Informatiebeveiligings- en privacy beleid

Versie: januari 2026



Documentgeschiedenis

Revisies

Versie	Datum	Auteur	Review
1.0	01-09-2025	Chris de Beer	Alex Raaijmakers Rob van Son
1.1	directeur-bestuurder	Roderik Rot	9-01-2026

Vaststelling

Naam	Functie	Versie	Datum
Schoolleiding			
RvT		1.2	10-02-2026
MR		1.2	02-02-2026

Documentclassificatie

Classificatie	Beschrijving
Openbaar	Dit document mag worden gepubliceerd op de website van het Erasmus College in een vorm welke niet is aan te passen of te kopiëren of distribueren. *www.erasmuscollege.nl*
Intern	Dit document mag als bestand in .PDF format worden gedeeld met en gedistribueerd onder zowel interne als externe medewerkers van Erasmus College .

Inhoudsopgave

Managementsamenvatting **7**

1 Inleiding **8**

1.1 Onze intentie 8

1.2 Missie, Visie en Strategie 9

1.3 Doelstelling 9

1.4 Reikwijdte en toepassingsgebied 9

1.5 Informatiebeveiliging en Security 10

1.6 Privacy & Gegevensbescherming (AVG) 10

1.7 Adequate technische en organisatorische beveiligingsmaatregelen 10

2 Context van de Instelling **12**

2.1 De Instelling en haar context 12

2.2 Wet- en regelgeving en normenkaders 12

2.3 De behoefte en verwachtingen van belanghebbenden 13

3 Management, eigenaarschap en verantwoordelijkheden **15**

3.1 Uitgangspunten van ons beleid 15

3.2 Structuur van ons beleid 15

3.3 Betrokkenheid, leiderschap en verantwoordelijkheden 15

3.3.1 Betrokkenheid en leiderschap 15

3.3.2 Rollen en verantwoordelijkheden 16

3.3.3 Medezeggenschap 16

3.3.4 Functiescheiding 16

3.3.5 Ketenbeheer en leverancier (risico)management 16

3.4 Three Lines model 17

3.4.1 Eerste lijn: eindverantwoordelijkheid bij het bestuur 17

3.4.2 Tweede lijn: adviseren en ondersteunen 18

3.4.3 Derde lijn: onafhankelijke controle 18

3.4.4 Rapportage 18

3.5 Architectuur 19

4 Beleidsthema's informatiebeveiliging 20
4.1 Verdeling verantwoordelijkheden ICT & Netwerkbeheer 20
4.2 Risicomanagement 20
4.3 Kennis en afhankelijkheid medewerkers 20
4.4 Bedrijfscontinuïteit 21
4.5 Back-up en herstel 21
4.6 Fysieke beveiliging 22
4.7 Systeem- en data-eigenaarschap en configuratiebeheer 22
4.8 Classificatie van systemen en data 23
4.9 Beveiligingsbaseline 23
4.10 Bewustwording en afhankelijkheid medewerkers 24
4.11 Incident- en problemmanagement 25
4.12 Risicomanagement leveranciers 25
4.13 Werkplekken en mobiele apparaten 26
4.14 Identiteits- en toegangsbeheer 26
4.15 Vulnerabilitymanagement en pentesting 26
4.16 Patchmanagement 27
4.17 Logging 27
4.18 Digitaal sleutelbeheer 27

5 Uitgangspunten Privacy en Gegevensbescherming (AVG) 29
5.1 Persoonsgegevens 29
5.2 Privacy principes 29

6 Beleidsthema's privacy 32
6.1 Verwerkingsregister 32
6.1.1 Legitiem doel en doelbinding 32
6.1.2 Grondslag 33
6.2 Informatieplicht 33
6.3 Toestemming 34
6.4 Privacy by design en privacy by default 34
6.5 Dataminimalisatie 34
6.6 Bewaartermijnen 35
6.7 Afhandelen van datalekken 35

6.8 Data Protection Impact Assessment ... 35
6.9 Uitwisseling persoonsgegevens ... 36
6.10 Gegevensverwerking buiten de EER ... 36
6.11 Rechten van betrokkenen ... 37
6.12 Geautomatiseerde besluitvorming en profilering ... 37
6.13 Naleving AVG ... 37
6.14 Functionaris gegevensbescherming (FG) ... 38

7 Continu verbeteren ... 39
7.1 Audits en compliance monitoring ... 39
7.2 Audit-proces ... 39
7.2.1 Auditjaarplanning ... 40
7.2.2 Auditplanning ... 40
7.2.3 Auditwerkzaamheden ... 40
7.2.4 Afronding van een audit ... 41
7.2.5 Rapportage ... 41
7.2.6 Resultaten ... 41
7.3 Directiebeoordeling en strategische evaluatie ... 41
7.4 Afwijkingen en corrigerende maatregelen ... 41

8 Vaststelling en beleidsherziening ... 43

Bijlage 1 Beleidspiramide ... 44
Strategisch beleid ... 44
Tactisch beleid ... 44
Processen ... 44
Operationele documentatie ... 44
Bijlage 2 Certificeringsschema ROSA ... 46
Kernpunten van het schema: ... 46
Toepassing in 2026: ... 46
Bijlage 3 FORA-processen ... 47
Belangrijkste kenmerken van FORA-processen (2026) ... 47
Algemene procesindeling ... 47
Bijlage 4 BIV classificatie ... 48

Hoe werkt het? 48
Bijlage 5 Overzicht met IBP onderwerpen voor de MR 49
Bijlage Afkortingen 50

Managementsamenvatting

Dit IBP-beleid (Informatiebeveiliging en Privacy) van het Erasmus College beschrijft de strategie en maatregelen om een veilige en betrouwbare leer- en werkomgeving te waarborgen. Het beleid is gebaseerd op wettelijke verplichtingen (AVG) en internationale best practice (ISO 27001).

Kernpunten:

- Doel: Bescherming van persoonsgegevens en bedrijfsinformatie tegen verlies, misbruik en onbevoegde toegang.
- Reikwijdte: Alle informatie, digitaal en fysiek, voor medewerkers, leerlingen en externe partijen.
- Governance: Heldere rollen en verantwoordelijkheden volgens het Three Lines model.
- Beveiligingsmaatregelen: Risicomanagement, toegangsbeheer, back-up, continuïteit en incidentrespons.
- Privacy: Naleving van AVG, verwerkingsregister, DPIA's en rechten van betrokkenen.
- Verbetercyclus: Jaarlijkse audits, managementreviews en PDCA-aanpak voor continue verbetering.

Dit beleid ondersteunt de missie van het Erasmus College om een veilige, transparante en toekomstbestendige omgeving te bieden. De directeur-bestuurder is eindverantwoordelijk voor de borging en naleving van dit beleid.

1 Inleiding

Dit document beschrijft het Informatiebeveiliging en Privacy beleid van het Erasmus College vanaf datum ondertekening door De directeur-bestuurder van het Erasmus College en vervangt hiermee het voorgaande beleid.

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Lesmateriaal wordt digitaal aangeboden, toetsingsprogramma's worden digitaal en de resultaten en ontwikkelingen van leerlingen worden opgenomen in een digitaal leerlingvolgsysteem. Daarnaast wordt ook veel gebruikgemaakt van digitale communicatie tussen de school, leerlingen en ouders/verzorgers. Door deze ontwikkelingen neemt het risico op verstoring van het onderwijs, verlies of misbruik van gegevens en overmatige dataverzameling toe. Het is de verantwoordelijkheid van het Erasmus College om dat te voorkomen en een veilige leeromgeving te bieden.

Dit beleid voor informatiebeveiliging en privacy (IBP-beleid) beschrijft hoe het Erasmus College omgaat met de beveiliging van informatie en hoe de verwerking van (persoons)gegevens wordt gewaarborgd en gehandhaafd. In het beleid worden de verschillende rollen en verantwoordelijkheden binnen het Erasmus College op het gebied van informatiebeveiliging en privacy (IBP) beschreven.

Dit Informatiebeveiliging en Privacy beleid, gebaseerd op NEN-ISO/IEC 27001:2023 en eisen en voorwaarden uit de Algemene Verordening Gegevensbescherming (hierna AVG) als ook de Uitvoeringswet AVG (hierna UAVG), stelt kaders en geeft richting. Op tactisch en operationeel niveau is dit beleid aangevuld met onderwerp specifieke documenten (standaarden, richtlijnen, procedures en handleidingen). Zie bijlage 1 van dit beleid voor een verdere uitwerking hiervan.

