonitord, geregistreerd en opgelost via het incidentmanagementproces van ons en van onze ICT-leverancier.
- De back-up van cloudapplicaties worden geregeld door de desbetreffende leverancier van de applicatie. De eisen rondom back-ups zijn opgenomen in onze inkoopeisen ICT (D:SD.01 - Software inkoopeisen). Er is één uitzondering en dat betreft de back-up van onze Microsoft365 omgeving. De back-up voor deze omgeving wordt uitgevoerd door onze ICT-leverancier.
- In overleg met de proces- en systeemeigenaren is bepaald welke data van deze omgeving wordt geback-upt. In geval van onze organisatie is dat:
    - medewerkers Entra-data
    - medewerkers Drive/User-data
    - De back-up wordt minimaal één keer per dag gemaakt
- De back-up en herstelprocessen zijn door VCO in samenwerking met de ICT-leverancier opgesteld en vastgelegd in het back-up- en herstelproces (C:OP.02 - Back-up- en herstelproces). Hierin is tevens opgenomen wie welke verantwoordelijkheid heeft tijdens dit proces.
- De jobprocessing en interfacebewaking worden centraal beheerd door onze ICT-leverancier. Dit beheer omvat tevens de interfacebewaking en de correlatie tussen verschillende systemen om verstoringen in de datastromen vroegtijdig te signaleren.
- Uitzonderingen of afwijkingen in de jobprocessing worden geregistreerd en opgelost via het incidentmanagementproces van ons en van onze ICT-leverancier.
- Back-ups worden periodiek getest door onze ICT-leverancier en gezamenlijk geëvalueerd. Waar nodig worden maatregelen genomen om de back-up volledig aan de organisatie-eisen te laten voldoen.
- De back-up en herstelprocessen, vastgelegd in C:OP.02, zijn formeel goedgekeurd door het schoolbestuur en zijn in lijn met de behoeften van de organisatie en de beveiligingseisen.
- In overleg met de proces- en systeemeigenaren is de prioriteit voor dataherstel bepaald. Deze prioriteit is gebaseerd op de eisen uit het Bedrijfscontinuïteitsplan (BCP) en de continuïteit van IT-diensten.

Capacity- en performancemanagement
Capacity- en performancemanagement maken geen onderdeel uit van de ICT-operatie omdat we als VCO geen servers zelf beheren.

- Hoewel VCO zelf geen servers beheert, wordt Capacity- en Performancemanagement in de dienstverlening van de ICT-leverancier contractueel afgedwongen (zie Ketenbeheer). De leverancier is verplicht tot het definiëren, invoeren en centraal bewerken van de raw performance metrics op infrastructuurniveau.
- Op basis van deze metrics stelt de ICT-leverancier geautomatiseerde periodieke rapportages op.

Deze rapportages maken het signaleren van trends en problemen mogelijk en geven inzicht in toekomstige capaciteitsbehoeften, ten behoeve van de sturing door VCO

15 Bedrijfscontinuïteitsmanagement

15.1 Bedrijfscontinuïteitsmanagement

Bedrijfscontinuïteitsmanagement (BCM) binnen het onderwijs richt zich op het waarborgen van de continuïteit van het primaire proces – het verzorgen van onderwijs – en op het beperken van de impact van calamiteiten, zoals ransomware-aanvallen of natuurrampen. Het doel is onderbreking van het onderwijsproces tegen te gaan en kritische bedrijfsprocessen te beschermen.

In dit hoofdstuk spreken we over:
BIA > Bedrijfsimpactanalyse
Het identificeren van kritieke bedrijfsprocessen en de impact van verstoringen daarop.

RTO > Recovery Time Objective
De maximale acceptabele tijdsduur waarbinnen een kritiek proces na een verstoring hersteld moet zijn.

BCP > Bedrijfscontinuïteitsplan
Het gedocumenteerde plan met procedures om essentiële processen tijdens en na een grote storing voort te zetten.

BCM > Bedrijfscontinuïteitsmanagement
Het totale proces om verstoringen te voorkomen en te zorgen voor herstel van kritieke bedrijfsprocessen.

15.2 Bedrijfscontinuïteitsplan

Het Business- en ICT-continuïteitsplan (BCP) is ontwikkeld om de impact van grote verstoringen op bedrijfsprocessen en kritieke ICT-services te minimaliseren. Het plan biedt een risicogericht kader met scenario’s, richtlijnen, rollen en maatregelen om effectief te reageren op incidenten en de gevolgen daarvan te beperken. Een goed ingericht BCP zorgt voor een snelle en gecoördineerde respons bij incidenten, zodat het primaire proces op zo kort mogelijke termijn kan worden hersteld.

Doelstellingen

- Het minimaliseren van de gevolgen van grote verstoringen op bedrijfsprocessen en ICT-services.
- Zorgen voor alternatieve verwerkings- en herstelmogelijkheden voor kritieke ICT-services om de continuïteit van het onderwijsproces te waarborgen.
- Het inrichten van een gestructureerde en gecoördineerde aanpak voor incidentrespons en snel herstel van de dienstverlening.

Uitgangspunten

- Ons bedrijfs- en ICT-continuïteitsplan (B:BC.01 - Bedrijfs- & ICT- continuïteitsplan), gebaseerd op een bedrijfsimpact analyse, is gedocumenteerd, geïntegreerd en goedgekeurd door de bestuurder.
- Een belangrijk onderdeel van ons BCP is een crisisplan (B:BC.05 - Crisisplan) dat onze organisatie in staat stelt essentiële bedrijfsactiviteiten voort te zetten terwijl het crisisteam de crisis beheert.
- Periodiek, eens per jaar, voeren we een crisisoefening uit om de effectiviteit van de plannen te toetsen en te evalueren. Evaluaties van oefeningen leiden tot verbeteringen van de plannen. De crisisoefening is opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Het BCP is formeel goedgekeurd door het schoolbestuur en is gebaseerd op een uitgevoerde Bedrijfsimpactanalyse (BIA).
- Op basis van de BIA zijn Recovery Time Objectives (RTO’s) bepaald, die als leidraad dienen voor het herstelplan.
- Alle betrokkenen zijn op de hoogte van hun rollen en verantwoordelijkheden tijdens een crisis, vastgelegd in het crisisplan (dat onderdeel is van het BCP).

15.3 Technische en organisatorische maatregelen voor BCM

Bedrijfs- en ICT-continuïteitsplannen zijn essentieel om verstoringen in kritieke systemen en diensten effectief te kunnen herstellen. Regelmatige tests van deze plannen zorgen ervoor dat eventuele

tekortkomingen worden geïdentificeerd en aangepakt zodat de plannen betrouwbaar en actueel blijven. Bovendien waarborgt zorgvuldig beheer van back-upmedia, documentatie en andere ICT-resources een snelle beschikbaarheid van essentiële gegevens en herstelopties in geval van calamiteiten.

VCO zorgt voor het veilig opslaan van back-ups van kritieke systemen en gegevens op een locatie buiten de primaire bedrijfsomgeving. Offsite back-upopslag is onderdeel van het continuïteitsmanagement en draagt bij aan het herstel van systemen en gegevens bij calamiteiten.

Er is een actueel overzicht van de kritieke back-ups die offsite worden opgeslagen. Dit overzicht is vastgesteld door het College van Bestuur of de schoolleiding en wordt periodiek beoordeeld.

Voor de offsite opslag van back-ups zijn passende beheersmaatregelen ingericht. Deze omvatten onder meer afspraken over opslaglocatie, beveiliging, transport, labeling, herstelinstructies en het beheer van voorraadlijsten van back-upmedia. Het management heeft inzicht in deze beheersmaatregelen.

De offsiteregeling voor back-ups is afgestemd op de vereisten voor bedrijfscontinuïteit en wordt periodiek geëvalueerd. Bevindingen uit evaluaties worden betrokken bij verbetermaatregelen.

Datareplicatie is het proces waarbij gegevens real-time worden gekopieerd en gesynchroniseerd tussen verschillende databases, servers en/of locaties. Binnen de applicaties binnen beheer van VCO passen wij datareplicatie niet toe. Waar nodig wordt dit voor onze kritieke systemen wel opgenomen in de inkoopeisen.

