Noorderpoort

Informatiebeveiligings- en Privacybeleid

Noorderpoort 2018-2020

ICT Governance

Colofon

Datum
9-2-2018

Titel
Informatiebeveiligings- en privacybeleid Noorderpoort 2018-2020

Auteurs
Werkgroep informatiebeveiliging & privacy

Versie
1

Status
Definitief

Inhoud

Definities

Algemene verordening gegevensbescherming (AVG): nieuwe Europese privacywetgeving. Deze wet vervangt de Wet bescherming persoonsgegevens.

Betrokkene: een individueel en natuurlijk persoon op wie een Persoonsgegeven betrekking heeft.

Datalek: Persoonsgegevens die in handen vallen van personen die geen toegang tot die gegevens (mogen) hebben.

Informatiebeveiliging: alle processen, maatregelen en procedures die zijn getroffen om informatie beschikbaar, integer en vertrouwelijk te houden.

Informatiesysteem: een systeem waarmee informatie over gegeven of objecten verwerkt kan worden.

Malware: alle software die wordt gebruikt om toegang te krijgen tot computersystemen, of om deze te verstoren, of om gevoelige informatie te verkrijgen.

Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.

Privacy: bescherming van de persoonlijke levenssfeer, wat betreft dit beleid: bescherming van persoonlijke gegevens in het bijzonder.

Privacy impact assessment (PIA): een hulpmiddel om privacyrisico's in kaart te brengen.

Verwerker: een door Noorderpoort ingeschakelde (derde) partij die ten behoeve van Noorderpoort Persoonsgegevens verwerkt.

Verwerking: elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens.

1 Inleiding

Informatiebeveiliging en privacy zijn onderwerpen die steeds meer leven in de maatschappij. Door incidenten als datalekken en aanvallen met ransomware, beseffen mensen steeds meer wat de gevolgen kunnen zijn van het weinig tijd en aandacht besteden aan informatiebeveiliging en privacy.

Binnen Noorderpoort wordt al geruime tijd gewerkt met een informatiebeveiligingsbeleid. Omdat informatiebeveiliging voortdurend aan verandering onderhevig is, wordt het informatiebeveiligingsbeleid van Noorderpoort periodiek herzien. Dit herzien en aanpassen aan de actualiteit van het informatiebeveiligingsbeleid vormt dan ook de eerste aanleiding voor de nieuwe versie van het beleid.

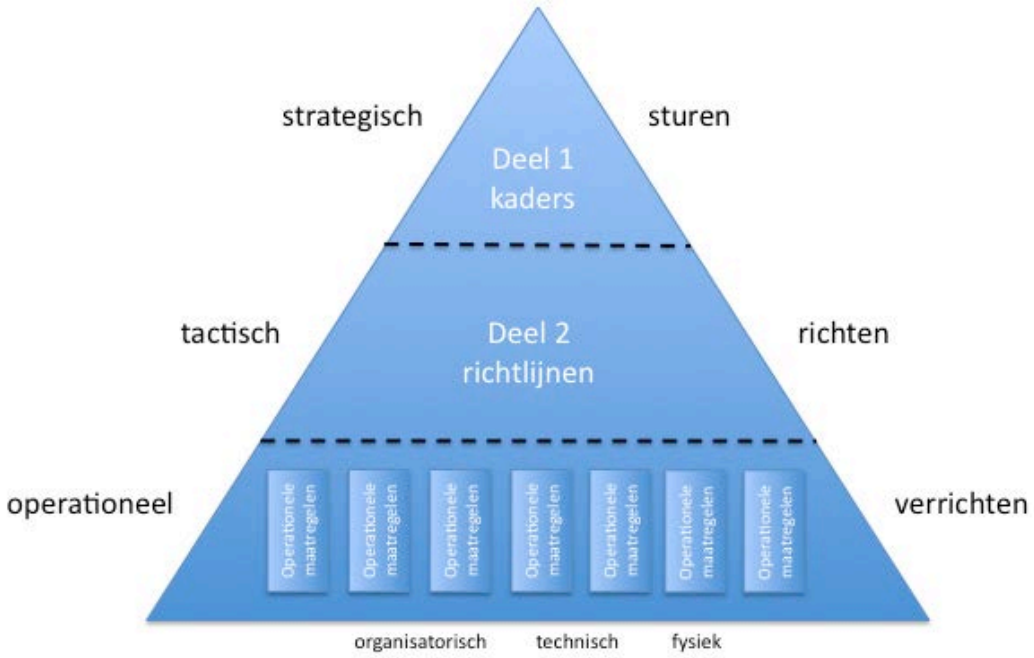
De tweede aanleiding voor het herschrijven is de introductie van nieuwe Europese wetgeving (Algemene Verordening Gegevensbescherming) op het gebied van privacy. De AVG is op 24 mei 2016 in werking getreden, maar is vanaf 25 mei 2018 van toepassing. De AVG valt dan ook binnen de periode van dit beleidsstuk, waardoor deze ook zal worden meegenomen. Dit houdt in dat privacy meer aandacht zal krijgen in het beleid, waardoor we vanaf nu spreken van het informatiebeveiligings- en privacybeleid.

In dit beleidsstuk wordt beschreven hoe Noorderpoort invulling geeft aan informatiebeveiliging en privacy. Hiervoor zal in hoofdstuk 2 een opbouw worden gegeven van het beleid. Om duidelijk te maken wat Noorderpoort precies onder informatiebeveiliging en privacy verstaat, worden deze begrippen gedefinieerd in hoofdstuk 3. De doelstelling en principes van het beleid worden beschreven in hoofdstuk 4. Vervolgens wordt in hoofdstuk 5 ingegaan op het besturingsmodel. Hierbij worden de rollen en verantwoordelijkheden beschreven. Ook wordt hier ingegaan op het (incidenten)proces. Hoofdstuk 6 tenslotte bevat de richtlijnen voor het beleid. Deze richtlijnen zijn gebaseerd op de ISO-normen 27001-27002 en gebaseerd op de kaders zoals gesteld in hoofdstuk 4 en 5.

2 Opbouw

Het Noorderpoort informatiebeveiligings- en privacybeleid is opgebouwd in drie niveaus. Dit om enerzijds richting te kunnen geven voor de komende jaren en anderzijds snel en flexibel in te kunnen spelen op bijvoorbeeld het beschikbaar komen van nieuwe technieken en methodieken.