1.1 Onze intentie

Het Erasmus College draagt de verantwoordelijkheid voor het creëren van een veilige werk- en leeromgeving. Dit houdt in dat het Erasmus College passende technische en organisatorische maatregelen toepast om informatie te beschermen en ongeoorloofde toegang, verlies of misbruik te voorkomen.
Het recht op privacy is een grondrecht. Iedereen heeft recht op privacy en bescherming van de persoonlijke levenssfeer. Dit geldt vanzelfsprekend ook voor leerlingen, ouders/verzorgers, medewerkers van school. Het Erasmus College is verantwoordelijkheid voor het waarborgen van de privacy van de leerlingen en het personeel. Dit betekent ook dat deze betrokkenen zeggenschap hebben over het gebruik van hun persoonsgegevens, zoals wettelijk bepaald.
Bij het Erasmus College staat het bieden van goed onderwijs voorop. Om dit te kunnen doen verwerken wij diverse persoonsgegevens van leerlingen, ouders/verzorgers, medewerkers (personeel in loondienst en personeel niet in loondienst) en docenten. Het Erasmus College vindt het belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van informatiebeveiliging en privacy in een beleid is noodzakelijk om de gevolgen van mogelijke informatiebeveiliging- en privacy risico's tot een aanvaardbaar niveau terug te brengen en de voortgang van het onderwijs te kunnen waarborgen.

1.2 Missie, Visie en Strategie

Missie

We streven naar een scholengemeenschap die voor medewerkers, leerlingen en ouders herkenbaar is en blijft voor opeenvolgende generaties. Herkenbaar als de bruisende daltonschool, die meer biedt dan het maatschappelijk zo belangrijke diploma. Een school waar je met plezier aan terugdenkt als een van de belangrijkste periodes in je leven.

Visie in relatie tot Informatiebeveiliging en Privacy

Het Erasmus College wil een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door het Erasmus College verzamelde, verwerkte en gepubliceerde informatie te allen tijde beschikbaar, correct en beschermd is. Dit vraagt om een strategisch samenhangende aanpak van Informatiebeveiliging en het waarborgen van privacy, die aantoonbaar aan de eisen voldoet, om blijvend een veilige en toekomstbestendige leer- en werkomgeving beschikbaar te stellen.

Strategie

Het Erasmus College wil groeien naar een professionele organisatie, waar op een veilige manier onderwijs verzorgd en ondersteund kan worden. In aansluiting hierop wil het Erasmus College met een strategische aanpak op het gebied van informatiebeveiliging en privacy groeien naar een professioneel volwassen organisatie, waar op een veilige manier met informatie wordt omgegaan en de privacy en rechten en vrijheden van de betrokkenen van het Erasmus College zijn gewaarborgd.

1.3 Doelstelling

Het Erasmus College versterkt met dit Informatiebeveiliging en Privacy beleid de cyberweerbaarheid, de groei in het volwassenheidsniveau van haar organisatie en de bescherming van informatie en persoonsgegevens van de betrokkenen van de organisatie. Hiermee borgen we een veilige leer- en werkomgeving voor onze leerlingen, ouders, medewerkers en overige betrokkenen.
Het uitgangspunt is dat een veilige werk- en leeromgeving wordt gecreëerd, de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en het Erasmus College voldoet aan relevante wet- en regelgeving. Dit gebeurt onder andere door bewustwording te vergroten over het belang van het zorgvuldig omgaan met informatie, systemen en persoonsgegevens.
Het Erasmus College maakt gebruik van het 'Normenkader Informatiebeveiliging en Privacy voor het funderend onderwijs' - oftewel het Normenkader IBP-FO - om inzichtelijk te maken waar de organisatie nu staat en welke maatregelen genomen moeten worden om een veilige leer- en werkomgeving te creëren en te voldoen aan de AVG.

1.4 Reikwijdte en toepassingsgebied

Bij het Erasmus College wordt informatiebeveiliging en de bescherming van de privacy van betrokkenen breed geïnterpreteerd. Het heeft betrekking op alle vormen van formeel en informeel vastgelegde informatie (dus niet alleen digitale informatie), die het Erasmus College of haar relaties en ketenpartners genereren en beheren.

Dit beleid is van toepassing op alle leerlingen, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van het Erasmus College. Het beleid heeft betrekking op de verwerking van alle soorten gegevens en informatie waaronder; persoonsgegevens, bedrijfsinformatie en technische gegevens. Het is van toepassing op alle gegevensverwerkingen die onder de AVG vallen.

Het beleid is tijd- en locatie-onafhankelijk en geldt dus 24x7 ook als men op een andere locatie dan op het terrein van het Erasmus College met informatie of informatievoorziening van het Erasmus College werkt, zoals thuis, in de trein, bij een andere organisatie of tijdens reizen naar het buitenland.

1.5 Informatiebeveiliging en Security

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.

Het Informatiebeveiliging en Privacy beleid geldt voor alle processen van het Erasmus College en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het bestuur, alle medewerkers, leerlingen en ouders, vrijwilligers, stagiaires, gasten, bezoekers en overige externe relaties en ketenpartners.

1.6 Privacy & Gegevensbescherming (AVG)

Het Erasmus College werkt met (persoons)gegevens van medewerkers, leerlingen en ouders, vrijwilligers, stagiaires, gasten, bezoekers en overige externe relaties en ketenpartners.
Deze gegevens verzamelt het Erasmus College voor het goed kunnen uitvoeren van haar wettelijke onderwijstaken en andere maatschappelijke bijdragen welke zij wenst te realiseren gerelateerd aan het organiseren en realiseren van onderwijs.

Bij de omgang met persoonsgegevens van alle betrokkenen van de instelling heeft de organisatie van het Erasmus College een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverleningen binnen de huidige informatie maatschappij, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele onderwijs organisatie en verdient, samen met informatiebeveiliging, continu aandacht. Alle betrokkenen moet erop kunnen vertrouwen dat het Erasmus College zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.7 Adequate technische en organisatorische beveiligingsmaatregelen

Zoals beschreven in artikel 32 van de AVG zijn organisaties verplicht tot het treffen van passende technische en organisatorische beveiligingsmaatregelen om persoonsgegevens te beschermen. Dit moet gebeuren op basis van de risico's voor de rechten en vrijheden van betrokkenen, de aard, omvang

en doeleinden van de gegevensverwerking en rekening houdend met de stand van de techniek van vandaag. Technische en organisatorische beveiligingsmaatregelen zijn essentieel voor het beschermen van gegevens en systemen, en vullen elkaar aan om een alomvattend beveiligingskader te creëren. Dit beveiligingskader richt zich op zowel Informatiebeveiliging als Privacy waarborging, als ook op zowel digitale en fysieke informatiedragers.

Technische maatregelen maken gebruik van technologie om informatiesystemen en netwerken te beschermen tegen cyberdreigingen. Ze zijn gericht op de technische infrastructuur. Ze vormen een belangrijk onderdeel van de beveiliging en kunnen worden aangevuld met maatregelen zoals sleutel- en toegangsbeheer, sluitrondes, risico-inventarisaties, en het creëren van beveiliging en privacy bewustzijn bij medewerkers.

Organisatorische maatregelen zijn gericht op de menselijke en procesmatige aspecten van een organisatie. Het zijn beleidsregels, procedures en werkafspraken die bepalen hoe medewerkers met informatie en systemen moeten omgaan om de beveiliging en privacy te waarborgen. Deze procedures en beleid die de beveiliging binnen een organisatie versterken, omvatten zeker ook het toewijzen van rollen, taken, verantwoordelijkheden en bevoegdheden, het opstellen van huisregels, en het continue trainen en opleiden van alle medewerkers, intern en extern.

2 Context van de Instelling

2.1 De Instelling en haar context

Onze onderwijsinstelling helpt leerlingen in een kwetsbare levensfase groeien en ontwikkelen en vervult een maatschappelijke rol in haar regio. Daarnaast wordt onderwijs veelal verricht op basis van publieke financiering hetgeen vraagt om transparantie en zorgvuldigheid van onze bedrijfsvoering. Diezelfde transparantie wordt verwacht ten aanzien van het verwerken van persoonsgegevens van alle betrokkenen van het Erasmus College . Tegelijkertijd verwachten ketenpartners en andere organisaties waar we mee samenwerken dat hun informatie vertrouwelijk wordt behandeld. Op basis van het cyberdreigingsbeeld bevat dit beleidsdocument de uitgangspunten voor informatiebeveiliging en privacy waarborging om daarmee een bijdrage te leveren aan de kennisveiligheid binnen het Erasmus College en het ecosysteem waarin wij ons bevinden. Dit document vormt de basis om eisen aan de beschikbaarheid, integriteit en vertrouwelijkheid van processen, bedrijfsinformatie, persoonsgegevens en systemen te realiseren.