Doelstellingen

- Het regelmatig testen van het BCP om zeker te stellen dat essentiële systemen en diensten effectief kunnen worden hersteld.
- Het verbeteren van het BCP op basis van testresultaten.
- Samenwerking tussen proces- en systeemeigenaren voor het bepalen van de inhoud en vorm van de back-ups gebaseerd op de wensen van VCO en ICT-beveiligingsnormen.

Uitgangspunten

- Periodiek testen we ons bedrijfs- en ICT-continuïteitsplan (B:BC.02 - BCP testplan) via goedgekeurde, geïntegreerde test-/herstelscenario’s. De BCP test is opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).
- De jaarlijkse testen omvatten geïntegreerde testscenario’s en, cruciaal, geïntegreerde leverancierstests met Serve IT, waarbij de vastgestelde RTO's uit de BIA worden gevalideerd
- Na elke test rapporteren we de resultaten en worden, indien nodig, maatregelen opgesteld en uitgevoerd (E:BC.02 - BCP test & maatregelen rapport) om tekortkomingen te verhelpen.
- Alle noodzakelijk geachte kritieke back-upmedia wordt off-site opgeslagen in overeenstemming met het beleid voor dataclassificatie. De inhoud en vorm van off-site opslag (D:BC.03 - Inhoud en vorm back-up) wordt vastgesteld in samenwerking tussen de proceseigenaren en systeemeigenaren en bijgehouden.
- Het gedetailleerde overzicht van alle kritieke offsite back-upmedia is vastgesteld door het bestuur.
- De beheerder is verplicht de beheersmaatregelen voor de opslagfaciliteit te documenteren (inclusief transport, herstelinstructies, labelen) en periodiek te evalueren.
- De essentiële financiële en operationele data die gerepliceerd moeten worden om de RTO's te halen, zijn vastgesteld en goedgekeurd door het schoolbestuur. Waar besloten is om replicatie niet toe te passen, is dit gebaseerd op de geaccepteerde RTO uit de BIA.
- De essentiële financiële en operationele data die gerepliceerd moeten worden om de RTO's te halen, zijn vastgesteld en goedgekeurd door het schoolbestuur. De beslissing tot non-replicatie, indien van toepassing, is een bewuste risico-acceptatie op basis van de BIA.

16 Ketenbeheer

16.1 Ketenbeheer

VCO maakt voor de levering van IT-diensten gebruik van externe ICT-dienstverleners. Ketenbeheer richt zich op het beheersen van uitbestede ICT-diensten, zoals SaaS-oplossingen, die veel voordelen bieden maar ook de controle beperken. Het is belangrijk om duidelijke afspraken te maken met leveranciers over minimale beveiligingseisen, vastgelegd in eisen ten aanzien van de Service Level Agreement (SLA). Het beheer van deze afspraken uit zich in het periodiek controleren of de afspraken uit de SLA worden nageleefd, in de vorm van Service Level Management (SLM). Het beheersen van risico's richting onze leveranciers, krijgt vorm door Leveranciersrisicomanagement (LRM) toe te passen. Toetsing van de beveiligingsmaatregelen van leveranciers is het laatste onderdeel van ketenbeheer.

Doelstellingen

- Vaststellen van duidelijke afspraken met ICT-leveranciers over serviceniveaus en ondersteuningsactiviteiten.
- Periodieke monitoring en rapportage van de prestaties van ICT-diensten, inclusief afwijkingen en verbetermaatregelen.
- Minimaliseren van risico's door effectief leveranciersrisicomanagement en naleving van wet- en regelgeving.
- Waarborgen dat leveranciersdiensten voldoen aan beveiligingseisen en bedrijfscontinuïteitsdoelen.
- Het beveiligen en handhaven van de informatie en ICT-voorzieningen van VCO waartoe externe partijen toegang hebben

Uitgangspunten

- Onze serviceniveaus zijn gebaseerd op de behoeften van VCO en vastgelegd in een SLA. Hiervoor hebben wij een door de bestuurder vastgestelde standaard SLA opgesteld (D:SC.01 - Standaard SLA). De inhoud van de SLA wordt per ICT-oplossing waar nodig aangevuld met oplossing specifieke eisen. De serviceniveaus en de SLA zijn opgenomen in het Programma van Eisen (PvE) (B:SD.01 - Software inkoopeisen) binnen het software inkoopproces (C: SD.01 - Software inkoopproces).
- ICT-leveranciers dienen te voldoen aan de overeengekomen contractuele verplichtingen, wet- en regelgeving en interne beveiligingsnormen. De gemaakte afspraken worden periodiek geëvalueerd volgens ons SLM-proces (C: SC.02 - SLM-proces). Van deze evaluatie wordt een SLM-rapport opgesteld (E:SC.02 - SLM rapport).
- Leveranciersrisicomanagement maakt onderdeel uit van ons bredere IBP-risicomanagementproces (D:RM.02 - Risicoanalyses). Binnen onze software inkoopeisen (B:SD.01 - Software inkoopeisen) worden geïdentificeerde risico's meegenomen in het PvE en meegenomen in de beoordeling van ICT-leveranciers.
- De risico's voor de informatie en ICT-voorzieningen van VCO vanuit processen waarbij externe partijen betrokken zijn, worden geïdentificeerd en beheersmaatregelen worden genomen voordat toegang wordt verleend.
- ICT-Leveranciers dienen te voldoen aan de overeengekomen contractuele verplichtingen, wet- en regelgeving en interne beveiligingsnormen. De status van interne beheersmaatregelen van leveranciers wordt indien er sprake is van een "hoog risicoverwerking" periodiek (eens per drie jaar) geëvalueerd door middel van een DPIA.

Uitwerking
Service Level Agreements
VCO stelt voor IT-diensten minimale eisen aan serviceniveaus die zijn gebaseerd op de continuïteit van het primaire onderwijsproces en de ondersteunende bedrijfsvoering. Deze eisen hebben in ieder geval betrekking op beschikbaarheid, incidentafhandeling, prestaties, continuïteit, informatiebeveiliging en rapportage.
Bij het aangaan van overeenkomsten worden deze serviceniveaus vastgelegd in een SLA of SLA-bijlage, die integraal onderdeel uitmaakt van de contractuele afspraken met de ICT-dienstverlener.

SLA’s worden formeel vastgesteld door het College van Bestuur en overeengekomen met de leverancier. De inrichting van het inkoop- en contracteringsproces is vastgelegd in het inkoopbeleid van VCO.

Servicelevelmanagement
De naleving van afgesproken serviceniveaus wordt periodiek beoordeeld via servicelevelmanagement. Hierbij worden rapportages van leveranciers (SLR’s) en interne bevindingen gebruikt om de daadwerkelijk geleverde prestaties te toetsen aan de gemaakte afspraken.
Afwijkingen worden vastgelegd en besproken met de leverancier. Indien nodig worden corrigerende maatregelen afgesproken of geëscaleerd. De resultaten van het servicelevelmanagement worden gebruikt voor evaluatie van de dienstverlening en het bijstellen van afspraken. Structurele of ernstige afwijkingen worden gerapporteerd aan het bestuur.

Leveranciersrisicomanagement
VCO past leveranciersrisicomanagement toe om risico’s te beheersen die samenhangen met de inzet van externe leveranciers en (cloud)diensten. Hierbij wordt onder meer gekeken naar continuïteit, informatiebeveiliging, privacy, compliance met wet- en regelgeving en afhankelijkheden.
Vastgestelde risico’s worden vastgelegd en waar mogelijk gemitigeerd door contractuele afspraken, aanvullende maatregelen of organisatorische beheersmaatregelen. Niet-gemitigeerde of geaccepteerde risico’s worden periodiek betrokken in de rapportage aan het management of bestuur.