De drie niveaus:

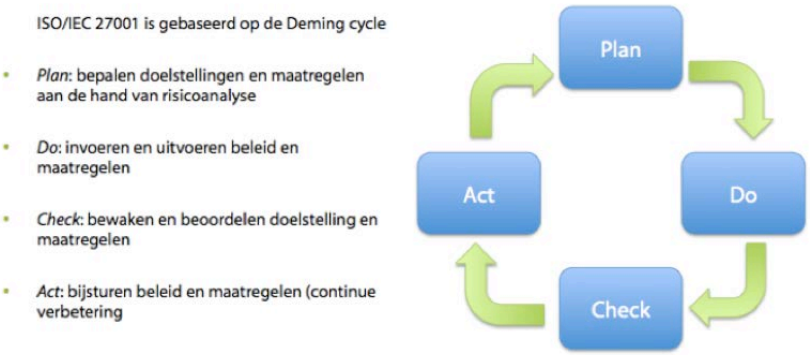


Niveau 1: strategisch

Hoofdstuk 4 en 5 bevatten de kaders binnen Noorderpoort. Hierin worden de doelstellingen, principes, taken en verantwoordelijkheden, evenals het procesmodel dat binnen Noorderpoort voor informatiebeveiliging en privacy wordt gehanteerd, beschreven.

Niveau 2: tactisch
Hoofdstuk 6 bevat de richtlijnen. Deze richtlijnen vormen het basisbeveiligingsniveau en zijn gericht op verschillende onderwerpen binnen Noorderpoort: beleid & organisatie, personeel, studenten & gasten, ruimtes & apparatuur, continuïteit, vertrouwelijkheid & integriteit en controle & logging.
Bij het definiëren van de richtlijnen wordt uitgegaan van de kaders zoals deze in hoofdstuk 4 en 5 zijn gesteld.

Niveau 3: operationeel
Per proces en per informatiesysteem worden maatregelen geïmplementeerd. Deze maatregelen zijn een directe doorvertaling van de richtlijnen die betrekking hebben op het proces dan wel het informatiesysteem. De maatregelen staan beschreven in afzonderlijke documenten die betrekking hebben op een proces of informatiesysteem. Denk hierbij aan AO-beleid, procedure-beschrijvingen, autorisatiematrices en beheerdocumenten.



Op alle drie de niveaus wordt de PDCA-cyclus doorlopen op basis van de Deming cycle. Daarbij geldt:

- De kaders (strategisch) worden in een 3-jaars cyclus herijkt
- De richtlijnen (tactisch) worden jaarlijks getoetst en waar nodig aangepast
- De maatregelen (operationeel) kunnen continue worden gewijzigd naar aanleiding van veranderde context, projecten of gebleken risico's.

Hoofdstuk 3 bevat een uitleg ten aanzien van wat informatiebeveiliging en privacy precies inhoudt.

3 Wat is informatiebeveiliging & privacy

3.1 Informatiebeveiliging

De term ‘informatiebeveiliging’ omvat alle maatregelen en processen die binnen een organisatie lopen om de informatie beschikbaar, integer en vertrouwelijk te houden. Met beschikbaarheid, integriteit en vertrouwelijkheid wordt het volgende bedoeld:

· *Beschikbaarheid:* de informatie moet op de gewenste momenten beschikbaar zijn;
Voorbeeld: de verbinding met de server naar de online toets mag niet verbroken worden.

· *Integriteit:* de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
Voorbeeld: de cijfers van een toets moeten niet aangepast kunnen worden door een buitenstaander.

· *Vertrouwelijkheid*: de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.
Voorbeeld: een bestand met persoonsgegevens van leerlingen mag niet voor iedereen inzichtelijk zijn.

Om de informatie aan deze voorwaarden te laten voldoen, dient er weerstand geboden kunnen worden tegen allerlei bedreigingen, die in verschillende vormen voorkomen. Zo kunnen ze fysiek van aard zijn, zoals brand of wateroverlast. Ook kunnen er technische bedreigingen zijn, bijvoorbeeld in de vorm van storingen in de programmatuur, apparatuur of stroomvoorziening. Hiernaast vormt ook de medewerker zelf een bedreiging voor de informatiebeveiliging. Te denken valt hierbij aan het maken van onopzettelijke fouten en/of vergissingen, zoals het klikken op een link van een phishing-mail, het onbewust installeren van kwaadaardige software, het onzorgvuldig omgaan met wachtwoorden etc. De afgelopen jaren is gebleken dat de mogelijke impact van de bedreigingen steeds groter worden, dit mede door de grotere afhankelijkheid van informatiesystemen. Ook worden bepaalde bedreigingen groter, zo worden phishing-mails steeds geraffineerder.

3.2 Privacy

De bescherming van de persoonlijke levenssfeer is een grondrecht. Daaronder valt ook de bescherming van persoonlijke gegevens. Binnen Noorderpoort zijn we ons bewust van onze verantwoordelijkheid voor de gegevens van onze studenten, medewerkers en eventuele anderen. Daarom houden we ons aan de volgende uitgangspunten.

3.2.1 Grond, Doel & Doelbinding

We verwerken alleen persoonsgegevens als dat mag van de wet. Elke verwerking van Persoonsgegevens binnen Noorderpoort is daarom gebaseerd op een van de wettelijke gronden zoals genoemd in artikel 6 Algemene Verordening Gegevensbescherming (AVG). Denk bijvoorbeeld aan de wettelijke verplichting om bepaalde gegevens over studenten door te geven aan DUO, of de gegevens die Noorderpoort nodig heeft om een arbeidsovereenkomst met een medewerker aan te kunnen gaan.
Als we binnen Noorderpoort persoonlijke gegevens verwerken, doen we dat altijd voor een duidelijk en gerechtvaardigd doel. Zo hebben we bijvoorbeeld de naam en vooropleiding van een student nodig om onderwijs te kunnen geven. De doelen worden vooraf vastgesteld door het College van Bestuur.
Eenmaal verkregen persoonsgegevens worden alleen gebruikt voor het doel waarvoor ze verkregen zijn, of voor doelen die daarmee verenigbaar zijn (doelbinding).

3.2.2 Dataminimalisatie

Noorderpoort zal alleen gegevens verwerken als dat noodzakelijk is. Dat betekent dat we niet meer gegevens vragen, gebruiken en registreren dan nodig is om de afgesproken doelen te bereiken. Hierbij wordt verwerken van bijzondere en gevoelige gegevens zo veel mogelijk vermeden. Daarnaast bewaren we persoonsgegevens niet langer dan voor de afgesproken doelen noodzakelijk is.