2.2 Wet- en regelgeving en normenkaders

Wet- en regelgeving

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

- Wet op het voortgezet onderwijs en/of Wet op de expertisecentra
- Wet onderwijstoezicht
- Archiefwet en Archiefbesluit
- Leerplichtwet
- Wet medezeggenschap op scholen
- Arbeidsregelgeving en CAO
- Belastingwetgeving
- Telecommunicatiewet en e-privacy wetgeving

De EU-wetgevingmonitor biedt een actueel overzicht van Europese wet- en regelgeving op het gebied van digitalisering, data, cybersecurity, digitale identiteit en meer.
Doel van de monitor is het vroegtijdig bieden van inzicht in nieuwe wetgeving. Hiermee zorgt de monitor voor tijdige voorbereiding en betere strategische besluitvorming.

https://eu-wetgevingsmonitor.realisatieibds.nl/

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 en Functionaris gegevensbescherming.

Binnen het Erasmus College is de directeur-bestuurder verantwoordelijk gesteld om de wijzigingen in de van toepassing zijnde wetgeving voor het Erasmus College, in het kader van Informatiebeveiliging en Privacy, te monitoren en relevante afdelingen en functionarissen tijdig te informeren en adviseren wanneer van toepassing en noodzakelijk.

Normenkaders

Intern uitgangspunt voor dit document is het Programma Digitaal Veilig Onderwijs (DVO).
Het Programma Digitaal Veilig Onderwijs (DVO) is een initiatief van het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad om scholen in het primair en voortgezet onderwijs te helpen bij het creëren van een digitaal veilige omgeving.

Een belangrijk onderdeel is de implementatie van het Normenkader Informatiebeveiliging en Privacy (IBP), waarbij scholen uiterlijk in 2030 aan bepaalde volwassenheidsniveaus moeten voldoen. Het kader, ook wel het IBP-FO normenkader, biedt normen en richtlijnen om de informatiebeveiliging van een instelling te toetsen, verbeteren en aantoonbaar te maken. Het framework helpt bij het waarborgen van de continuïteit en veiligheid van gegevens en de privacy van alle betrokkenen van het Erasmus College . Dit normenkader wordt actief ingezet en benut door het Erasmus College vanuit een Governance Risk en Compliance applicatie Privacy Control Center (GRC-applicatie).

Extern uitgangspunten voor dit document en de samenstelling van het IBP-FO normenkader zijn enerzijds de NEN-ISO/IEC 27001:2023-norm aangezien dit wereldwijd de ‘best practice’ vormt voor informatiebeveiliging op strategisch niveau. En anderzijds de eisen en voorwaarden uit de Algemene Verordening Gegevensbescherming (AVG) en de binnen Nederland geldende uitvoeringswet hiervan, de UAVG.

2.3 De behoefte en verwachtingen van belanghebbenden

De verwachtingen zijn afhankelijk van de rol van de belanghebbenden.

- Medewerkers verwachten een omgeving waarin de data en systemen voor het werk betrouwbaar en veilig zijn en waarin hun privacy geborgd is.
- Leerlingen en ouders verwachten een omgeving waarin de data en systemen voor de opleiding of studie betrouwbaar en veilig zijn en waarin hun privacy geborgd is.
- Alle overige betrokkenen van het Erasmus College verwachten dat hun gegevens veilig zijn en hun privacy geborgd is.
- Onderwijsinstellingen, ketenpartners en stagebedrijven verwachten een vertrouwelijke en betrouwbare omgang met hun informatie en de persoonsgegevens van hun betrokkenen. Daarnaast mag onze omgeving geen bron vormen van eventuele malafide activiteiten.
- Het Ministerie van OCW verwacht dat ons bestuur controle heeft over de staat van de informatiebeveiliging, persoonsgegevens verwerkt volgens eisen en voorwaarden uit de AVG, en in staat is om daar in detail over te rapporteren.
- Koepelorganisaties verwachten dat we gezamenlijk in staat zijn om als sector een veilig ecosysteem te realiseren.

Deze verwachtingen vormen de basis voor een correcte classificatie van data, (bedrijfs-) informatie en persoonsgegevens, om vervolgens bijpassende technische, fysieke, mensgerichte en/of organisatorische maatregelen te kunnen toepassen.

Om te voorkomen dat de hiervoor genoemde verwachtingen van belanghebbenden geschaad worden, organiseren we onze informatieveiligheid en privacy waarborging met behulp van dit IBP beleid. Hiermee monitoren en verbeteren we continue de informatiebeveiliging binnen alle processen in onderwijs, bedrijfsvoering en daaruit voortvloeiende activiteiten die namens en/of voor het Erasmus College worden uitgevoerd.

3 Management, eigenaarschap en verantwoordelijkheden

3.1 Uitgangspunten van ons beleid

Centraal uitgangspunt van ons beleid zijn de gebruikers van onze informatie en systemen. Om de beschikbaarheid, integriteit en vertrouwelijkheid te borgen hanteren we de volgende uitgangspunten. Binnen het Erasmus College:

- **werken we risico gebaseerd**
  We baseren de te treffen maatregelen op de mogelijke veiligheidsrisico's van onze gegevens, processen, informatievoorzieningen en -systemen en op de risicobereidheid (risk appetite) van de directeur-bestuurder.
- **is iedereen verantwoordelijk**
  Iedereen voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
- **wordt het informatiebeveiliging en privacy beleid altijd en overal gevolgd**
  Informatiebeveiliging en privacy waarborging zit in het DNA van het Erasmus College en is integraal onderdeel van al onze werkzaamheden.
- **hanteren we Security en Privacy by Design**
  Informatiebeveiliging en bescherming van persoonsgegevens en privacy is vanaf de start een integraal onderdeel van ieder project of iedere verandering van onze gegevens, processen, informatievoorzieningen en -systemen.
- **hanteren we Security en Privacy by Default**
  Informatievoorzieningen en -systemen standaard zijn geconfigureerd met de meest veilige instellingen.
- **heeft iedereen toegang tot alleen dat wat nodig is**
  Gebruikers hebben alleen toegang tot gegevens, processen, informatievoorzieningen en -systemen passend bij hun functie en rollen.
- **gaan we uit van controle in plaats van blind vertrouwen (Zero Trust principe)**
  We hanteren een gelaagd beveiligingsmodel waarbij we verifiëren of aan voorwaarden voor toegang tot en het gebruik van gegevens, processen, informatievoorzieningen en -systemen is voldaan.

3.2 Structuur van ons beleid

De structuur van ons beleid is opgebouwd in vier lagen (zie Bijlage 1 Beleidspiramide). De bovenste laag is het strategisch Informatiebeveiliging en Privacy beleid en is beschreven in dit document. Verdere specificering van het Informatiebeveiliging en Privacy beleid is vastgelegd in de onderliggende standaarden, richtlijnen, procedures en handleidingen.

3.3 Betrokkenheid, leiderschap en verantwoordelijkheden

3.3.1 Betrokkenheid en leiderschap

De directeur-bestuurder toont leiderschap en betrokkenheid door ervoor te zorgen dat het Informatiebeveiliging en Privacy beleid en de doelstellingen in lijn zijn met de strategische richting van het Erasmus College. De eisen van het IBP beleid integreren we in de processen van onderwijs en bedrijfsvoering. De directeur-bestuurder communiceert het belang van effectieve informatiebeveiliging

en privacy waarborging, zorgt dat de doelstellingen worden behaald, ondersteunt medewerkers in hun bijdragen aan het beleid, bevordert continue verbetering en spreekt andere managementrollen aan op hun verantwoordelijkheden.

3.3.2 Rollen en verantwoordelijkheden

Een belangrijk onderdeel van effectieve informatiebeveiliging en privacy waarborging binnen het Erasmus College is het kunnen vertrouwen dat de organisatie-inrichting zo is dat alle betrokkenen hun verantwoordelijkheden kennen en hun rollen en taken op de juiste manier en met de juiste bevoegdheden uitvoeren. Dit zijn de zaken die worden gevat onder de term governance.

De directeur-bestuurder draagt er zorg voor dat er binnen het Erasmus College duidelijkheid bestaat over verantwoordelijkheden en bevoegdheden van rollen met betrekking tot informatiebeveiliging en privacy waarborging. De directeur-bestuurder kent de verantwoordelijkheden en bevoegdheden toe voor het waarborgen van de naleving van het Informatiebeveiliging en Privacy beleid en voor het rapporteren over de prestaties ervan.