Interne beheersing bij derden
VCO borgt dat externe dienstverleners voldoen aan de overeengekomen contractuele en beveiligingseisen. De werking van beheersmaatregelen bij leveranciers wordt periodiek beoordeeld op basis van contractafspraken, rapportages en evaluaties.
Bij beëindiging van een contract zorgt VCO voor een gecontroleerde en sluitende afwikkeling. Alle logische en fysieke toegangen worden ingetrokken. De leverancier verstrekt een schriftelijke verklaring waaruit blijkt dat persoonsgegevens en overige data van VCO zijn verwijderd of vernietigd conform de afspraken in de verwerkersovereenkomst en de AVG.

17 Bijlagen

17.1 Bijlagen

Bijlagen

1. Privacy reglement
2. Overzicht van activiteiten per rol
3. Begrippenlijst informatiebeveiliging

18 IBP-processen

18.1 IBP-processen

Het schoolbestuur is verantwoordelijk voor het zorgvuldig omgaan met persoonsgegevens en het waarborgen van de bescherming daarvan. Om deze verantwoordelijkheid aantoonbaar en beheersbaar in te vullen, zijn binnen VCO IBP-processen ingericht.

De IBP-processen beschrijven op samenhangende wijze hoe binnen de organisatie wordt omgegaan met persoonsgegevens en privacy-risico’s. Deze processen ondersteunen het schoolbestuur bij het verkrijgen en behouden van overzicht over gegevensverwerkingen en bij het naleven van wet- en regelgeving op het gebied van privacy en gegevensbescherming.

De IBP-processen vormen de verbinding tussen het vastgestelde beleid en de dagelijkse uitvoering. Zij maken inzichtelijk op welke wijze privacy structureel is geborgd binnen de organisatie en hoe wordt toegezien op correcte toepassing, toetsing en verantwoording.

De IBP-processen worden vastgelegd, actueel gehouden en periodiek beoordeeld. Waar nodig worden zij aangepast naar aanleiding van wijzigingen in wet- en regelgeving, organisatorische veranderingen of bevindingen uit evaluaties en toezicht.

Doel
Ervoor zorgen dat iedereen binnen VCO weet welke rol hij of zij heeft in de bescherming van persoonsgegevens, wie verantwoordelijk is voor welke taken en wie nog geraadpleegd moet worden bij privacyvraagstukken.

Uitgangspunten
1. Heldere rolverdeling: het schoolbestuur is eindverantwoordelijk; de Privacy Officer / IBP-adviseur en systeem- of proceseigenaren voeren het beleid operationeel uit.

2. Adviserende en toezichthoudende rol FG: de Functionaris Gegevensbescherming (FG) heeft de wettelijke taken en werkt nauw samen met het bestuur en de IBP-organisatie.

3. Rapportage: rollen zijn beschreven, verantwoordelijkheden gedocumenteerd, en er is structurele terugkoppeling (bijv. via jaarrapport FG).

18.2 Operationele processen in kaart

Om uitvoering te kunnen geven aan het IBP-beleid en de bijbehorende IBP-processen, brengt VCO de operationele processen waarin persoonsgegevens worden verwerkt systematisch in kaart. Dit betreft alle processen waarin persoonsgegevens worden verzameld, geraadpleegd, vastgelegd, gewijzigd, verstrekt of verwijderd.

Het in kaart brengen van operationele processen maakt inzichtelijk:

- welke persoonsgegevens binnen de organisatie worden verwerkt;
- voor welke doelen deze verwerkingen plaatsvinden;
- welke systemen en applicaties hierbij worden gebruikt;
- welke functionarissen en externe partijen bij de verwerking betrokken zijn.

Dit overzicht vormt een noodzakelijke basis voor verdere privacybeheersing binnen de organisatie. De in kaart gebrachte processen worden gebruikt bij het bijhouden van het register van verwerkingen, het uitvoeren van (pre-)DPIA’s en het toepassen van Privacy by Design en Privacy by Default.

De operationele processen worden actueel gehouden. Wijzigingen in processen, systemen of werkwijzen worden meegenomen in het overzicht, zodat het inzicht in gegevensverwerkingen binnen VCO volledig en betrouwbaar blijft.

18.3 Register van verwerkingen

VCO houdt een register van verwerkingen bij waarin de verwerkingen van persoonsgegevens binnen de organisatie zijn vastgelegd. Het register van verwerkingen geeft inzicht in welke persoonsgegevens worden verwerkt, met welk doel en onder welke voorwaarden dit plaatsvindt.

In het register van verwerkingen worden ten minste vastgelegd:

- het doel van de verwerking;
- de categorieën persoonsgegevens en betrokkenen;
- de grondslag voor de verwerking;
- de categorieën ontvangers van persoonsgegevens;
- de bewaartermijnen;
- de toegepaste technische en organisatorische beveiligingsmaatregelen;
- het register bevat alle noodzakelijke metadata (grondslag, categorie betrokkenen, ontvangers, bewaartermijnen, beveiliging

Het register van verwerkingen wordt gebruikt als centraal instrument voor het beheer van privacy en gegevensbescherming binnen VCO. Het register ondersteunt de organisatie bij het aantoonbaar voldoen aan wettelijke verplichtingen en vormt een basis voor toezicht, toetsing en verantwoording.

Het register van verwerkingen wordt actueel gehouden. Nieuwe of gewijzigde verwerkingen worden tijdig opgenomen en bestaande verwerkingen worden periodiek beoordeeld op juistheid en volledigheid

Doelstellingen

- Het opzetten en actueel houden van een volledig en betrouwbaar register van verwerkingen waarin alle verwerkingen van persoonsgegevens binnen onze organisatie zijn vastgelegd.
- Minimaal voldoen aan de wettelijke verplichtingen zoals opgenomen in de AVG.
- Inzicht verkrijgen in risico’s per verwerkingsactiviteit door beoordeling van de verwerkersovereenkomst, ten behoeve van gerichte beheersmaatregelen.
- Bevorderen van transparantie, verantwoordingsplicht en gegevensbescherming binnen onze organisatie.
- Ondersteunen van snelle en adequate reactie bij datalekken of andere IBP-incidenten.

Uitgangspunten

- Het register van verwerkingen (D:PR.02 - Register van verwerkingen) bevat alle wettelijk verplichte onderdelen zoals beschreven in de AVG en de onderstaande aanvullingen zodat het register van verwerkingen daarmee aan extra normen van het normenkader voldoet:
    - verwerkingsproces (op basis van FORA)
    - proceseigenaar
    - systeemeigenaar
    - gedetailleerde persoonsgegevens
    - soort persoonsgegevens
    - bron
    - uitvoerder bewaartermijn (verwerkingsverantwoordelijke of verwerker)
    - grondslag
    - juridisch/beleidsmatig kader
    - naam ontvanger
    - AVG-rol
    - verwerkersovereenkomst
    - toetsing gegevensverstrekking aan derden
    - pre-DPIA toets
    - pre-DPIA uitkomst
    - hoog risicoverwerking
    - DPIA uitgevoerd
    - uitzonderingsgronden bijzondere persoonsgegevens
    - geautomatiseerde besluitvorming
    - artificial intelligence
    - technische en organisatorische beveiligingsmaatregelen
    - BIV-classificatie
- Er is een vast proces (C:PR.03 - Verwerkingsregister proces) ingericht voor het aanmaken en actualiseren van verwerkingen in het register van verwerkingen.
- Er is een verantwoordelijke functionaris aangewezen voor het beheer, de beoordeling en

actualisatie van het register. Nieuwe verwerkingen worden direct opgenomen in het register en eens per [kwartaal/half jaar/jaar] worden bestaande verwerkingen gecontroleerd.
- Nieuwe verwerkingen of wijzigingen in verwerkingen worden gesignaleerd via het software inkoopproces (C:SD.01 - Software inkoopproces) en/of het changemanagementproces (C:CH.01 - Changemanagementproces).

18.4 (pre-)DPIA

Binnen het onderwijs worden persoonsgegevens verwerkt in uiteenlopende processen. Sommige van deze verwerkingen kunnen een hoog risico vormen voor de rechten en vrijheden van betrokkenen, zoals leerlingen of medewerkers. Het is daarom essentieel dat de organisatie deze risico's tijdig en systematisch identificeert, beoordeelt en beperkt.