3.2.3 Datakwaliteit- en integriteit

Noorderpoort treft maatregelen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn. Denk bijvoorbeeld aan autorisatieschema's om te zorgen dat alleen personen die de gegevens echt moeten gebruiken, deze gegevens ook kunnen invoeren en wijzigen. Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen, in het bijzonder de ISO 27001.

3.2.4 Rechten betrokkene

Iedereen heeft recht op inzage, verbetering, aanvulling, overdraagbaarheid, verwijdering en afscherming van de hem betreffende persoonsgegevens. Daaronder valt ook het recht om vergeten te worden. Daarnaast heeft een betrokkene het recht om op grond van bijzondere omstandigheden of als het gaat om marketingdoeleinden, bezwaar in te stellen tegen verwerking.

3.2.5 Toestemming

Wanneer binnen Noorderpoort persoonlijke gegevens verwerkt worden met toestemming van de betrokkene, wordt deze van tevoren duidelijk geïnformeerd over wat er met de gegevens gedaan wordt. De toestemming wordt schriftelijk vastgelegd en er wordt een eenvoudige procedure aangeboden om de toestemming weer in te trekken. Denk bijvoorbeeld aan het plaatsen van foto's van een klassenuitje op de Facebookpagina van de klas. Hiervoor zal elke herkenbare student toestemming gevraagd moeten worden, deze toestemming wordt vastgelegd, en, indien een

student zich er toch niet prettig bij voelt, wordt de foto zonder aarzelen weer verwijderd. Zo zorgt Noorderpoort ervoor dat iedereen grip op zijn persoonsgegevens blijft houden.

3.2.6 Privacy by design & Default

Privacy is geen sluitstuk, maar een volwaardig onderdeel van bedrijfsvoering binnen Noorderpoort. Daarom wordt bij het ontwerpen en beheren van (delen van) informatiesystemen en processen altijd rekening gehouden met de bescherming van persoonlijke gegevens (privacy by design). Bijvoorbeeld door al in de projectfase of voor de aankoop van systemen de privacyrisico's in kaart te brengen middels een Privacy Impact Assessment (PIA) en door met leveranciers afspraken te maken over de omgang met persoonsgegevens (zogenaamde verwerkersovereenkomsten). In systemen worden de instellingen standaard zo privacyvriendelijk mogelijk gezet (Privacy by default).

3.2.7 Informatie- en verantwoordingsplicht

Noorderpoort legt op transparante wijze verantwoording af over welke persoonsgegevens verwerkt worden, wat er met de gegevens gebeurt en de daarbij gehanteerde principes. Bijvoorbeeld door middel van privacystatements voor studenten en medewerkers.

3.2.8 Functionaris Gegevensbescherming

Noorderpoort neemt de bescherming van de persoonlijke gegevens die onder haar verantwoordelijkheid verwerkt worden, serieus. Daarom is een Functionaris Gegevensbescherming (FG) aangesteld. De FG is een onafhankelijke functionaris binnen Noorderpoort, die adviseert over en toezicht houdt op, de naleving van privacywetgeving. Ook kunnen betrokkenen bij de FG terecht met alle vragen over de omgang met hun persoonsgegevens en hun rechten daarbij.

4 Doelstelling en principes

Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden, of in gesproken vorm). Informatie is een bedrijfsmiddel dat net als andere belangrijke bedrijfsmiddelen van waarde is voor Noorderpoort en dat, ongeacht de gegevensdrager, voortdurend op een passende manier beveiligd dient te zijn.

Informatie kan gaan over personen; over studenten, medewerkers of andere betrokkenen bij Noorderpoort. Deze informatie is ons in vertrouwen gegeven en dit vertrouwen zullen we als organisatie niet beschamen. We moeten daarom ook de privacy borgen bij alle informatie die we verkrijgen, opslaan en gebruiken.

*Het doel van informatiebeveiliging en privacy is het waarborgen van de **beschikbaarheid**, **integriteit** en **vertrouwelijkheid** van informatie en het borgen van de **privacy** van de betrokkenen op wie de informatie betrekking heeft.*

4.1 Principes

Noorderpoort hanteert de volgende principes ten aanzien van informatiebeveiliging en privacy:

4.1.1 By design, by default

Bij het gebruiken en/of ontwerpen van informatiesystemen worden informatiebeveiliging en privacy automatisch meegenomen. Daarbij is het uitgangspunt het borgen van die beveiliging en de privacy van onze studenten en medewerkers. Bij al ons doen en laten zijn we ons bewust van gevolgen voor privacy en beveiliging; het zit ons in de genen.

4.1.2 Cyclisch

Noorderpoort beschouwt het sturen en borgen van informatiebeveiliging en privacy als een cyclisch proces waarin continue aandacht is voor risicobeheersing, voorkomen en verbeteren.
Het is in een snel veranderende wereld en met wisselende technieken en methoden van belang dat er continu aandacht is voor risicobeheersing. Dit kan en moet door continu en cyclisch te kijken naar risico's en aan de hand van incidenten of risico's in te zetten op het voorkomen van herhaling en verbeteren van maatregelen.

4.1.3 Open karakter

Noorderpoort wil voor haar studenten en haar partners in het onderwijsproces transparant, toegankelijk en open zijn. Samenwerking in de regio ten dienste van de student is een speerpunt. Het informatiebeveiliging- en privacybeleid moet recht doen aan dit open karakter van onze organisatie.

4.1.4 Voldoen aan wetgeving

Het informatiebeveiligings- en privacybeleid moet voldoen aan de door de wetgeving gestelde eisen.
Bij Noorderpoort wordt op de volgende wijze omgegaan met relevante wet- en regelgeving:

- Wet Educatie en Beroepsonderwijs (WEB) en Wet Voorgezet Onderwijs (WVO)

Noorderpoort heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studenten administratie en met de zorgdossiers is gewaarborgd.

- Algemene Verordening Gegevensbescherming (AVG)

Noorderpoort heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het informatiebeveiligings- en privacybeleid.
De ingangsdatum van de AVG is 25 mei 2016 en de inwerkingtreding is 25 mei 2018. De AVG komt in plaats van de Wbp (Wet bescherming persoonsgegevens).

- Archiefwet

Noorderpoort houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d.