3.3.3 Medezeggenschap

Het Erasmus College betrekt de medezeggenschapsraad (MR) bij besluiten over regelingen en procedures ten aanzien van Informatiebeveiliging en Privacy waarborging. De directeur-bestuurder is eindverantwoordelijk voor het informeren van de medezeggenschapsraad en voor het opstellen van instemmingsprocedures. De directeur-bestuurder is ook bepalend in welke beleidsdocumenten en protocollen instemming vereisen van de medezeggenschapsraad. Een overzicht hiervan is opgenomen in bijlage 2 van dit beleid.

3.3.4 Functiescheiding

Functiescheiding betreft het scheiden van taken die een risico vormen voor misbruik of onbedoelde / onbevoegde beschikking over informatie en bedrijfsmiddelen. Hierbij is het zaak conflicterende taken en verantwoordelijkheden te scheiden om de kans op onbevoegd of onbedoeld wijzigen van informatie of misbruik van bedrijfsmiddelen te verminderen.
Met behulp van functiescheiding worden daartoe de taken binnen het Erasmus College zo verdeeld dat er tegengestelde belangen ontstaan. Door deze tegengestelde belangen wordt getracht misbruik van een functie te voorkomen. Het is in dezen een controle technische interne beheersmaatregel die in het financiële domein zeer gebruikelijk is, echter ook vanuit informatiebeveiliging en privacy waarborging van groot belang is. Vanuit informatiebeveiliging en privacy waarborging is het bijvoorbeeld van belang om de verantwoordelijke voor de implementatie van een (technische) beveiligingsmaatregel functioneel te scheiden van een controlerende of monitorende functie. Voor die gevallen waarin er onvoldoende medewerkers beschikbaar zijn om de functiescheiding strikt door te voeren worden mitigerende maatregelen toegepast om eventuele conflicten af te dekken.

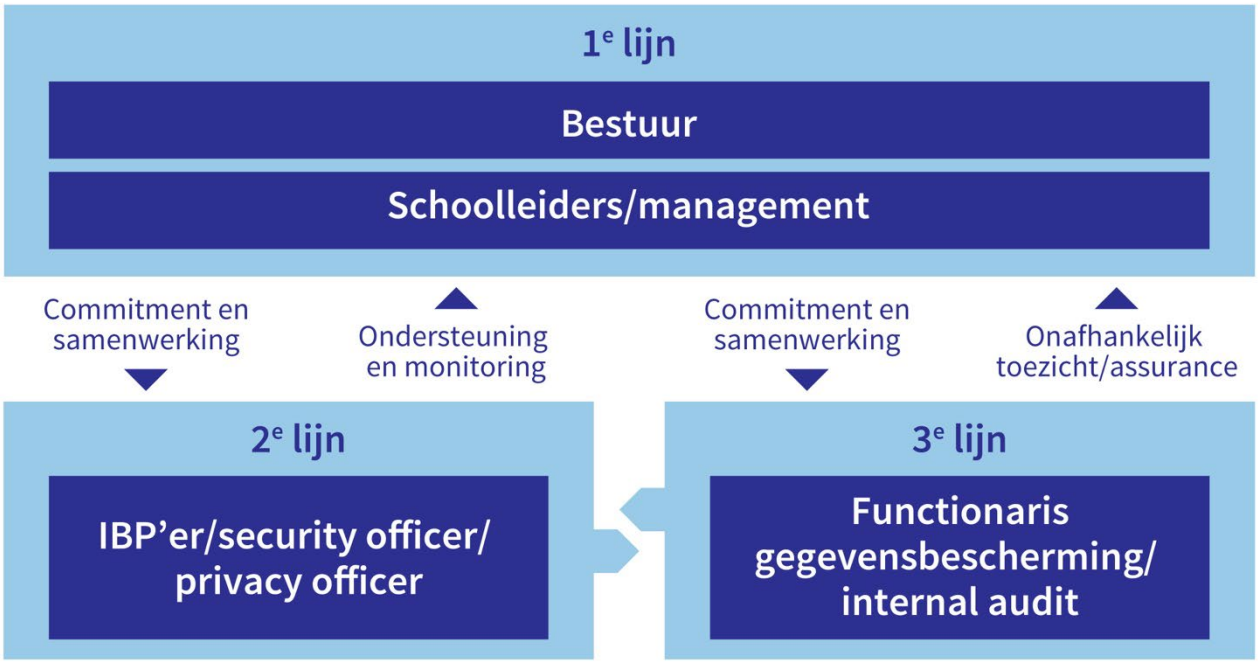
3.3.5 Ketenbeheer en leverancier (risico)management

Het Erasmus College besteedt een deel van de IT uit aan leveranciers, maar blijft eindverantwoordelijk voor beveiliging van informatie en persoonsgegevens binnen de keten die zij zelf opzet en creëert door keuzes te maken voor uitbesteding van bepaalde activiteiten. Om ervoor te zorgen dat ook leveranciers

zich houden aan de technische en organisatorische maatregelen die volgen uit de beveiligingsbaseline, zijn bepaalde stappen toegevoegd aan het leveranciersmanagementproces.

- Er is een lijst met maatregelen opgesteld op basis van de beveiligingsbaseline van het Erasmus College .
- Er is een leveranciersmanagementproces waar de volgende stappen onderdeel van zijn:
    - Voor de aanschaf van een nieuw systeem wordt een BIV-classificatie uitgevoerd.
    - Op basis van deze BIV-classificatie en de lijst met maatregelen worden aanbestedingseisen opgesteld.
    - Er wordt een periodieke controle gedaan op het voldoen aan de aanbestedingseisen en het nakomen van SLA afspraken door de leverancier.

3.4 Three Lines model



Informatiebeveiliging en privacy bij het Erasmus College is ingericht volgens het Three Lines model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van de organisatie.

3.4.1 Eerste lijn: eindverantwoordelijkheid bij het bestuur

Het 3L-model heeft als uitgangspunt dat de eerste lijn verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het treffen van de juiste maatregelen om de risico's te verkleinen. De eerste lijn bestaat uit de directeur bestuurder, de directeuren, teamleiders, en de hoofden van diensten (financiën, personeel, leerlingadministratie, ICT-systeembeheer) van het Erasmus College .
De directeur-bestuurder is binnen de eerste lijn eindverantwoordelijk voor informatiebeveiliging en privacy, maar kan bepaalde verantwoordelijkheden beleggen bij andere functies binnen de organisatie.

Bij de beschrijving van de beleidsthema's in hoofdstuk 4 en 6 wordt per thema beschreven wie er verantwoordelijk is.

3.4.2 Tweede lijn: adviseren en ondersteunen

Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. De tweede lijn bestaat uit security officers (systeembeheer, veldwerk), privacy officer (hoofd financiën), IBP-adviseurs en juridische adviseurs (BLC-advocaten).

3.4.3 Derde lijn: onafhankelijke controle

De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, opereert los van de andere organisatieonderdelen en suggereert waar nodig verbeteringen. De functionaris gegevensbescherming (FG, privaty) en de interne auditor (heeft het Erasmus College nog niet) vallen binnen de derde lijn. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een reglement dat door het bestuur wordt vastgesteld.

3.4.4 Rapportage

De Raad van Toezicht en de directeur-bestuurder ontvangen van deze drie lijnen rapportages over het uitgevoerde maatregelen ten behoeve van informatiebeveiliging, privacy waarborging en risicomanagement en besluit over geëscaleerde risico-acceptatie. De directeur-bestuurder zorgt tevens voor het vaststellen van de juiste mandaten voor acceptatie van risico's en van vaststelling van de risicotolerantie- en -accepteerbaarheidslimieten. Ook besluit de directeur-bestuurder over geconstateerde bevindingen en de afhandeling daarvan.

De CISO (chief information officer) rapporteert periodiek minimaal aan het management en de directeur-bestuurder, over de status van de informatiebeveiliging van de organisatie, inclusief genomen maatregelen, risico's en strategieën, als ook de effectiviteit van het geheel hiervan. Deze functie is vooralsnog belegd bi de directeur-bestuurder van het Erasmus College.

De Functionaris gegevensbescherming rapporteert over de naleving van de AVG, waarbij de Functionaris gegevensbescherming onafhankelijk toezicht houdt en gevraagd en ongevraagd advies geeft zoals beschreven in artikel 39 van de AVG. De Functionaris gegevensbescherming dient periodiek intern te rapporteren aan minimaal het management en directeur-bestuurder van het Erasmus College. Jaarlijks dient de Functionaris Gegevensbescherming een jaarverslag op te stellen met bevindingen en aanbevelingen. Ook kan de Functionaris gegevensbescherming extern rapporteren zoals bijvoorbeeld aan de accountant, de Raad van Toezicht, het ministerie van OCW en de Nederlandse Autoriteit Persoonsgegevens.