VCO past het instrument van de (pre-)Data Protection Impact Assessment ((pre-)DPIA) toe om privacyrisico's bij gegevensverwerkingen tijdig te signaleren en te beheersen. De beslisboom uit het Normenkader IBP wordt toegepast om te bepalen of een DPIA nodig is. De (pre-)DPIA wordt ingezet bij de introductie van nieuwe verwerkingen en bij wezenlijke wijzigingen in bestaande verwerkingen.

De pre-DPIA wordt gebruikt als eerste toets om te bepalen of een verwerking mogelijk leidt tot verhoogde risico's voor de rechten en vrijheden van betrokkenen. Indien uit de pre-DPIA blijkt dat sprake is van een hoog risico, wordt een volledige DPIA uitgevoerd. De uitkomst van de pre-DPIA wordt vastgelegd en gebruikt als onderbouwing in besluitvorming door bestuur / Privacy Officer.

De DPIA brengt de aard, omvang en context van de verwerking in kaart en beschrijft de risico's voor betrokkenen, evenals de maatregelen die worden genomen om deze risico's te beperken. De uitkomsten van de DPIA worden vastgelegd en betrokken bij besluitvorming over het al dan niet uitvoeren of aanpassen van de verwerking.

1. Uitvoeren van DPIA vóór ingebruikname van risicovolle verwerking.

2. Rapportage van risico's, mitigatie, residual risk en besluitvorming (go/no-go) naar het bestuur en de FG.

3. Herbeoordeling van DPIA's bij wijzigingen, zoals systeemwijzigingen, proceswijzigingen of veranderende risico's.

De Functionaris Gegevensbescherming (FG) wordt betrokken bij het uitvoeren en beoordelen van DPIA's. DPIA's worden herzien wanneer zich relevante wijzigingen voordoen in de verwerking, de gebruikte systemen of de bijbehorende risico's.

Doelstellingen

- Tijdig en gestructureerd signaleren van gegevensverwerkingen met een potentieel hoog privacyrisico.
- Voldoen aan de verplichting om DPIA's uit te voeren bij potentiële 'hoog'-risico verwerkingen.
- Verantwoorde besluitvorming over gegevensverwerking met duidelijke onderbouwing van risico's en maatregelen.
- Beheersing en beperken van privacyrisico's voor betrokkenen.
- Borging van het (pre-)DPIA-proces binnen de organisatie, inclusief opvolging van beheersmaatregelen en documentatie van besluiten.

Uitgangspunten

- De organisatie past bij alle nieuwe en gewijzigde verwerkingen van persoonsgegevens een gestandaardiseerde pre-DPIA toe (D:PR.04 - pre-DPIA toets) om te beoordelen of er sprake is van een potentieel hoog risico.
- Het resultaat van de pre-DPIA wordt vastgelegd in het register van verwerkingen (D:PR.02 - Register van verwerkingen) en is raadpleegbaar voor audits en toezicht.
- Indien een hoog risico wordt vastgesteld, wordt een volledige DPIA uitgevoerd volgens een vast DPIA format (D:PR.05 - DPIA format) dat voldoet aan de wettelijke eisen.
- Alle potentiële 'hoog'-risico verwerkingen zijn onderworpen aan een DPIA.
- Er is een proces vastgesteld voor het opstellen van de DPIA en het opvolgen van geïdentificeerde risico's, het treffen van beheersmaatregelen inclusief de acceptatie van (rest-

)risico’s (C:PR.05 - DPIA proces).
- Afwijkingen van het advies van de Functionaris Gegevensbescherming (FG) worden opgenomen en toegelicht in het DPIA rapport.
- DPIA-rapporten worden centraal opgeslagen binnen de AVG-omgeving van de organisatie en zijn beschikbaar voor interne en externe verantwoording.
- Het proces rondom pre-DPIA’s en DPIA’s is gekoppeld aan het verwerkingsregister proces (C:PR.03 - Verwerkingsregister proces).

18.5 Privacy by Design & Default

De bescherming van persoonsgegevens begint bij de bron: het ontwerpen, ontwikkelen, inkopen en gebruiken van toepassingen, diensten en processen. Om de rechten van betrokkenen structureel te waarborgen, past de VCO de beginselen van Privacy by Design en Privacy by Default toe.

Privacy by Design houdt in dat al in de ontwerpfase van nieuwe systemen, processen en diensten bewust rekening wordt gehouden met privacy risico’s en de beginselen van de AVG. Door deze waarborgen vroegtijdig en structureel in te bouwen, wordt voorkomen dat achteraf kostbare en/of ingrijpende aanpassingen nodig zijn.

Privacy by Default betekent dat de standaardinstellingen van systemen en diensten automatisch zijn afgestemd op maximale privacybescherming. Denk hierbij aan het beperken van gegevensverzameling tot wat strikt noodzakelijk is, het beperken van bewaartermijnen en het uitsluiten van ongewenste toegang tot persoonsgegevens.

Door deze principes te integreren in het risicomanagement, bij inkoop en in samenwerking met externe partijen, borgt de organisatie structureel een hoge mate van gegevensbescherming.

Binnen VCO wordt bij nieuwe of gewijzigde verwerkingen beoordeeld:

- of de verwerking noodzakelijk en proportioneel is;
- of zo min mogelijk persoonsgegevens worden verwerkt;
- of passende technische en organisatorische maatregelen zijn getroffen;
- of de toegang tot persoonsgegevens is beperkt tot geautoriseerde personen.

De toepassing van Privacy by Design en Privacy by Default wordt ondersteund door het uitvoeren van een pre-DPIA en, indien van toepassing, een DPIA. De uitkomsten hiervan worden betrokken bij besluitvorming over de inrichting en het gebruik van processen en systemen.

Doelstelling

- Door het toepassen van Privacy by Design & by Default wordt al in een vroeg stadium rekening gehouden met privacybeginselen, waardoor risico’s tijdig worden gesignaleerd en beperkt.

Uitgangspunten

- We zorgen voor bewustwording van de noodzaak tot Privacy by Design & by Default onder al onze medewerkers. Dit onderwerp is opgenomen in ons bewustwordingsprogramma (B:HR.06 - Bewustwordingsprogramma) waarmee medewerkers bij indiensttreding en tijdens het dienstverband worden geïnformeerd over privacy en de bescherming van (persoons)gegevens.
- De pragmatische aanpak van het principe ‘Privacy by Design’ bevindt zich in de Handleiding Privacy by Design versie 1.0, van het Ministerie van Justitie en Veiligheid.
- Bij de ontwikkeling, het ontwerp, de selectie, de inkoop en het gebruik van toepassingen, diensten en producten houden we zo vroeg mogelijk rekening met privacyrisico’s en bouwen we passende waarborgen in om de privacy van betrokkenen te beschermen. Deze passende waarborgen zijn opgenomen in de inkoopeisen bij nieuwe software (D:SD.01 - Software inkoopeisen).

18.6 Datavernietiging op applicatieniveau

Een zorgvuldig ingericht bewaar- en vernietigingsbeleid op applicatieniveau is essentieel voor het waarborgen van de privacy en het voldoen aan de beginselen van gegevensminimalisatie en opslagbeperking. Wanneer persoonsgegevens langer worden bewaard dan noodzakelijk, vergroot dit het risico dat deze gegevens onrechtmatig worden ingezien, verwerkt of gelekt. Door persoonsgegevens tijdig te verwijderen of te anonimiseren binnen de gebruikte applicaties, voorkomt

VCO dat gegevens buiten de gestelde doelen worden verwerkt of onbedoeld te lang toegankelijk zijn. Voor bepaalde gegevens geldt een wettelijk vastgestelde bewaartermijn, die specifieke bewaartermijn is dan leidend.

VCO draagt zorg voor het tijdig en zorgvuldig vernietigen van persoonsgegevens wanneer deze niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verzameld. Datavernietiging vindt plaats in overeenstemming met vastgestelde bewaartermijnen en geldende wet- en regelgeving.

1. Bewaartermijnen zijn gedocumenteerd in een bewaartermijnenbeleid, dat gebaseerd is op wettelijke verplichtingen en realistische risico-inschattingen.