- Auteurswet

Noorderpoort verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat Noorderpoort het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

- Wetboek van Strafrecht

In het Wetboek van Strafrecht zijn de laatste decennia een aantal specifieke bepalingen opgenomen over de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat “enige beveiliging” vereist is alvorens er sprake kan zijn van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling.

Naleving van dit informatiebeveiligings- en privacybeleid en implementatie van de basismaatregelen bij Noorderpoort moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van het Wetboek van Strafrecht.

5 Besturingsmodel

5.1 Rollen en verantwoordelijkheden

Informatiebeveiliging en privacy is een integrale verantwoordelijkheid van het management. Dit houdt in dat het onderdeel is van de normale taken en verantwoordelijkheden van het lijnmanagement (directie en teammanagers) en de eigenaren van informatiesystemen. Om Noorderpoort-breed te zorgen voor een adequate sturing op dit thema, zijn er extra rollen belegd bovenop de al bestaande structuren. In dit hoofdstuk wordt beschreven hoe de rollen en verantwoordelijkheden belegd zijn.

5.1.1 College van Bestuur

Het College van bestuur stelt het beleid vast en is eindverantwoordelijk t.a.v. informatiebeveiliging en de borging van privacy bij Noorderpoort.

5.1.2 Security Officer

De Security Officer is vanuit het CvB gedelegeerd verantwoordelijke t.a.v.:

- Het coördineren en communiceren van concern-breed beleid op het gebied van informatiebeveiliging.
- Het coördineren en communiceren van concern-breed beleid op het gebied van privacy

De Security Officer zorgt ervoor dat de verschillende actoren binnen Noorderpoort op de hoogte zijn van het beleid, in staat zijn om het beleid uit te kunnen voeren en zorgt ook voor controle op en borging van de Noorderpoort-brede implementatie van het informatiebeveiligings- en privacybeleid.

5.1.3 Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG)[1] heeft twee primaire rollen:

1. Het houden van toezicht op de naleving privacy binnen Noorderpoort.

In deze rol is de FG onafhankelijk en dient als toezichthouder. Binnen deze rol zijn er de volgende taken/verantwoordelijkheden:

- Toezicht houden op de naleving van wet- en regelgeving, alsmede op naleving van het privacybeleid, met inbegrip van de toewijzing van verantwoordelijkheden
- (Ongevraagd) Adviseren van het CvB en alle bij gegevensverwerkingen betrokken medewerkers over hun (wettelijke) verplichtingen
- Inventarisaties van gegevensverwerkingen maken
- Registeren van gegevensverwerkingen

[1] Tot 25 mei 2018 heeft Noorderpoort een Privacy Adviseur. Vanaf 25 mei 2018 zal de Privacy Adviseur opgevolgd worden door de Functionaris Gegevensbescherming (FG). In dit beleidsdocument zijn beide personen dezelfde waarbij ten aanzien van rollen en verantwoordelijkheden staat beschreven wat de FG vanaf 25 mei 2018 aan bevoegdheden heeft.

- Toezien op de uitvoering van audits

2. ***Het meewerken aan de vormgeving en borging van het privacybeleid.***
   Voor het vormgeven van het privacybeleid en de implementatie hiervan ligt de primaire verantwoordelijkheid bij de Security Officer, de directeuren en de eigenaren van informatiesystemen. Met de expertise van de FG helpt deze mee en adviseert deze met betrekking de invulling van het privacybeleid en de implementatie hiervan. Binnen deze rol zijn er de volgende taken/verantwoordelijkheden:
   - Vragen en klachten van mensen binnen en buiten de organisatie (laten) afhandelen
   - Interne regelingen ontwikkelen op het gebied van informatiebeveiliging en privacy
   - Adviseren over en uitvoeren van gegevensbeschermingseffectbeoordelingen (PIA)
   - Adviseren over technologie en beveiliging (privacy by design)
   - Bewustwording stimuleren van de bij de verwerking betrokken medewerkers
   - Input leveren bij het opstellen of aanpassen van een gedragscode

5.1.4 Security Specialist

De Security Specialist houdt zich bezig met het detecteren, analyseren en afhandelen van securityincidenten. Hiervoor wordt zowel de expertise van cybersecurity als verschillende (preventie- en detectie) middelen en tools gebruikt. De Security Specialist is constant bezig om deze middelen en kennis aan te passen aan de laatste ontwikkelingen op het gebied van beveiliging. Noorderpoort is een dynamische omgeving met, behalve persoonsgegevens, ook andere gevoelige informatie. Security staat daarom bij Noorderpoort hoog in het vaandel.

5.1.5 ICT Governance

Informatiebeveiliging en privacy moet onderdeel zijn van de normale bedrijfsprocessen, geïntegreerd in de normale praktijk en de al bestaande structuren en verantwoordelijkheden. Vandaar dat informatiebeveiliging en privacy wordt besproken binnen de stuurgroep ICT Governance. Beleid wordt onder verantwoordelijkheid van de Security Officer ingebracht, besproken en van advies voorzien richting het CvB. De stuurgroep ICT Governance onderhoudt en legt voor aan het CvB.

5.1.6 Informatiemanagement, ICT en HRM

Bij een aantal diensten/afdelingen zijn expliciete taken t.a.v. informatiebeveiliging en privacy belegd:

- Facilities (onderdeel huisvesting/gebouwbeheer):
  - Taken met betrekking tot fysieke informatiebeveiliging.
- Facilities (afdeling ICT):
  - Taken met betrekking tot technische en logische informatiebeveiliging van IT-functionaliteiten en informatiesystemen

- HRM:
  - Taken met betrekking tot informatiebeveiliging en privacy bij medewerkers
- Bestuursdienst (afdeling Informatiemanagement):
  - Taken met betrekking tot logische informatiebeveiliging van informatiesystemen
  - Actualisatie van beleid en procesverantwoordelijke voor informatiebeveiliging en privacy voor Noorderpoort

Informatiemanagement geeft invulling aan de beleidscyclus in opdracht van de Security Officer. Informatiemanagement heeft concreet als taak het vormgeven van het proces waarin het beleid actueel wordt gehouden binnen de kaders meegegeven door de stuurgroep ICT Governance en de Security Officer. Directbetrokkenen bij het aanpassen van het beleid zijn de informatiesysteemeigenaren en de beveiligingsspecialist vanuit de afdeling ICT. Input voor aanpassing komt vanuit de organisatie op basis van wijzigingen in processen, informatiesystemen, risicoanalyses of bijvoorbeeld incidenten.