3.5 Architectuur

Werken vanuit een vastgestelde architectuur geeft duidelijkheid over waar welke informatie verwerkt wordt. Inzicht in het applicatielandschap en procesmatig werken zijn noodzakelijk om informatieveiligheid en privacy te kunnen borgen in de hele organisatie.

Het Erasmus College zal voor de onderwijsprocessen als ook voor de bedrijfsvoeringprocessen binnen de gehele organisatie de FORA (Funderend Onderwijs Referentie Architectuur) als enterprise information architecture model (EIAM) hanteren. De FORA is een referentiearchitectuur die onderwijsinstellingen in het funderend onderwijs inzicht geeft in processen en activiteiten en aan welke spelregels deze moeten voldoen.

Architectuur is een manier om de structuur en werking van iets uit te drukken. Het woord ‘referentie’ betekent hier dat de FORA niet de architectuur van één specifieke onderwijsorganisatie beschrijft, maar een architectuurmodel dat de structuur en werking van onderwijsorganisaties in het algemeen weergeeft.

De processen zoals opgenomen in de FORA en zijn leidend binnen het Erasmus College .

4 Beleidsthema's informatiebeveiliging

In hoofdstuk 4 zijn de beleidsthema's op het gebied van informatiebeveiliging opgenomen.

4.1 Verdeling verantwoordelijkheden ICT & Netwerkbeheer

Binnen het Erasmus College worden de verantwoordelijkheden voor ICT- en netwerkbeheer gescheiden uitgevoerd. De interne systeembeheerder is verantwoordelijk voor het opstellen, implementeren en beheren van processen, maatregelen en configuraties die betrekking hebben op alle ICT-middelen en -diensten die door het Erasmus College zelf worden beheerd, waaronder cloudomgevingen, servers, werkplekapparatuur, applicaties en overige hardware.

De netwerkcomponenten (zoals switches, firewalls, access points en de routing- en netwerkarchitectuur) worden beheerd door externe dienstverlener Veldwerk. Voor deze componenten draagt Veldwerk verantwoordelijkheid voor het technisch beheer, de beveiligingsconfiguraties en het uitvoeren van netwerk gerelateerde maatregelen. Waar beleidsthema's in dit hoofdstuk betrekking hebben op zowel ICT-systemen als netwerkcomponenten, zijn zowel de interne systeembeheerder als Veldwerk gezamenlijk verantwoordelijk, ieder binnen het eigen domein.

4.2 Risicomanagement

Het Erasmus College hanteert een losstaand risicomanagementbeleid. Zie <naam beleid, nog opstellen>.

4.3 Kennis en afhankelijkheid medewerkers

Het Erasmus College is voor de beveiliging van informatie en de continuïteit van het onderwijs afhankelijk van de kennis en beschikbaarheid van medewerkers. Het Erasmus College wil voorkomen dat er onvoldoende kennis aanwezig is bij medewerkers of dat kritieke kennis en vaardigheden onvoldoende aanwezig zijn binnen de organisatie. Taken van sleutelfiguren moeten daarom altijd overgenomen kunnen worden door andere medewerkers. Hiervoor hanteert het Erasmus College de volgende maatregelen:

- Een back-up plan voor kritieke medewerkers.
- Voldoende training en certificering.
- Een indienst-/uitdiensttredingproces waarin rekening gehouden wordt met aansluiting op het proces voor het beheren van rechten en rollen, de overdracht van kennis en documentatie en screening van medewerkers.

Verantwoordelijkheden:

- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van het back-up plan voor kritieke medewerkers.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van het back-up plan voor kritieke medewerkers.
- De directeur met personeel in haar portefeuille van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van het in dienst/uitdiensttreding proces.

4.4 Bedrijfscontinuïteit

Het Erasmus College zorgt ervoor dat mogelijke verstoringen van het onderwijs zo snel mogelijk verholpen worden en dat de impact van verstoringen beperkt blijft. Door processen te analyseren worden de meest kritieke applicaties en medewerkers geïdentificeerd, en wordt bepaald welke terugvalopties nu aanwezig zijn. Hierna kunnen maatregelen geïmplementeerd worden om verstoringen zo veel mogelijk te voorkomen of de impact te beperken. Er is een crisismanagementteam aanwezig om snel en adequaat op incidenten te reageren.

Het Erasmus College hanteert de volgende maatregelen voor bedrijfscontinuïteit:

- Business impact analyses (BIA) op basis van de processen van de organisatie. De processen worden op basis van een risicogestuurde aanpak geanalyseerd, waarbij eerst de meest kritieke processen behandeld worden. Nieuwe risico's die tijdens deze BIA's geïdentificeerd zijn, worden opgenomen in het risicoregister. Zie hiervoor het risicomanagementbeleid.
- Een bedrijfscontinuïteitsplan (BCP). Een crisismanagementaanpak waaronder periodieke crisisoefeningen maken onderdeel uit van het BCP. Taken en verantwoordelijkheden zijn duidelijk toegewezen in het BCP. Het BCP wordt na een jaarlijkse oefening steeds geactualiseerd.

Verantwoordelijkheden:

- De directeur-bestuurder is verantwoordelijk voor het formeel goedkeuren van het bedrijfscontinuïteitsplan.
- De systeembeheerder en de directeur-bestuurder is verantwoordelijk voor het opstellen en het beheren van het bedrijfscontinuïteitsplan.

Het Erasmus College hanteert een losstaand bedrijfscontinuïteitsplan. Zie <bedrijfscontinuïteitsplan Erasmus College naam protocol, nog opstellen>.

4.5 Back-up en herstel

Om de impact van verstoringen of dataverlies te beperken zorgt het Erasmus College voor back-ups van systemen en data. Op basis van de BIV-classificatie van systemen worden de back-upvereisten voor de systemen en de data binnen deze systemen vastgesteld. Back-ups worden regelmatig getest om te verifiëren of gegevens kunnen worden hersteld binnen de vastgestelde periode. De volgende uitgangspunten worden hierbij gehanteerd:

- De proceseigenaar is degene die beslist over de continuïteitsvereisten van een dataverwerking of een systeem. Het initiatief voor deze afweging komt van de systeemeigenaar.
- We stellen dezelfde back-upeisen aan diensten van externe leveranciers als aan systemen die we zelf beheren.
- Bij voorkeur maken we bij externe leveranciers gebruik van de back-upfaciliteit die ze zelf bij hun dienst aanbieden. Ontbreekt die of voldoet die niet, dan maken we zelf back-ups van de informatie die we verwerken in de dienst van deze leverancier.
- We evalueren jaarlijks de manier waarop we zelf back-ups maken.

Verantwoordelijkheden:

- Het Erasmus College stelt een procesbeschrijving op voor back-up en herstel.
- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van de back-up en herstel procesbeschrijving.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van de back-up en herstel procesbeschrijving.
- De systeemeigenaar is verantwoordelijk voor het toepassen van het back-up en herstelproces.

4.6 Fysieke beveiliging

Het Erasmus College hanteert een losstaand fysiek beveiligingsbeleid. Zie <naam beleid, nog opstellen>.

4.7 Systeem- en data-eigenaarschap en configuratiebeheer

Om IT-processen te beheren is inzicht nodig in welke systemen worden gebruikt binnen de organisatie. Veel van de IBP-thema's in dit beleid zijn afhankelijk van dit inzicht. De rol van systeemeigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die specifiek voor een systeem gelden. De rol van proceseigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die te maken hebben met een specifiek proces. Het Erasmus College maakt de keuze om eigenaarschap van data niet vast te leggen, maar zich te beperken tot het beleggen van eigenaarschap van systemen waar deze data in is vastgelegd. Voor het vastleggen van processen en het eigenaarschap van systemen en processen treft het Erasmus College de volgende maatregelen:

- Het Erasmus College heeft een configuratiemanagementdatabase (CMDB) waarin alle systemen, het eigenaarschap en andere benodigde eigenschappen bijgehouden worden.
- Systeemeigenaarschap wordt bepaald vóór implementatie van nieuwe systemen. De eigenaren van systemen worden vastgelegd in het CMDB.
- Proceseigenaarschap wordt bepaald en vastgelegd binnen het verwerkingsregister.

Verantwoordelijkheden:

- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van de CMDB.

- De systeemeigenaar van elk systeem is verantwoordelijk voor het vastleggen van de juiste eigenschappen in de CMDB.