2. Vernietigingsproces: er is een procedure (digitaal/fysiek) voor het verwijderen van gegevens, met duidelijke rollen (wie vernietigt, wie valideert).

3. Review: bewaartermijnen en vernietiging worden periodiek geëvalueerd en bijgesteld waar nodig.

Op applicatieniveau zijn voorzieningen en werkwijzen ingericht om persoonsgegevens te verwijderen of onomkeerbaar te anonimiseren. Hierbij wordt rekening gehouden met de aard van de applicatie, de mogelijkheden van het systeem en de verantwoordelijkheden binnen de organisatie.

De datavernietiging op applicatieniveau wordt uitgevoerd op een controleerbare en veilige wijze. Waar van toepassing wordt vastgelegd dat gegevens zijn verwijderd, zodat aantoonbaar is dat aan de bewaartermijnen wordt voldaan. Dit betekent ook dat systemen en applicaties zo worden ingericht dat bewaartermijnen worden bewaakt en vernietiging of anonimisering van persoonsgegevens automatisch of procedureel wordt uitgevoerd. Dit vraagt om duidelijk beleid, praktische procedures en structurele toepassing binnen alle relevante systemen.

De werking van datavernietiging op applicatieniveau wordt periodiek beoordeeld en, indien nodig, aangepast naar aanleiding van wijzigingen in applicaties, processen of regelgeving.

Doelstellingen

- Voldoen aan de AVG-beginselen van opslagbeperking en gegevensminimalisatie door persoonsgegevens niet langer te bewaren dan noodzakelijk is voor het beoogde doel.
- Voorkomen van onrechtmatige verwerking en/of datalekken door tijdige verwijdering of anonimisering van persoonsgegevens in applicaties en/of andere omgevingen waarin persoonsgegevens worden verwerkt, bewaard en/of gedeeld.
- Structurele en gecontroleerde toepassing van bewaartermijnen binnen applicaties en systemen.
- Zicht en grip houden op de naleving van de bewaartermijnen in de praktijk, inclusief duidelijke verantwoordelijkheden en aantoonbare naleving.

Uitgangspunten

- Er is een vastgesteld en gedocumenteerd proces voor het verwijderen of anonimiseren van persoonsgegevens (C:PR.07 - Proces bewaren en vernietigen persoonsgegevens), afgestemd op toepasselijke bewaartermijnen, welke zijn vastgelegd in het register van verwerkingen (D:PR.02 - Register van verwerkingen). De verantwoordelijkheden voor het uitvoeren van datavernietiging zijn duidelijk belegd bij systeembeheerders, applicatiebeheerders of proceseigenaren en is eveneens opgenomen in het register van verwerkingen. De planning rondom dit proces leggen we vast in het Jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Applicaties worden bij voorkeur ingericht met automatische functies voor verwijdering of anonimisering zodra gegevens niet langer noodzakelijk zijn. Deze voorkeur is opgenomen in de software inkoopeisen (D:SD.01 - Software inkoopeisen) op basis van het principe Privacy by Design.
- Vanuit het register van verwerkingen (D:PR.02 - Register van Verwerkingen) zijn we in staat een overzicht op te leveren van applicaties en omgevingen waarbij we als organisatie zelf verantwoordelijk zijn voor de uitvoering van de bewaartermijn.
- In samenwerking met leveranciers of verwerkers worden specifieke afspraken gemaakt over de uitvoering van bewaartermijnen en gegevensverwijdering, opgenomen in de verwerkersovereenkomst.

18.7 Toetsing gegevensverstrekking aan derden

VCO toetst gegevensverstrekkingen aan derden voordat persoonsgegevens worden gedeeld. Deze toetsing is erop gericht vast te stellen of de gegevensverstrekking rechtmatig, noodzakelijk en proportioneel is en in overeenstemming met geldende wet- en regelgeving plaatsvindt.

Bij de toetsing wordt onder meer beoordeeld:

- het doel van de gegevensverstrekking;
- de grondslag voor de verstrekking;
- de aard en omvang van de te verstrekken persoonsgegevens;
- de rol van de ontvangende partij (verwerker of verwerkingsverantwoordelijke);
- de getroffen afspraken en maatregelen ter bescherming van persoonsgegevens.

De uitkomst van de toetsing wordt vastgelegd. Indien sprake is van structurele of risicovolle gegevensverstrekkingen aan derden, worden deze opgenomen in het register van verwerkingen en worden aanvullende beheersmaatregelen getroffen waar dit noodzakelijk is.

Medewerkers zijn geïnformeerd over het belang van deze toetsing en weten dat gegevensverstrekking aan derden uitsluitend plaatsvindt na een zorgvuldige afweging en vastlegging.

Doelstellingen

- Voorkomen van onrechtmatige (ondoelmatige) verstrekking van persoonsgegevens aan externe partijen.
- Verhogen van de kwaliteit, doelgerichtheid en juridische onderbouwing van gegevensuitwisseling.
- Verankeren van een uniforme en aantoonbare toetsingsprocedure bij externe gegevensverstrekkingen.
- Zicht houden op alle datastromen naar externe verwerkers of verantwoordelijken en daarover transparant kunnen rapporteren.

Uitgangspunten

- De organisatie hanteert een organisatiebreed toetsingskader voor gegevensverstrekkingen aan derden, dat consequent wordt toegepast. Dit toetsingskader is opgenomen in het verwerkingsregister proces (C:PR.03 - Verwerkingsregister proces). De uitkomst van de toets wordt vastgelegd in het register van verwerkingen (D:PR.02 - Register van Verwerkingen).
- Alle medewerkers zijn geïnformeerd over het belang van voorafgaande toetsing door dit op te nemen in ons bewustwordingsprogramma (B:HR.06 - Bewustwordingsprogramma) en zij weten bij wie zij terecht kunnen met vragen over gegevensuitwisseling.
- Bij iedere verstrekking wordt expliciet beoordeeld of de gegevens relevant, proportioneel en rechtmatig zijn in relatie tot het doel en de ontvanger.
- Toetsing vindt plaats vóórdat gegevens worden gedeeld en eventuele risico’s of afwijkingen worden gedocumenteerd.
- Alleen verstrekken op basis van geldige rechtsgrond (bijv. wettelijke taak, toestemming, gerechtvaardigd belang).

19 Organisatorische inbedding

19.1 Organisatorische inbedding

De bescherming van persoonsgegevens is binnen VCO organisatorisch ingebed. Dit betekent dat privacy en gegevensbescherming onderdeel zijn van de reguliere aansturing, besluitvorming en uitvoering van werkzaamheden binnen de organisatie. Dit hoofdstuk beschrijft hoe de organisatie IBP heeft verankerd door middel van een duidelijke positionering van de functionaris voor gegevensbescherming (FG) en de betrokkenheid van de medezeggenschapsraad (MR).

De organisatorische inbedding waarborgt dat verantwoordelijkheden duidelijk zijn belegd en dat privacy-aspecten tijdig worden betrokken bij processen, projecten en wijzigingen. Privacy en gegevensbescherming maken daarmee integraal deel uit van de dagelijkse praktijk en de bestuurlijke verantwoordelijkheid van het schoolbestuur.
De FG is onafhankelijk gepositioneerd, beschikt over voldoende tijd en middelen en kan effectief adviseren en toezicht houden. Daarnaast is de (gemeenschappelijke) medezeggenschapsraad ((G)MR) actief betrokken bij het privacybeleid, wat bijdraagt aan draagvlak en kwaliteit van besluitvorming.

19.2 Functionaris Gegevensbescherming

VCO heeft een Functionaris Gegevensbescherming (FG) aangesteld. De FG vervult een onafhankelijke rol binnen de organisatie en houdt toezicht op de naleving van de privacywetgeving en het privacybeleid.

De FG adviseert het schoolbestuur en de organisatie over privacyvraagstukken, is betrokken bij DPIA’s en fungeert als aanspreekpunt voor betrokkenen en toezichthoudende autoriteiten. De positie en taken van de FG zijn zodanig ingericht dat deze onafhankelijk, deskundig en effectief kunnen worden uitgevoerd.