Onderdeel van de beleidscyclus is de check en act. Dit wordt vormgegeven door Informatiemanagement. Middelen hiervoor zijn o.a.:

- Periodieke compliance rapportages
- Audits
- IT-audits (extern)
- Businesscases in het kader van veranderingen (inclusief change board checklist en privacy impact assessment)
- Incidentenoverzichten

5.1.7 Directeur school/dienst

Informatiebeveiliging en privacy is een verantwoordelijkheid van de lijn. Dit betekent dat de school- en dienstdirecteuren verantwoordelijk zijn voor de implementatie en operationele sturing met betrekking tot informatiebeveiliging en privacy aangaande hun afdelingen, medewerkers en processen.

5.1.8 Eigenaren informatiesystemen

Informatiesystemen ondersteunen processen die vaak afdeling overstijgend zijn. Vanuit de informatiearchitectuur is bepaald dat de eigenaar van het proces ook de eigenaar is van het ondersteunende informatiesysteem. Eigenaarschap houdt in dit geval ook verantwoordelijkheid voor de beveiliging en privacy van het informatiesysteem in.

5.1.9 Alle medewerkers

Alle medewerkers binnen Noorderpoort hebben toegang tot informatie. De medewerker is verantwoordelijk voor het zorgvuldig omgaan met deze informatie en daarnaast voor alle aspecten van informatiebeveiliging en privacy binnen de eigen invloedssfeer, zoals het zich houden aan de opgestelde richtlijnen.

5.1.10 Deelnemers

Alle deelnemers binnen Noorderpoort hebben toegang tot informatie. De deelnemer is verantwoordelijk voor het zorgvuldig omgaan met deze informatie en daarnaast voor alle aspecten van informatiebeveiliging en privacy binnen de eigen invloedssfeer, zoals het zich houden aan de opgestelde richtlijnen.

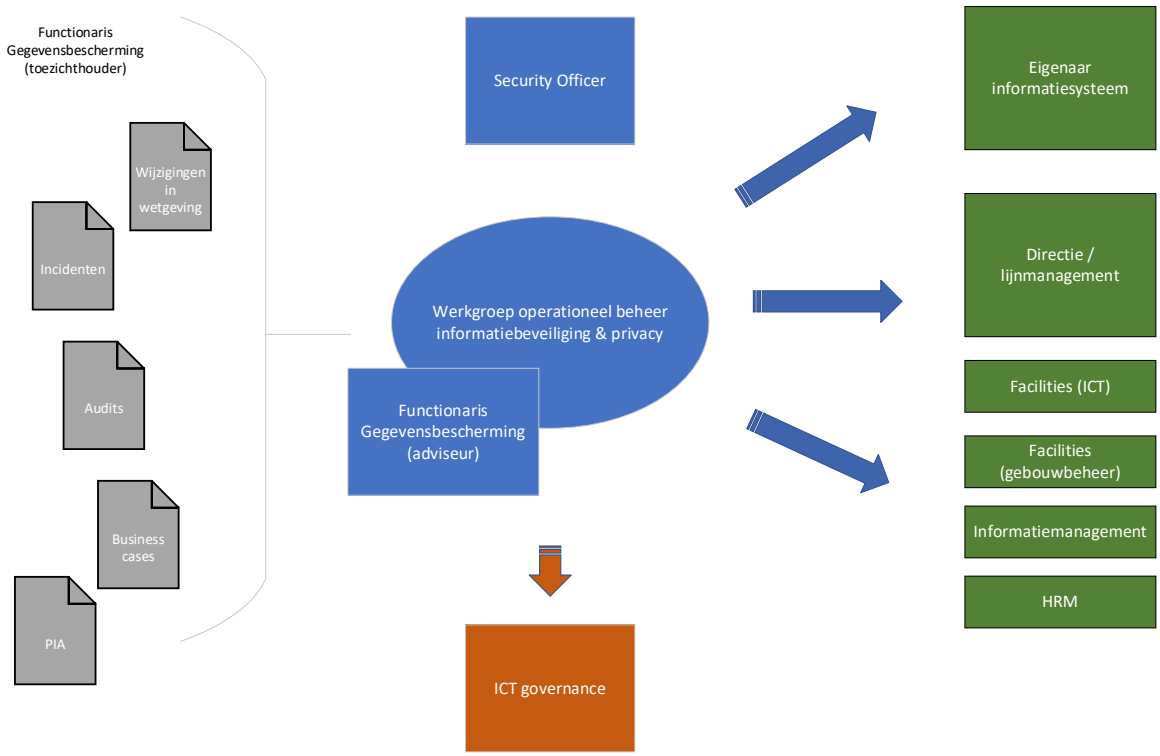
5.2 Organisatie en proces

Informatiebeveiliging en privacy is een integrale verantwoordelijkheid van het management. Dit betekent dat het onderdeel is van de normale taken en verantwoordelijkheden van lijnmanagement (directie en teammanagers) en eigenaren van informatiesystemen.
Om Noorderpoort breed te zorgen voor een adequate sturing op het thema zijn er een tweetal extra organisatiestructuren en processen. Deze worden hieronder beschreven.

5.2.1 Beleid en PDCA

Het is van belang om rondom informatiebeveiliging en privacy cyclisch te werken aan verbetering. In onderstaande schema wordt uitgelegd op welke wijze het Noorderpoort borgt dat er cyclisch aandacht is niet alleen voor het plannen en uitvoeren maar ook de controle en het verbeteren.

PDCA Noorderpoort informatiebeveiliging en privacy



Blauw: Werkgroep operationeel beheer informatiebeveiliging & privacy en Security Officer
Centraal in dit proces is de werkgroep operationeel beheer informatiebeveiliging & privacy. In deze werkgroep zit de gecombineerde expertise van Informatiemanagement en ICT (securityspecialist), aangevuld met de Functionaris Gegevensbescherming als adviseur.

De werkgroep rapporteert aan de Security Officer en richt zich op verbeteringen op gebied van beleid, proces en operationele aanpassingen.