4.8 Classificatie van systemen en data

Om risico gestuurd beslissingen te kunnen nemen is belangrijk om per systeem het benodigde niveau van ***beschikbaarheid, integriteit en vertrouwelijkheid*** (BIV) te bepalen. De classificatie is beperkt tot systeemniveau. Het Erasmus College kiest ervoor om de classificatie niet per individueel dataobject toe te passen. Het Erasmus College heeft voor elk systeem dat opgenomen is in de CMDB een BIV-classificatie uitgevoerd. Deze BIV-classificatie wordt gebruikt om te bepalen welke maatregelen er voor het betreffende systeem geïmplementeerd moeten worden. Voor het goed toepassen van de BIV-classificatie treft het Erasmus College de volgende maatregelen:

- Er wordt eigenaarschap aangebracht voor alle processen, systemen en data die daarbinnen wordt verwerkt. Deze eigenaren zijn verantwoordelijk voor de BIV-classificatie hiervan.
- De BIV-classificatie wordt uitgevoerd vóór de aanschaf van een nieuw systeem, het in uitvoering brengen van nieuwe (voorgenomen) processen en verwerkingen van persoonsgegevens.
- De BIV-classificatie wordt in detail ook vooraf vastgesteld voor de gegevens welke binnen een systeem of proces gaan worden verwerkt.
- De BIV-classificatie wordt vastgelegd in de CMDB.

Verantwoordelijkheden:

- De systeemeigenaar van elk systeem is verantwoordelijk voor het uitvoeren van de BIV-classificatie en het vastleggen hiervan in de CMDB.

4.9 Beveiligingsbaseline

Een beveiligingsbaseline voor IT-systemen is vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. Het Erasmus College maakt gebruik van het certificeringsschema ROSA als beveiligingsbaseline voor IT-systemen in eigen beheer. De beveiligingsbaseline is formeel vastgelegd, wordt periodiek geactualiseerd en wordt goedgekeurd door het schoolbestuur. De toepassing van de beveiligingsbaseline voor IT-middelen wordt periodiek beoordeeld op naleving. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

Verantwoordelijkheden:

- De systeembeheerder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van de beveiligingsbaseline.
- De systeemeigenaar van elk systeem is verantwoordelijk voor het voldoen aan de beveiligingsbaseline en het vastleggen van afwijkingen op de baseline.

4.10 Bewustwording en afhankelijkheid medewerkers

Het Erasmus College is voor de beveiliging van informatie, privacy waarborging en de continuïteit van het onderwijs afhankelijk van de kennis en beschikbaarheid van medewerkers. Het Erasmus College wil voorkomen dat er onvoldoende kennis aanwezig is bij medewerkers of dat kritieke kennis en vaardigheden onvoldoende aanwezig zijn binnen de organisatie. Taken van sleutelfunctionarissen moeten daarom altijd overgenomen kunnen worden door andere medewerkers. Hiervoor hanteert het Erasmus College minimaal de volgende maatregelen:

- Een in dienst-/uitdiensttredingproces waarin rekening gehouden wordt met aansluiting op het proces voor het beheren van rechten en rollen, de overdracht van kennis en documentatie en screening van medewerkers;
- Het Erasmus College identificeert de vereiste vaardigheden (kennis, inzicht in de materie, competenties en bewustzijn) voor alle in- en externe medewerkers die taken uitvoeren die de beschikbaarheid, integriteit en/of vertrouwelijkheid beïnvloeden;
- Voor Informatiebeveiliging en Privacy verantwoordelijk taakhouders en functionarissen zijn functieprofielen in lijn met en afgestemd op bovengenoemde geïdentificeerde vereiste vaardigheden;
- Dit principe wordt ook toepast voor personeel van leveranciers welke (kritieke) diensten en producten (ICT) leveren aan het Erasmus College, vaak ook verwerkers in de zin dan de AVG.
- Een back-upplan voor kritieke medewerkers;
- Voldoende opleiding, training en certificering organisatie breed, voor alle lagen in de organisatie, volgens een meerjarig continue bewustwordingsprogramma. Dit moet leiden tot inzicht en daarmee bewustwording bij het handelen van alle medewerkers (personeel in loondienst en personeel niet in loondienst) en externen.

De focus ligt hierbij op zowel digitale vaardigheden en geletterdheid als ook informatiebeveiliging en privacy vaardigheden, kennis en inzicht. Een belangrijk principe hierbij is het doorvoeren en handhaven van ‘Clear Desk’ en ‘Clear Screen’ werkwijzen.

We waarborgen dat deze medewerkers bekwaam zijn. Indien nodig ondernemen we stappen om de benodigde vaardigheden te ontwikkelen en evalueren we de doeltreffendheid van deze inspanningen. Structureel worden voor de activiteiten budgetten opgenomen in de jaarlijkse begroting.

Medewerkers die werkzaamheden verrichten namens, voor en/of binnen het Erasmus College dienen zich bewust te zijn van het Informatiebeveiliging en Privacy beleid, hun rol bij het bevorderen van de doeltreffendheid van de genomen technische en organisatorische maatregelen en de consequenties van het niet naleven hiervan.

Verantwoordelijkheden:

- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van het bewustwordingsprogramma.

- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van het bewustwordingsprogramma

4.11 Incident- en problemmanagement

Incidentmanagement is het proces voor het melden van incidenten binnen de organisatie. Sommige incidenten kunnen een datalek tot gevolg hebben. Incidenten binnen de organisatie zijn nooit helemaal uit te sluiten. Een helder beschreven incidentmanagementproces is aanwezig om incidenten op tijd te herkennen en ze adequaat af te handelen. De manier waarop dat gebeurt is vastgelegd in een procesbeschrijving waarbij de volgende onderwerpen minimaal terugkomen:

- **Een centraal punt** voor het melden van incidenten**.**
- **Incidentenregister:** Binnen dit incidentenregister wordt er duidelijk onderscheid gemaakt tussen datalekken en andere type incidenten.
- **De classificatie van incidenten:** Bij elk incident moet worden vastgesteld om wat voor type incident het gaat (beveiliging, privacy, etc.)
- **De afhandeling van het incident**: Het is duidelijk wie bij welk type incident betrokken moeten worden en wie verantwoordelijk is voor het afhandelen van de incidenten.
- **Problemmanagement:** Indien incidenten regelmatig terugkomen worden deze aangemerkt als een *known error*. De procesbeschrijving beschrijft de vervolgstappen voor een terugkerend incident.
- **Monitoren en rapporteren:** Afhandeling van incidenten en problemen worden gemonitord. Hierover wordt periodiek gerapporteerd.

Verantwoordelijkheden:

- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van de incidentmanagement procesbeschrijving.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van de incidentmanagementprocesbeschrijving.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het inrichten en beheren van het incidentenregister.

4.12 Risicomanagement leveranciers

Het Erasmus College besteedt een deel van de IT uit aan leveranciers, maar blijft eindverantwoordelijk voor beveiliging van informatie en persoonsgegevens. Om ervoor te zorgen dat ook leveranciers zich houden aan de technische maatregelen die volgen uit de beveiligingsbaseline zijn bepaalde stappen toegevoegd aan het leveranciersmanagementproces.

- Er is een lijst met maatregelen opgesteld op basis van de beveiligingsbaseline van het Erasmus College
- Er is een leveranciersmanagementproces waar de volgende stappen onderdeel van zijn:
    - Voor de aanschaf van een nieuw systeem wordt een BIV-classificatie uitgevoerd.

- Op basis van deze BIV-classificatie en de lijst met maatregelen worden aanbestedingseisen opgesteld.
- Er wordt een periodieke controle gedaan op het voldoen aan de aanbestedingseisen.

Verantwoordelijkheden:

- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van de leveranciersmanagementprocesbeschrijving.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van de leveranciersmanagementprocesbeschrijving.
- De systeemeigenaar is verantwoordelijk voor de periodieke controle op het voldoen aan de aanbestedingseisen.

4.13 Werkplekken en mobiele apparaten

Persoonsgegevens en andere informatie uit systemen die binnen onze organisatie worden gebruikt, worden ontsloten via verschillende apparaten zoals laptops, tablets, smartphones en desktop-pc's. Deze apparaten brengen risico's met zich mee op het gebied van beveiliging, dataverlies en compliance. Daarom treft het Erasmus College de volgende maatregelen:

- Het Erasmus College hanteert een richtlijn voor het gebruik van werkplekken en mobiele apparaten.

Verantwoordelijkheden:

- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.

4.14 Identiteits- en toegangsbeheer

Het Erasmus College heeft een apart IAM-beleid. Zie hiervoor <naam beleid>.

4.15 Vulnerabilitymanagement en pentesting

Vulnerabilitymanagement en pentesting vormen een essentieel onderdeel voor het verminderen van risico's, het voorkomen van ongeautoriseerde toegang tot IT-systemen en het beschermen van gegevens tegen mogelijke dreigingen.