In lijn met de AVG en het normenkader is een FG aangesteld en onafhankelijk gepositioneerd zodat deze effectief en onafhankelijk toezicht kan houden op de naleving van de AVG en de verwerking van grote hoeveelheden, vaak ook gevoelige en bijzondere persoonsgegevens. Door deze rol goed te verankeren in de organisatie, wordt zowel voldaan aan de wettelijke verplichting, als actief bijgedragen aan het beschermen van de rechten en vrijheden van leerlingen, ouders, medewerkers en andere betrokkenen.

De FG heeft als belangrijkste taken:

- Informeren en adviseren over onze verplichtingen op grond van de AVG.
- Toezien op naleving van de AVG door VCO.
- Advies uitbrengen bij DPIA’s en toezien op de uitvoering daarvan.
- Adviseren over de afhandeling van datalekken en daarbij optreden als contactpunt voor de Autoriteit Persoonsgegevens.

Doelstellingen

- Het waarborgen van onafhankelijk en deskundig toezicht op de naleving van de AVG binnen VCO .
- De bescherming van persoonsgegevens (verder) verbeteren.
- Versterken van het privacybewustzijn en kennis bij medewerkers, schoolbestuur en andere betrokkenen.
- Betrokkenheid bij beleidsvorming en besluitvorming met betrekking tot persoonsgegevens.
- Zorgen voor een transparante en toegankelijke invulling van de functie, zichtbaar en vindbaar voor alle betrokkenen.

Uitgangspunten

- Wij hebben een FG aangesteld volgens het FG aanstellingsproces (C:OI.01 - FG aanstellingsproces) en onafhankelijk gepositioneerd zodat deze onafhankelijk en effectief toezicht kan houden. De FG rapporteert rechtstreeks aan het bestuur.
- Om het voorgaande te borgen en taken en verantwoordelijkheden van de FG voor onze organisatie duidelijk vast te leggen, hebben wij een door het bestuur vastgesteld FG Reglement (D:OI.01 - FG reglement). In het FG-reglement zijn alle wettelijke- en normenkadereisen

opgenomen. -De (G)MR wordt geïnformeerd over de aanstelling van de FG en stemt in met het FG-reglement.

19.3 Medezeggenschapsraad

De (G)MR speelt een belangrijke rol bij het waarborgen van privacy en gegevensbescherming binnen VCO. De (G)MR wordt actief betrokken bij besluitvorming over de verwerking en bescherming van persoonsgegevens van leerlingen, ouders en medewerkers.

De Wet medezeggenschap op scholen (WMS) kent instemmingsbevoegdheid toe aan de ouder/leerling- en personeelsgeleding van de (G)MR bij de vaststelling of wijziging van regelingen over het verwerken van en de bescherming van persoonsgegevens. Door de (G)MR hierbij tijdig te betrekken wordt niet alleen voldaan aan de wettelijke vereisten, maar wordt ook het draagvlak voor het IBP-beleid vergroot en de kwaliteit van besluitvorming versterkt.

Doelstelling

- Naast het voldoen aan de wettelijke verplichtingen, willen wij door het betrekken van de (G)MR transparantie bevorderen en draagvlak vergroten voor IBP binnen VCO.

Uitgangspunten

- VCO stimuleert een open, tijdige en constructieve dialoog met de (G)MR over informatiebeveiliging en privacy.
- Regelingen over het verwerken en de bescherming van persoonsgegevens van leerlingen, ouders en personeel worden altijd ter instemming voorgelegd aan de (G)MR. Of een beleidsstuk hieronder valt wordt uiteindelijk bepaald door het CvB, op advies van de IBP-verantwoordelijke. Als VCO hebben we een richtlijn opgesteld met documenten die bij de (G)MR ingebracht moeten worden. Deze richtlijn is verwerkt in het proces betrokkenheid (G)MR (C:OI.03 - Betrokkenheid (G)MR proces).
- DPIA-rapportages worden altijd voorgelegd aan de (G)MR als vertegenwoordigers van de betrokkenen. Eventuele vragen en opmerkingen van de (G)MR worden, indien relevant voor het onderzoek meegenomen in de definitieve DPIA rapportage.
- De (G)MR ontvangt tijdig alle relevante informatie om haar instemmings- en adviesrol goed te kunnen vervullen.

20 Rechten van betrokkenen

20.1 Rechten van betrokkenen

Wanneer een organisatie persoonsgegevens verwerkt, spreekt de AVG van ‘betrokkenen’. Binnen het onderwijs zijn dit met name leerlingen, ouders en medewerkers. Deze betrokkenen hebben diverse rechten ten aanzien van de verwerking van hun (persoons)gegevens. Het is de verantwoordelijkheid van het bestuur om de betrokkenen hierover helder te informeren en hen in staat te stellen hun rechten effectief uit te oefenen.

Om dit te waarborgen, beschikt VCO over duidelijke procedures voor het tijdig en zorgvuldig afhandelen van verzoeken, zoals inzage, correctie, verwijdering of bezwaar. Daarnaast is het van belang dat betrokkenen vooraf geïnformeerd worden over welke gegevens worden verwerkt, met welk doel en op welke grondslag. Ook bij geautomatiseerde besluitvorming of profilering moet VCO transparant zijn en zorgen voor een menselijke toets.

Door deze rechten zorgvuldig te borgen, versterkt de organisatie het vertrouwen van betrokkenen en laat zij zien dat de verwerking van persoonsgegevens op een rechtmatige, transparante en respectvolle manier gebeurt, zoals de AVG dat vereist.

20.2 Afhandeling rechten van betrokkenen

VCO heeft een procedure ingericht voor de afhandeling van verzoeken van betrokkenen met betrekking tot hun privacyrechten. Deze procedure waarborgt dat verzoeken zorgvuldig, tijdig en in overeenstemming met de wettelijke vereisten worden behandeld.

Verzoeken worden geregistreerd en beoordeeld op ontvankelijkheid en inhoud. Indien nodig wordt de Functionaris Gegevensbescherming (FG) betrokken bij de beoordeling en afhandeling van het verzoek. VCO zorgt ervoor dat verzoeken binnen de wettelijk vastgestelde termijnen worden afgehandeld.

Wanneer een verzoek geheel of gedeeltelijk wordt afgewezen, wordt de betrokkene hierover gemotiveerd geïnformeerd, inclusief informatie over mogelijke vervolgstappen.

Doelstellingen

- Verzoeken van betrokkenen tot uitoefening van hun privacyrechten worden als zodanig door onze medewerkers herkend en worden vervolgens correct behandeld, in lijn met wet- en regelgeving.
- Vergroten van het vertrouwen van betrokkenen in de bescherming en het kunnen uitoefenen van controle op de verwerking van hun persoonsgegevens.
- Hanteren van een consistente en transparante werkwijze binnen de organisatie.

Uitgangspunten

- 1. Er bestaat een duidelijk procesbeschrijving voor afhandeling van rechtenverzoeken (inzage, correctie, verwijdering, bezwaar) (C:RB.01 - Rechten van betrokkenen proces)
- We informeren betrokkenen op de juiste wijze over hun rechten (zie 18.2 Informatieplicht).
- Verzoeken worden geverifieerd (identiteitscontrole) om misbruik te voorkomen.
- De afhandeling gebeurt binnen de wettelijke termijnen en met transparantie (eerder informeren over beslissing, motiveer weigering).
- Verzoeken tot uitoefening van privacyrechten worden consequent geregistreerd in een register (D:RB.01 - Rechten van betrokkenen register) en gebruikt om verzoeken te beoordelen, voortgang monitoren en periodiek te rapporteren.
- Betrokkenen ontvangen een ontvangstbevestiging van hun verzoeken en worden tijdig geïnformeerd over de status van de behandeling.
- Naast het opgestelde proces werken we structureel aan kennis en bewustwording over de rechten van betrokkenen. Dit om te ervoor te zorgen dat inzageverzoeken ook als zodanig worden herkend en correct behandeld. Het inzagerecht vraagt om extra aandacht voor de wijze waarop o.a. meningen en visies worden vastgelegd, in bijvoorbeeld het leerlingdossier. In ons bewustwordingsprogramma (B:HR.06 – Bewustwordingsprogramma) wordt nadrukkelijk aandacht besteed aan het onderwerp privacyrechten.
- Systemen ondersteunen de uitvoering van AVG-rechten (Privacy by Design).