Grijs: input
De werkgroep komt regelmatig bij elkaar en krijgt input vanuit diverse kanten:

- Aanpassingen in wetgeving worden bijgehouden
- Incidenten en incidentenrapportages
- Interne of externe audits (met daarbij ook benchmarks en IT-audit van de accountant)
- Businesscases n.a.v. nieuwe projecten of plannen
- PIA's (privacy impact assessments)

Groen: maatregelen in proces, systeem, operatie

Vanuit deze input wordt gekeken of er maatregelen nodig zijn t.a.v. informatiebeveiliging & privacy. Deze maatregelen worden besproken in de werkgroep, indien nodig met extra expertise, en uitgezet richting de diverse al bestaande organisatiestructuren. Deze kanalen zijn:

- Actie door en bij informatiesystemen, via de systeemeigenaren. Dit kan bijvoorbeeld aanpassing van autorisatie zijn of veranderingen in beheerprocessen.
- Actie door en bij de directie en de teammanagers, bijvoorbeeld rondom bewustwording van medewerkers en afspraken in teams.
- Specifieke maatregelen met betrekking tot ruimtes (Facilities), ICT, Informatiemanagement of HRM

Bruin: beleid

Op het moment dat aanpassing van beleid nodig is zal dit door de werkgroep worden voorbereid en via de Security Officer ingebracht worden bij de stuurgroep ICT Governance. Door deze opzet wordt optimaal gebruik gemaakt van al bestaande gremia en verantwoordelijkheden. De werkgroep en de Security Officer zorgen voor de integrale aanpassingen waar nodig.

5.2.2 Incidenten

Er zijn vier soorten incidenten die kunnen optreden met betrekking tot informatiebeveiliging en privacy:

- Reguliere IT-beveiligingsincidenten
  De escalatielijn loopt bij deze incidenten via eventueel de leidinggevende naar de Servicedesk en indien nodig naar de Security Specialist. Afhandeling van het incident gebeurt door de afdeling ICT in samenwerking met de security specialist (indien nodig), de lijnmanager en de betrokkene zelf.

- Fysieke beveiligingsincidenten (worden gemeld bij de gebouwenbeheerder)
  Bij fysieke beveiligingsincidenten zoals bijvoorbeeld diefstal loopt de escalatielijn (eventueel weer via de leidinggevende) naar Facilities (conciërge/hoofdconciërge /gebouwenbeheerder). Afhandeling gebeurt door Facilities in samenwerking met de afdeling ICT (indien nodig), de lijnmanager en de betrokkene zelf

- Beveiligingsincidenten met een vertrouwelijk karakter
  Voor deze incidenten is er een aparte escalatielijn. Incidenten worden gemeld bij de Security Officer of Security Specialist. Afhandeling van het incident gebeurt door Security Officer en de Security Specialist, indien nodig wordt hierbij de leidinggevende geïnformeerd/betrokken.

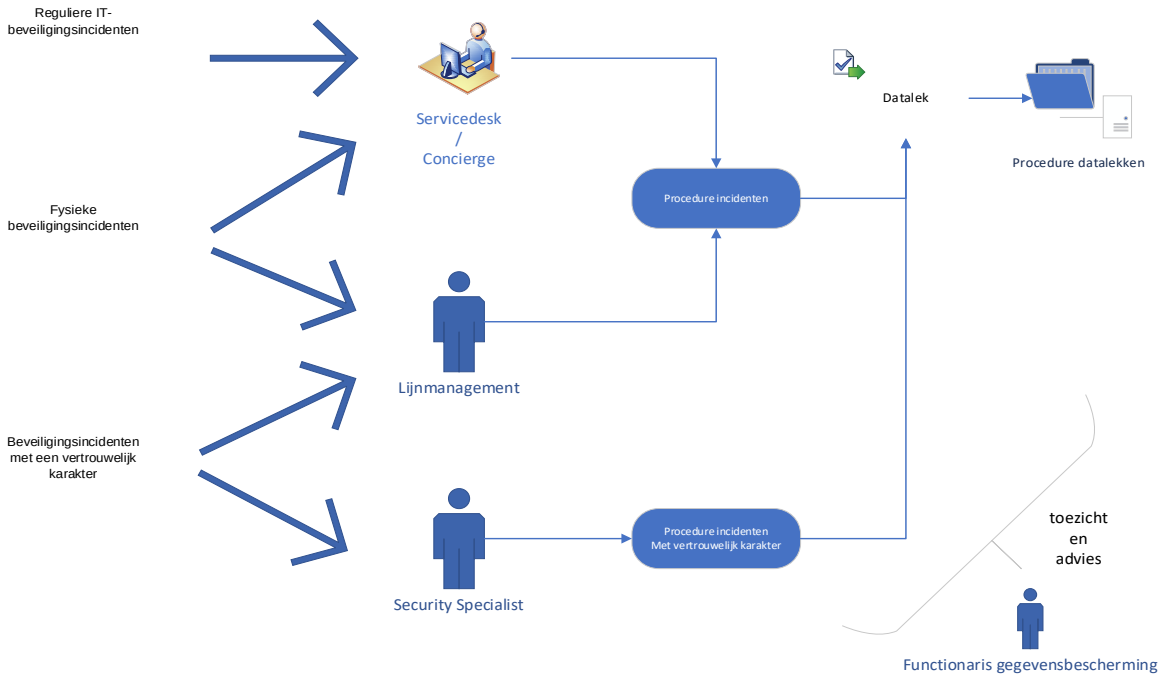
- Datalekken
  Een incident kan tot gevolg hebben dat er ook sprake is van een datalek. De afweging

hierbij wordt gedaan door de Security Specialist waarna in het geval van een datalek de procedure datalekken wordt gevolgd.

Belangrijk bij incidenten is naast de afhandeling ook de vertaalslag naar het verbeteren/leren van het incident. Vandaar dat alle incidenten worden geregistreerd en worden besproken binnen de werkgroep operationeel beheer informatiebeveiliging & privacy (zie ook 5.2.1).

De organisatie en processen rondom incidenten worden op de volgende pagina visueel weergegeven:

Incidenten proces Noorderpoort



De rol van de functionaris gegevensbescherming (FG) bij het incidentenproces is die van toezichthouder (hij/zij moet ook geïnformeerd worden) en adviseur. De eindverantwoordelijke voor het proces is de Security Officer.

6 Richtlijnen

De richtlijnen vormen het basisbeveiligingsniveau en zijn gericht op verschillende doelgroepen binnen Noorderpoort: leerlingen/studenten, medewerkers, het management en specifieke afdelingen. Bij het definiëren van de richtlijnen wordt uitgegaan van de kaders zoals deze in hoofdstuk 4 en 5 zijn gesteld. De richtlijnen zijn onderverdeeld in zes clusters:

- Beleid en organisatie
- Personeel, studenten en gasten
- Ruimtes en apparatuur
- Continuïteit
- Vertrouwelijkheid en integriteit
- Controle en logging

Met behulp van de bovenstaande zes clusters zijn de richtlijnen gegroepeerd die logischerwijs met elkaar samenhangen.