De wijze waarop, door welke externe partij en met welke frequentie aan dit onderdeel vorm wordt gegeven door het Erasmus College, is verder uitgewerkt en opgenomen in het risicomanagementbeleid. Zie <naam beleid>.

4.16 Patchmanagement

Met patchmanagement verhelp je kwetsbaarheden in systemen, applicaties en hardware. Het doel is om de beveiliging, stabiliteit en prestaties van IT-omgevingen te waarborgen door het tijdig testen en implementeren van patches. Hiervoor neemt het Erasmus College de volgende maatregel:

- Het Erasmus College heeft een proces voor het inrichten van patchmanagement.

Verantwoordelijkheden:

- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving patchmanagement.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving patchmanagement.
- De systeemeigenaar is verantwoordelijk voor tijdig testen en implementeren van patches.

4.17 Logging

Loggegevens bieden inzicht in de activiteiten van systemen en spelen een sleutelrol bij het detecteren, onderzoeken en voorkomen van beveiligingsincidenten. Om loggegevens vast te leggen neemt het Erasmus College de volgende maatregel:

- Het Erasmus College heeft een procesbeschrijving voor het vastleggen van loggegevens binnen systemen.

Verantwoordelijkheden:

- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving voor logging.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor logging.

4.18 Digitaal sleutelbeheer

Het Erasmus College gebruikt encryptie voor de volgende doeleinden:

- Bescherming van vertrouwelijke gegevens: Door het toepassen van sterke versleutelingstechnieken bij opslag, verzending en verwerking van gegevens.
- Verificatie van identiteit: Gebruik van cryptografische methoden zoals digitale handtekeningen en certificaten om betrouwbare communicatie te waarborgen.
- Waarborgen van gegevensintegriteit: Detecteren van wijzigingen in gegevens.

Om encryptie toe te passen treft het Erasmus College de volgende maatregel:

- Het Erasmus College hanteert een procesbeschrijving voor het beheer van digitale sleutels.

Verantwoordelijkheden:

- De directeur-bestuurder van het Erasmus College is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving digitaal sleutelbeheer.
- De systeembeheerder van het Erasmus College is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor digitaal sleutelbeheer.

5 Uitgangspunten Privacy en Gegevensbescherming (AVG)

Het algemene uitgangspunt in dit IBP-beleid is dat persoonsgegevens in overeenstemming met de AVG en gerelateerde wet- en regelgeving op zorgvuldige wijze worden verwerkt. Om aan dit uitgangspunt te voldoen verwerkt het Erasmus College persoonsgegevens in overeenstemming met de privacy vuistregels die in verderop in dit hoofdstuk worden uiteengezet. Het Erasmus College treft verdiepende maatregelen om de beleidsthema's in dit IBP-beleid in te vullen.

5.1 Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect over iemand gaan en dus naar een persoon te herleiden zijn, zoals een naam of e-mailadres. Naast gewone persoonsgegevens - denk aan contactgegevens en onderwijsnummers - onderscheidt de AVG bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Daarnaast bestaat een categorie 'gevoelige' persoonsgegevens die niet expliciet in de AVG is benoemd. Dit zijn persoonsgegevens die vanwege hun aard privacygevoelig zijn en daarom extra bescherming verdienen.

- **Bijzondere persoonsgegevens** zijn gegevens die te maken hebben met bijvoorbeeld ras of etnische afkomst, gezondheid, religie of seksueel gedrag. De verwerking van deze gegevens is verboden, tenzij een wettelijke uitzondering bestaat zoals toestemming van de betrokkene.
- **Strafrechtelijke gegevens** zijn gegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. De verwerking van deze gegevens is ook verboden, tenzij hiervoor een wettelijke uitzondering geldt.
- **Gevoelige persoonsgegevens** zijn gegevens die een groter privacy risico vormen dan gewone persoonsgegevens. Denk aan financiële gegevens, burgerservicenummers (BSN), beoordelingen of gegevens van kwetsbare leerlingen.

NB: Nummers ter identificatie van een persoon, zoals het BSN, mogen alleen worden gebruikt voor specifieke doeleinden die in de wet zijn vastgelegd. Een onderwijsnummer (persoonsgebonden nummer) is gelijk aan het BSN.

5.2 Privacy principes

Bij het verwerken van persoonsgegevens houdt het Erasmus College rekening met onderstaande privacy principes en uitgangspunten. Door deze te volgen zorgen we ervoor dat we kunnen voldoen aan de AVG.

We verwerken persoonsgegevens rechtmatig en transparant
Het Erasmus College verzamelt en gebruikt persoonsgegevens op een eerlijke en transparante manier. Persoonsgegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat in de AVG. We leggen altijd duidelijk uit waarom we bepaalde gegevens nodig hebben, wat we ermee doen en hoe lang we deze gegevens bewaren. Daarom informeren we ouders en leerlingen tijdig over het gebruik van hun persoonsgegevens, via een transparante privacyverklaring. Dit gebeurt bijvoorbeeld op het moment van inschrijving van een leerling.

We verwerken persoonsgegevens voor specifieke doeleinden
Het Erasmus College verwerkt persoonsgegevens alleen wanneer vooraf de specifieke doeleinden voor de verwerking zijn bepaald. Deze doeleinden worden vastgelegd. Persoonsgegevens worden niet voor andere, niet-verenigbare, doelen verwerkt. We zullen dus niet persoonsgegevens verzamelen omdat die wellicht ooit van pas gaan komen. We doen dit alleen met vooraf bepaalde, duidelijke en gerechtvaardigde doelen, zoals het plannen van onderwijs en communiceren met leerlingen en ouders over de voortgang en schoolactiviteiten.

We verwerken alleen noodzakelijke persoonsgegevens
Het Erasmus College verzamelt alleen persoonsgegevens die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt. We vragen dus niet om meer gegevens dan we daadwerkelijk nodig hebben en hanteren hierbij het uitgangspunt 'zo min mogelijk'. We onderzoeken altijd of we met minder gegevens of enkel met anonieme gegevens kunnen werken. Zo vragen we bij de inschrijving van een leerling alleen om de gegevens die relevant zijn voor het kunnen bieden van onderwijs en bewaren we geen overbodige gegevens die niet nodig zijn voor onze schoolactiviteiten.

We zorgen dat persoonsgegevens juist en actueel zijn
Het Erasmus College treft maatregelen om ervoor te zorgen dat persoonsgegevens correct en actueel zijn. Onjuiste of achterhaalde gegevens worden geactualiseerd of verwijderd. Leerlingen en ouders kunnen op een laagdrempelige manier doorgeven dat persoonsgegevens incorrect zijn en/of gewijzigd moeten worden. Onze processen en systemen worden zo ingericht dat de juistheid van gegevens zoveel mogelijk wordt afgedwongen en gecontroleerd.

We bewaren persoonsgegevens niet langer dan nodig
Het Erasmus College bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Zodra gegevens niet meer nodig zijn, worden ze verwijderd of geanonimiseerd. We houden ons hierbij aan vooraf vastgestelde bewaartermijnen. Zo wordt het leerlingendossier (inclusief rapporten en schoolprestaties) na uitschrijving van een leerling niet langer bewaard dan nodig is voor administratieve en onderwijsdoeleinden en dus zo spoedig mogelijk verwijderd, in ieder geval binnen 2 jaar na uitschrijving.

We zorgen voor een passende bescherming van persoonsgegevens
We kunnen de privacy van leerlingen, ouders en medewerkers alleen goed beschermen als we op een veilige manier met hun persoonsgegevens omgaan. We zijn daarom verantwoordelijk voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. Die maatregelen moeten ervoor zorgen dat de persoonsgegevens op een passende wijze worden beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking. Dit doen we bijvoorbeeld door het gebruik van veilige systemen voor de opslag van leerlinggegevens en het opleiden van personeel in het veilig omgaan met gevoelige gegevens.

We kunnen aantonen dat we voldoen aan de AVG
We zijn verantwoordelijk voor het naleven van bovengenoemde vuistregels en kunnen daarmee aantonen dat we voldoen aan de belangrijkste uitgangspunten van de AVG. Dit doen we bijvoorbeeld

door het bijhouden van een verwerkingsregister en het uitvoeren van *Data Protection Impact Assesments* (DPIA's) voor gegevensverwerkingen met een hoog privacy risico.