20.3 Informatieplicht

VCO voldoet aan de informatieplicht door betrokkenen op een transparante en begrijpelijke wijze te informeren over de verwerking van hun persoonsgegevens. Deze informatie wordt verstrekt op het moment dat persoonsgegevens worden verkregen, of, indien dit niet rechtstreeks bij de betrokkene gebeurt, binnen de daarvoor geldende wettelijke termijn.

De informatieplicht omvat onder meer informatie over:

- de doeleinden van de verwerking;
- de rechtsgrond;
- de bewaartermijnen;
- de rechten van betrokkenen;
- eventuele verstrekking van gegevens aan derden.

VCO stelt deze informatie beschikbaar via passende communicatiemiddelen, zodat betrokkenen op eenvoudige wijze kennis kunnen nemen van de verwerking van hun persoonsgegevens

Doelstellingen

- Transparant zijn richting leerlingen, ouders, medewerkers en andere betrokkenen over de verwerking van hun persoonsgegevens door tijdige, begrijpelijke en volledige informatie aan betrokkenen over de verwerking van hun persoonsgegevens te verstrekken.
- Bevorderen van transparantie en vertrouwen in de gegevensverwerking binnen onze organisatie.
- Voldoen aan de wettelijke informatieplicht uit de AVG.

Uitgangspunten

- Er is een toegankelijke privacyverklaring of -verklaringen (leerlingen, ouders, medewerkers) die de noodzakelijke informatie biedt volgens de AVG.
- Bij wijzigingen in dataverwerking of beleid wordt de betrokkenen tijdig geïnformeerd.
- Informatie is begrijpelijk, contextualiseert terminologie en legt processen uit (zoals verzoeken, bezwaar, intrekking).
- Betrokkenen worden vooraf geïnformeerd over de verwerking van hun persoonsgegevens, in lijn met het beginsel van behoorlijke en transparante verwerking en we verwijzen daarbij altijd (met een directe link) naar onze privacyverklaring(en) (D:RB.02 - Privacy verklaring) op onze website(s).
- Wij zorgen dat de informatie begrijpelijk en toegankelijk is voor betrokkenen.
- Wij beschikken binnen onze organisatie over een actueel privacyreglement voor leerlingen en ouders (D:RB.02 - Privacy reglement leerlingen en ouders), een privacyreglement voor medewerkers (D:RB.02 - Privacy reglement medewerkers), een privacyverklaring (D:RB.02 - Privacy verklaring) voor leerlingen, ouders, medewerkers en sollicitanten[, waarin eveneens een cameratoezicht verklaring is opgenomen] en een cookieverklaring (D:RB.02 - Cookieverklaring) voor onze website(s), waarop we ook een passende cookiebanner laten zien. De privacyverklaring is in begrijpelijke taal (taalniveau B1) op de website(s) van de scholen en het schoolbestuur terug te vinden. Er hoeft maximaal 1 maal doorgeklikt te worden.
- Wij werken met een coördinated vulnerability disclosure (D:RB.02 - Coördinated vulnerability disclosure), waarmee ethische hackers of andere melders op veilige wijze kwetsbaarheden in systemen kunnen rapporteren.
- Wij wijzen betrokkenen in onze privacyverklaring duidelijk op de rechten die de AVG hen toekent en hoe ze deze rechten kunnen uitoefenen.
- De privacyverklaring is altijd actueel en gebaseerd op het register van verwerkingen. Bij veranderingen in het register van verwerkingen wordt altijd gecontroleerd of dit invloed heeft op de privacyverklaring. Deze controle is opgenomen in het Verwerkingsregister proces (C:PR.03 - Verwerkingsregister proces).

20.4 Toestemming

Elke verwerking van persoonsgegevens moet gebaseerd zijn op een geldige grondslag, zoals vastgelegd in de AVG. Zonder grondslag is de verwerking onrechtmatig. In het onderwijs worden

verwerkingen op verschillende grondslagen gebaseerd, waarvan de grondslag ‘wettelijke verplichting’ het meest voorkomt. Soms kan een verwerking echter alleen worden gebaseerd op de grondslag ‘toestemming’.

Wanneer toestemming de grondslag vormt voor de verwerking van persoonsgegevens, zorgt VCO ervoor dat deze toestemming vrijelijk, specifiek, geïnformeerd en ondubbelzinnig wordt verkregen.

Betrokkenen worden duidelijk geïnformeerd over het doel waarvoor toestemming wordt gevraagd en hebben de mogelijkheid om hun toestemming op ieder moment in te trekken. Het intrekken van toestemming heeft geen gevolgen voor de rechtmatigheid van de verwerking die plaatsvond vóór de intrekking.

1. Toestemmingsformulieren zijn gebruiksvriendelijk, duidelijk en voldoen aan de eisen van de AVG (vrij, geïnformeerd, specifiek).

2. Toestemming wordt gedocumenteerd en bewaard, en de intrekking ervan is net zo eenvoudig als het geven.

3. Bij intrekking van toestemming wordt de verwerking aangepast of stopgezet, tenzij er een andere rechtsgrondslag van toepassing is.

Aan het gebruik van de rechtsgrond toestemming worden door de AVG een aantal strikte eisen verbonden. Toestemming moet vrijwillig (vrije keuze/ongedwongen en zonder gevolgen), specifiek (voor een specifieke verwerking), geïnformeerd (welke gegevens en doel) en ondubbelzinnig (met actieve handeling) door betrokkenen worden gegeven. Bovendien moeten betrokkenen - zoals leerlingen en ouders - in staat zijn hun toestemming op elk moment in te trekken, zonder nadelige gevolgen.

Het zorgvuldig en transparant omgaan met toestemming draagt bij aan de rechtmatigheid van gegevensverwerking en versterkt het vertrouwen van betrokkenen in VCO.

Doelstellingen

- Inzicht in welke verwerkingen op toestemming zijn gebaseerd.
- Borgen dat alle verwerkingen waarvoor toestemming als grondslag nodig is, ook daadwerkelijk op geldige toestemming zijn gebaseerd.
- Borgen dat betrokkenen goed geïnformeerd zijn en in vrijheid een keuze kunnen maken.
- Faciliteren dat toestemming eenvoudig en aantoonbaar kan worden gegeven én ingetrokken.
- Voldoen aan de eisen die de AVG stelt aan het gebruik van de grondslag toestemming.

Uitgangspunten

- We zijn terughoudend met het gebruiken van toestemming als grondslag. Omdat er een gezagsrelatie bestaat tussen de school en haar leerlingen/medewerkers moet goed worden beargumenteerd dat toestemming in specifieke gevallen in vrijheid kan worden gegeven.
- Wanneer we een verwerking baseren op toestemming zorgen we ervoor dat dit vooraf is getoetst.
- We werken uitsluitend met gestandandaardiseerde formats voor toestemming in applicaties en/of formulieren, die vooraf zijn getoetst.
- Toestemming wordt op de juiste wijze gevraagd en vastgelegd, in overeenstemming met de AVG. We kunnen alle verleende toestemmingen aantonen in een overzicht (vanuit o.a. applicaties en/of formulieren). Dit overzicht is actueel, volledig en herleidbaar.
- De toestemming is:
    - vrijwillig; het wel of niet geven van toestemming mag geen gevolgen hebben voor de betrokkene(n) (geen discriminatie op basis van privacy keuzes)
    - specifiek; voor een specifieke verwerking (geen algemene toestemming voor mogelijke en/of toekomstige verwerkingen)
    - geïnformeerd; er wordt bekend gemaakt welke persoonsgegevens worden verzameld, voor welk doeleinde, wie de verwerkingsverantwoordelijke is en er wordt gewezen op het recht om de toestemming te allen tijde weer in te trekken. Het intrekken van toestemming is voor betrokkenen net zo eenvoudig als het geven ervan
    - ondubbelzinnig; toestemming wordt gegevens met een duidelijke actieve handeling (geen

    - automatische toestemming met het vervolgen van een proces binnen een bepaalde omgeving en/of vooraf aangevinkte selectievakken)
    - begrijpelijk; het wordt gevraagd op een begrijpelijke en toegankelijke manier, in duidelijke taal en niet verborgen in lange teksten
- Op de plaats waar toestemming verleend kan worden, wordt altijd met een directe link verwezen naar de privacyverklaring van de organisatie.
- Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven.
- Alle verwerkingen die gebaseerd zijn op toestemming zijn opgenomen in ons register van verwerkingen (D:PR.02 - Register van verwerkingen).