6.1 Beleid en organisatie

Statement	ISO
Het Informatiebeveiligings- en privacybeleid van Noorderpoort wordt gecommuniceerd met medewerkers en, voor zover relevant, met studenten en externen.	5.1.1.1, 5.1.1.2
Het CvB benoemd een Functionaris Gegevensbescherming en stelt een reglement vast met diens taken en bevoegdheden.	
Informatiebeveiliging en privacy vormen standaardonderdelen bij projectbeheer.	6.1.5
De uitgangspunten uit paragraaf 3.2.1 t/m 3.2.7 worden bij elke verwerking van persoonsgegevens nageleefd.	
Elke verwerking van persoonsgegevens wordt gemeld aan de Functionaris Gegevensbescherming die daartoe een register bijhoudt.	
Informatie binnen Noorderpoort is geclassificeerd op laag, midden of hoog op basis van de vereiste mate van beschikbaarheid, integriteit en vertrouwelijkheid. Deze classificatie wordt gebruikt voor het nemen van passende maatregelen op het gebied van informatiebeveiliging en privacy.	8.2.1, 8.2.2
Persoonsgegevens worden niet langer bewaard dan nodig is voor de doelen waarvoor zij verzameld zijn.	
Er zijn richtlijnen voor het gebruik van cryptografische beheersmaatregelen. In overeenstemming met de richtlijnen worden hiervoor applicaties beschikbaar gesteld.	10.1.1.1, 10.1.1.2

Noorderpoort heeft richtlijnen opgesteld voor het gebruik, de bescherming en de levensduur van cryptografische sleutels.	10.1.2.1
Noorderpoort verwerkt geen bijzondere persoonsgegevens tenzij daarvoor een wettelijke grond aanwezig is.	
Indien Noorderpoort bijzondere persoonsgegevens verwerkt, wordt de noodzaak daarvan gemotiveerd en worden extra beveiligingsmaatregelen getroffen.	
Indien Noorderpoort gebruik maakt van geautomatiseerde besluitvorming, is er altijd sprake van menselijke tussenkomst en toestemming van de betrokkene. De betrokkene wordt geïnformeerd over het besluitvormingsproces, mag daar over zijn zienswijze naar voren brengen en zich verzetten tegen het uiteindelijke besluit.	
Voor interne en externe informatie-uitwisseling zijn, ter bescherming en beveiliging van de informatie, richtlijnen, procedures en beheersmaatregelen van kracht.	13.2.1, 13.2.2
Met iedere leverancier of andere derde die persoonsgegevens voor of namens Noorderpoort verwerkt, wordt een verwerkersovereenkomst afgesloten. Deze wordt geregistreerd en gemeld aan de Functionaris Gegevensbescherming.	
Bij implementatie of uitbreiding van (nieuwe) informatiesystemen wordt rekening gehouden met de informatiebeveiligings- en privacy-eisen. Deze eisen zijn tevens bekendgemaakt aan elke leverancier die toegang heeft tot de IT-infrastructuur en/of informatie van Noorderpoort.	14.1.1, 15.1.2
Eisen in verband met informatiebeveiligings- en privacyrisico's worden benoemd in de overeenkomst tussen een leverancier en Noorderpoort. Bij wijzigingen in de dienstverlening worden deze eisen, indien nodig, herzien.	15.1.3
Conflicterende taken en verantwoordelijkheden worden binnen Noorderpoort gescheiden.	6.1.2

6.2 Personeel, studenten en gasten

Statement	ISO
Noorderpoort informeert betrokkenen beknopt, eenvoudig toegankelijk en begrijpelijk over de verwerking(en) en het privacybeleid.	
De arbeidsovereenkomst tussen Noorderpoort en haar medewerkers (arbeids- of werkrelatie) bevat hun verantwoordelijkheden m.b.t. informatiebeveiliging en privacy. In deze overeenkomst is voorzien in een vertrouwelijkheids- of geheimhoudingsbeding ten aanzien van de verwerkte persoonsgegevens.	7.1.2.
De eisen voor een vertrouwelijkheids- of geheimhoudingsovereenkomst zijn vastgesteld en worden regelmatig beoordeeld.	13.2.4
Alle medewerkers (met een arbeids- of werkrelatie) krijgen, voor zover relevant, een passende training op het gebied van informatiebeveiliging en privacy.	7.2.2
Noorderpoort stelt betrokkenen in staat om hun persoonsgegevens in te zien. Daarnaast hebben zij het recht om: • Gegevens te laten aanvullen en corrigeren • Gegevens te laten afschermen	

• Gegevens te laten verwijderen indien de gegevens onjuist, onvolledig of overbodig zijn (geworden). Betrokkenen kunnen een verzoek doen om volledig vergeten te worden. Verbetering, aanvulling en verwijdering worden zoveel als mogelijk doorgegeven aan alle personen en organisaties die de gegevens van Noorderpoort hebben ontvangen. Aan het verzoek tot verwijdering van gegevens en vergetelheid wordt slechts voldaan voor zover er geen bewaarplicht geldt.	
Toegangsrechten voor informatie of informatiesystemen worden bij beëindiging van het dienstverband, of bij wijziging van de functie, ingetrokken/gewijzigd.	9.2.6
Binnen Noorderpoort geldt zowel een clear desk- als een clear screen-beleid.	11.2.9
Van alle medewerkers (met een arbeids- of werkrelatie) die gebruik maken van informatiesystemen en -diensten wordt verwacht dat ze zwakke plekken op het gebied van informatiebeveiliging en privacy, in systemen of diensten rapporteren.	16.1.3
Verificatie van de achtergrond van alle kandidaten wordt uitgevoerd in overeenstemming met de relevante wet- en regelgeving en staat in verhouding met de functie en informatietoegang.	7.1.1

6.3 Ruimten en apparatuur

Statement	ISO
Bij verwijdering of hergebruik van apparatuur/opslagmedia, dient er een controle plaats te vinden op de aanwezigheid van gevoelige gegevens, persoonsgegevens en in licentie gegeven software. Deze gegevens/software dient te worden verwijderd/overschreven.	11.2.7
Media worden op een veilige manier verwijderd als ze niet langer nodig zijn. Hiervoor zijn formele procedures opgesteld.	8.3.2
Medewerkers van Noorderpoort tekenen een bruikleenovereenkomst voor mobiele apparatuur. Deze overeenkomst heeft betrekking op het gebruik van hard- en software, maar ook op het gebied van de verantwoordelijkheden en risico's op het gebied van informatiebeveiliging en privacy.	6.2.1.2 6.2.1.1, 11.2.5,
Binnen Noorderpoort zijn beveiligingszones gedefinieerd om gebieden met gevoelige informatie te beschermen. Deze beveiligde gebieden worden beschermd door een passende toegangsbeveiliging.	11.1.1, 11.1.2
Voor kantoren, ruimten en faciliteiten is fysieke beveiliging ontworpen en toegepast. Ook is er sprake van fysieke bescherming tegen natuurrampen, kwaadwillige aanvallen of ongelukken.	11.1.3, 11.1.4
Voor het werken in beveiligde gebieden binnen Noorderpoort zijn procedures ontwikkeld.	11.1.5
Punten waar onbevoegde personen het terrein kunnen betreden worden beheerst en afgeschermd van informatie verwerkende faciliteiten.	11.1.6

Apparatuur wordt binnen Noorderpoort op een dusdanige manier geplaatst en beschermd, dat de kans op onbevoegde toegang, verstoringen en overige bedreigingen is geminimaliseerd.	11.2.1, 11.2.2
Voedings-, telefonie- en internetkabels worden beschermd tegen interceptie, verstoring of schade.	11.2.3
Apparatuur binnen Noorderpoort wordt goed onderhouden zodat de beschikbaarheid en integriteit gewaarborgd is.	11.2.4
Bedrijfsmiddelen buiten het terrein worden op een passende manier beveiligd, rekening houden met de mogelijke risico's.	11.2.6

6.4 Continuïteit

Statement	ISO
Noorderpoort gaat zorgvuldig om met de verwerkte persoonsgegevens en waarborgt het behoud en bescherming van de juistheid en de consistentie van die gegevens.	
Alle veranderingen binnen Noorderpoort die van invloed zijn op informatiebeveiliging en privacy dienen te worden beheerst.	12.1.2
Beveiligingsincidenten die (vermoedelijk) leiden tot ongeoorloofde vernietiging, verlies, wijziging, toegang of verstrekking van persoonsgegevens zijn datalekken en moeten worden gemeld bij de ICT-Servicedesk of de Security Specialist. Noorderpoort heeft een procedure voor datalekken.	
Informatiebeveiligings- en privacy gebeurtenissen worden zo snel mogelijk, via de vaste procedures en verantwoordelijkheden, gerapporteerd.	16.1.1, 16.1.2
Bij alle informatiebeveiligings- en privacy gebeurtenissen wordt gekeken of ze geclassificeerd dienen te worden als informatiebeveiligingsincident. Hierop wordt vervolgens gereageerd in overstemming met de opgestelde procedures.	16.1.4, 16.1.5
Productieomgevingen zijn binnen Noorderpoort gescheiden van de OTA-omgevingen.	12.1.4
Binnen Noorderpoort zijn maatregelen genomen ter bescherming tegen malware.	12.2.1.1, 12.2.1.2
Om de continuïteit van informatie te waarborgen neemt Noorderpoort diverse maatregelen, waaronder back-ups. Deze maatregelen worden periodiek getest en gelogd.	12.3.1.1
Technische kwetsbaarheden binnen gebruikte informatiesystemen worden geëvalueerd en er worden passende maatregelen genomen om het risico dat daarmee samenhangt te verkleinen.	12.6.1
Noorderpoort streeft ernaar om, door middel van diverse processen, procedures en beheersmaatregelen, het vereiste niveau van continuïteit en beschikbaarheid voor informatiebeveiliging te waarborgen.	17.1.2, 17.2.1

6.5 Vertrouwelijkheid en integriteit

Statement	ISO
Binnen Noorderpoort is een beleid voor toegangsbeveiliging vastgelegd, zodat gebruikers alleen toegang hebben tot het netwerk en diensten/systemen waartoe zij toegang moeten hebben op basis van hun werkzaamheden.	9.1.1, 9.1.2, 9.2.1
Zowel logfaciliteiten als de logbestanden zelf worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2
Het Noorderpoortnetwerk wordt beheerd en beheerst om informatie in zowel systemen als in toepassingen te beschermen.	13.1.1
Informatie in elektronische berichten worden passend beschermd.	13.2.3

6.6 Controle en logging

Statement	ISO
Bij het gebruiken en/of ontwerpen van informatiesystemen en processen die persoonsgegevens verwerken, worden privacyregels zoals privacy by design en privacy by default aangehouden.	
De systeemeigenaren beoordelen periodiek de toegangsrechten van gebruikers.	9.2.5
Noorderpoort voert een (tweejaarlijks terugkerende) evaluatie uit van de mogelijke effecten van de verschillende gegevensverwerking op de rechten en vrijheden van de betrokkenen. Deze evaluatie vindt eveneens plaats in geval van een wijziging in de verwerking van persoonsgegevens die specifiek de risico's wijzigt voor de privacy van de betrokken deelnemers en medewerkers.	
Logbestanden die activiteiten en gebeurtenissen registreren worden bewaard en steekproefsgewijs beoordeeld. Dit geldt in het bijzonder voor activiteiten van systeembeheerders en –operators.	12.4.1, 12.4.3
Er wordt regelmatig gecontroleerd of de mensen, processen en systemen werken volgens het Informatiebeveiligings- en privacybeleid en andere eisen en normen op het gebied van informatiebeveiliging en privacy.	18.2.2.
Zowel interne als externe systeemontwikkeling staat onder supervisie van en wordt gemonitord door de organisatie.	14.2.7
Bij het implementeren van nieuwe informatiesystemen, of bij wijzigingen bij bestaande informatiesystemen, worden acceptatietests uitgevoerd.	
In informatiesystemen met persoonsgegevens vindt altijd logging plaats. Beheerders hebben niet de mogelijkheid om logbestanden van eigen activiteiten te wissen. Er worden bewaartermijnen vastgesteld voor de logbestanden.	
Noorderpoort monitort, beoordeeld en audit regelmatig de dienstverlening van haar leveranciers.	15.2.1
Noorderpoort heeft een procedure voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	16.1.7

Informatiesystemen worden technisch inhoudelijk beoordeeld op naleving van de beleidsregels en normen voor informatiebeveiliging.	18.2.3