20.5 Geautomatiseerde besluitvorming/profilering

VCO maakt vooralsnog geen gebruik van geautomatiseerde besluitvorming en profilering. Indien hiervan sprake is, waarborgt VCO dat dit gebeurt binnen de kaders van de AVG en met inachtneming van de rechten en belangen van betrokkenen.

1. Identificatie: alle vormen van geautomatiseerde besluitvorming of profilering zijn geregistreerd in het verwerkingsregister.

2. Beoordeling: voor deze verwerkingen wordt een DPIA uitgevoerd om risico’s te analyseren en te mitigeren.

3. Transparantie en rechten: betrokkenen worden geïnformeerd over de logica, impact en bestaan van dergelijke verwerkingen, en hebben toegang tot herziening door een mens waar dat wettelijk is vereist.

Bij het gebruik van individuele geautomatiseerde besluitvorming en/of profilering spelen de bescherming van persoonsgegevens en de rechten van betrokkenen een belangrijke rol. Volgens de AVG hebben mensen recht op een menselijke tussenkomst bij besluiten die rechtsgevolgen hebben, of hen anderszins aanmerkelijk raken. Dit geldt ook binnen het onderwijs, bijvoorbeeld bij beslissingen over toelating, ondersteuning of beoordeling. Volgens de AVG vereist geautomatiseerde besluitvorming bij kinderen bijzondere bescherming en is terughoudendheid vereist.

Wanneer gebruik wordt gemaakt van geautomatiseerde besluitvorming moet dit zorgvuldig, transparant en in overeenstemming met de wettelijke eisen gebeuren. VCO moet daarbij borgen dat betrokkenen goed worden geïnformeerd en in staat zijn om besluiten aan te vechten of aanvullende toelichting te vragen. Zo worden onrechtmatige of onbedoeld discriminerende uitkomsten voorkomen.

Geautomatiseerde besluitvorming: een besluit dat volledig automatisch wordt genomen. Uitsluitend gebaseerd op een volledig geautomatiseerde verwerking (dus zonder menselijke tussenkomst) en die rechtsgevolgen heeft voor de betrokkene of hem/haar in aanmerkelijke mate treft (zoals toelating, afwijzing en toekenning van extra ondersteuning).

Profilering: elke vorm van geautomatiseerde ‘verwerking’ van persoonsgegevens waarbij die gegevens worden gebruikt om bepaalde persoonlijke aspecten van een natuurlijke persoon te evalueren, in het bijzonder om aspecten met betrekking tot werkprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
Dus profilering is het analyseren of voorspellen van gedrag op basis van persoonsgegevens. Profilering ‘kan’ een vorm zijn van geautomatiseerde besluitvorming, dit is echter niet per definitie het geval. Bij profilering is geen sprake van geautomatiseerde besluitvorming, wanneer er menselijke tussenkomst is en/of er geen sprake is van besluiten die rechtsgevolgen hebben of betrokkenen anderszins aanmerkelijk raken.

Artificial Intelligence (AI) is geen synoniem voor geautomatiseerde besluitvorming en/of profilering. Een AI-systeem is een op machines gebaseerd systeem dat ontworpen is om, met een bepaalde mate van autonomie, output te genereren zoals voorspellingen, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen. AI is dus de technologie, profilering en geautomatiseerde besluitvorming zijn de toepassingen of vormen van gegevensverwerking waarbij AI kan worden ingezet.

Het gebruik van AI volgens de AI Act en met toepassing van de AVG, hebben wij geregeld in separaat AI-beleid.

Doelstellingen

- Zorgen voor transparantie over het gebruik van geautomatiseerde besluitvorming en/of profilering.
- Waarborgen van de rechten van betrokkenen, zoals het recht op informatie, bezwaar en menselijke tussenkomst.
- Als we geautomatiseerde besluitvorming en/of profilering toepassen voldoen we aan de relevante wet- en regelgeving.
- Beheersen van de risico’s op onrechtmatige of discriminerende uitkomsten.

Uitgangspunten

- Geautomatiseerde besluitvorming bij kinderen staan we in principe niet toe en indien noodzakelijk, dan alleen onder uitzonderlijke, gerechtvaardigde omstandigheden en met verzwaarde waarborgen.
- We zijn terughoudend met het toepassen van geautomatiseerde besluitvorming en zijn ons daarbij bewust van de leeftijd van de betrokkenen.
  OF
  Wij passen per definitie geen uitsluitend geautomatiseerde besluitvorming toe zonder menselijke tussenkomst. Profilering gebruiken wij uitsluitend met passende waarborgen en menselijke controle.
- [We beschikken over een volledig overzicht (D:PR.02 - Register van verwerkingen) en documentatie van processen waarin geautomatiseerde besluitvorming plaatsvindt.]
- [Betrokkenen worden vooraf en duidelijk geïnformeerd over het gebruik van geautomatiseerde besluitvorming conform de informatieplicht.]
- [Voor elk nieuw proces met geautomatiseerde besluitvorming of profilering wordt een DPIA uitgevoerd.]
- [Passen we geautomatiseerde besluitvorming toe dan is er altijd de mogelijkheid voor herbeoordeling van een besluit door een menselijke functionaris.]
- Binnen ons bewustwordingsprogramma (B:HR.06 - Bewustwordingsprogramma) is aandacht voor geautomatiseerde besluitvorming en/of profilering.

21 Verantwoording

21.1 Verantwoording

Transparantie over de wijze waarop persoonsgegevens worden verwerkt én beschermd is essentieel voor het vertrouwen van leerlingen, ouders, medewerkers en andere betrokkenen.

Het schoolbestuur rapporteert periodiek aan interne en externe stakeholders over de naleving van de AVG en over de stand van zaken rond informatiebeveiliging en privacy. Dit gebeurt via een gestructureerd verslaggevingsproces, waarbij ook de Functionaris Gegevensbescherming (FG) wordt betrokken.

In het jaarverslag (ten behoeve van het Ministerie van OCW) wordt, conform de wettelijke verplichting, specifiek aandacht besteed aan IBP. Omdat het jaarverslag openbaar is, worden hierin geen (eventuele) concrete zwakheden in de informatiebeveiliging opgenomen.

Doelstellingen

- Verantwoording afleggen aan interne en externe stakeholders over de naleving van de AVG, het normenkader en ons IBP-beleid.
- Inzicht geven in de voortgang en resultaten van IBP-activiteiten binnen de organisatie.
- Vertrouwen bevorderen bij leerlingen, ouders en medewerkers in de zorgvuldige omgang met (persoons)gegevens.
- Voldoen aan de wettelijke verplichting tot verslaglegging over IBP in het jaarverslag van het schoolbestuur.

Uitgangspunten

- We stellen jaarlijks een verslag op voor interne en externe stakeholders. Het moment van opleveren is opgenomen in het jaarplan IBP (B:GO.03 - Jaarplan IBP).
- Voor het jaarlijks rapporteren over de naleving van de AVG wordt een gestructureerd en gedocumenteerd proces (C:VW.01 - Jaarverslag IBP proces) gevolgd dat aan de eisen van de AVG en het Normenkader voldoet. Om de kwaliteit en de volledigheid te waarborgen is er een door het schoolbestuur goedgekeurd format voor het jaarverslag IBP (D:OI.01 - Jaarverslag IBP format) vastgesteld. De FG kan om een review gevraagd worden.
- Voor het opstellen van dit verslag wordt tevens gebruikt gemaakt van de input die voortkomt uit de jaarlijkse aandacht IBP op schoolniveau (D:GO.02 - Jaarlijkse aandacht IBP op schoolniveau).