We kunnen ons ethisch verantwoorden

Bij het beoordelen van verwerkingen van persoonsgegevens houdt het Erasmus College niet alleen rekening met de vereisten uit de AVG ('*mogen we dit?*'), maar nadrukkelijk ook met ethische aspecten ('*willen we dit*?). Het gaat hierbij dus niet om de vraag of we iets 'mogen' of 'kunnen', maar juist om de vraag of we iets zouden moeten 'willen' als school. Ethische aspecten spelen in het bijzonder een rol bij verwerkingen die privacy risico's kunnen opleveren, bijvoorbeeld bij het gebruik van meekijksoftware of schermcontroles. Dit moet ook worden bezien vanuit een ethisch afwegingskader. We stellen ons dan ook eerst de vraag of we het kunnen uitleggen aan leerlingen en ouders.

6 Beleidsthema's privacy

6.1 Verwerkingsregister

Het Erasmus College heeft maatregelen getroffen om aantoonbaar te voldoen aan de eisen uit de AVG. Dit houdt onder meer in dat het Erasmus College kan aantonen dat de verwerking van persoonsgegevens voldoet aan de uitgangspunten uit de AVG. Het Erasmus College geeft onder meer invulling aan haar verantwoordingsplicht door een overzicht bij te houden met informatie over de persoonsgegevens die zij verwerkt. Dit heet het verwerkingsregister. Dit register bevat bijvoorbeeld informatie over de leerlingenadministratie of het HR-systeem. Het bijhouden van het verwerkingsregister zorgt voor een goed overzicht van welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt. Het register stelt het Erasmus College in staat te voldoen aan haar verantwoordingsplicht.

Het verwerkingsregister bevat van afzonderlijke verwerkingsactiviteiten informatie over onder meer de doeleinden voor de verwerking, de toepasselijke grondslag onder de AVG, een beschrijving van de betrokkenen, een beschrijving van de persoonsgegevens, de toepasselijke bewaartermijnen en de ontvangers waarmee persoonsgegevens worden gedeeld.

6.1.1 Legitiem doel en doelbinding

Persoonsgegevens worden alleen verwerkt als een specifiek, vooraf bepaald doel is vastgesteld door het Erasmus College. Dit doel moet duidelijk en in begrijpelijke taal aan de betrokkenen worden uitgelegd. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt.

Het Erasmus College verwerkt persoonsgegevens om haar verplichtingen als onderwijsinstelling na te kunnen komen. Het schoolbestuur verwerkt persoonsgegevens in de eerste plaats om onderwijs te kunnen bieden aan haar leerlingen en om activiteiten die hieraan ondersteunend zijn te kunnen uitvoeren. Hierbij valt te denken aan verwerkingen in het kader van het aanmeldproces, om te communiceren met leerlingen en ouders/verzorgers, het bijhouden van de leerlingenadministratie, het maken van roosters en om de voortgang bij te houden. Ook verwerkt het schoolbestuur persoonsgegevens van haar medewerkers in haar rol als werkgever. Het Erasmus College verwerkt bij deze werkzaamheden verschillende (categorieën) persoonsgegevens, waaronder contactgegevens, naam, geboortedatum en gegevens betreffende de aard en het verloop van het onderwijs. Het Erasmus College verwerkt deze persoonsgegevens op basis van grondslagen uit de AVG, bijvoorbeeld omdat sprake is van een wettelijke taak of verplichting, een gerechtvaardigd belang of op basis van toestemming.

Als gegevens toch voor een ander doel nodig zijn, dan mag dit alleen als dat doel verenigbaar is met het oorspronkelijke doel. Om te bepalen of dit het geval is, moet onder andere worden gekeken naar:

- De relatie tussen het nieuwe en het oorspronkelijke doel.
- De context waarin de gegevens zijn verzameld en de redelijke verwachtingen van de betrokkenen.

- Het soort persoonsgegevens; gevoelige gegevens verdienen extra bescherming.
- De mogelijke gevolgen voor betrokkenen.
- Bescherming van de gegevens, zoals versleuteling of pseudonimiseren.

Voor elke nieuwe verwerking moet het Erasmus College de rechtmatigheid, zorgvuldigheid en noodzaak opnieuw beoordelen. De specifieke doeleinden worden voorafgaand aan de verwerking bepaald en vermeld in de privacyverklaring om betrokken te informeren. Ook worden de doeleinden opgenomen in het verwerkingsregister. Voordat gegevens voor een ander doel worden gebruikt, vindt altijd overleg plaats met de privacy officer en ook altijd met de functionaris gegevensbescherming.

6.1.2 Grondslag

Het Erasmus College moet voor iedere verwerking van persoonsgegevens een geldige reden hebben. De AVG noemt dit een grondslag. Het Erasmus College verwerkt persoonsgegevens alleen op basis van de in de AVG genoemde grondslagen:

- de betrokkene heeft **toestemming** verleend, bijvoorbeeld voor het maken en delen van foto's of video's.
- de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, bijvoorbeeld het verwerken van salaris om de arbeidsovereenkomst met werknemers na te komen.
- de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting,** bijvoorbeeld het delen van salarisinformatie met de Belastingdienst voor de uitvoering van de belastingwetgeving.
- de verwerking is noodzakelijk om **de vitale belangen** van de betrokkene te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarbij het noodzakelijk is dat bepaalde gegevens van een leerling acuut aan hulpverleners moeten worden doorgeven.
- de verwerking is noodzakelijk om uitvoering te geven aan een **taak van algemeen belang**, hierbij gaat het om wettelijk vastgestelde taken en bevoegdheden. Zo heeft het Erasmus College de wettelijke taak om onderwijs te bieden.
- de verwerking is noodzakelijk voor de behartiging van een **gerechtvaardigd belang** van het Erasmus College of van een derde. Denk hierbij aan het verwerken van medewerkersgegevens voor het opstellen van managementrapportages ten behoeve van beleidsontwikkeling of het gebruik van bewakingscamera's op het schoolplein.

De toepasselijke grondslag wordt vooraf vastgesteld, bijvoorbeeld middels een DPIA, en benoemd in de privacyverklaring om betrokken te informeren. Ook wordt de toepasselijke grondslag opgenomen in het verwerkingsregister.

6.2 Informatieplicht

Het Erasmus College verwerkt persoonsgegevens op een behoorlijke en transparantie manier. Dit is in begrijpelijke taal inzichtelijk voor de betrokkenen. Het Erasmus College informeert leerlingen en ouders voorafgaand aan de gegevensverwerking op transparante wijze via een duidelijke privacyverklaring. Deze privacyverklaring wordt gepubliceerd op de website. Daarnaast informeert de school

medewerkers en sollicitanten ook via een aparte privacyverklaring. Hiermee zorgt het Erasmus College ervoor dat betrokkenen weten welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Ook worden zij middels de privacy verklaringen geïnformeerd over de rechten die ze hebben.

6.3 Toestemming

Bij het gebruik van toestemming als grondslag gelden een aantal voorwaarden:

- Toestemming moet op een begrijpelijke en toegankelijke manier worden gevraagd, in duidelijke taal en niet verborgen in algemene voorwaarden of lange teksten.
- Toestemming moet vrijwillig worden gegeven en moet ook weer gemakkelijk ingetrokken kunnen worden.
- Het Erasmus College moet kunnen aantonen dat toestemming is verkregen, bijvoorbeeld door logs of ondertekende formulieren.
- Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven. Dit geldt ook voor personen onder curatele, bewind of mentorschap. Het Erasmus College verifieert of deze vertegenwoordiger daadwerkelijk toestemming heeft gegeven.

Leerlingen (of hun wettelijke vertegenwoordigers) worden in bepaalde situaties om toestemming gevraagd. Denk aan de situatie dat het Erasmus College foto's of video's van leerlingen maakt en publiceert. Dit mag alleen als de school vooraf toestemming heeft verkregen. Omdat een gezagsrelatie bestaat tussen het Erasmus College en haar leerlingen en medewerkers, moet goed worden beargumenteerd waarom toestemming in specifieke gevallen in vrijheid kan worden gegeven. Het Erasmus College gaat daarom terughoudend om met het gebruik van deze grondslag. Voordat toestemming als grondslag wordt gebruikt, vindt altijd overleg plaats met de privacy officer en ook altijd met de functionaris gegevensbescherming.

6.4 Privacy by design en privacy by default

Privacy by design betekent dat het Erasmus College bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk rekening houdt met privacy risico's en passende waarborgen inbouwt om de privacy van betrokkenen te beschermen. Neemt het Erasmus College bijvoorbeeld een leerlingvolgsysteem in gebruik? Dan moet in een vroeg stadium al worden nagedacht over passende toegangsbeperkingen. Leraren horen alleen inzicht te krijgen in de noodzakelijke gegevens van hun eigen leerlingen. *Privacy by default* betekent dat de standaardinstellingen van een product, dienst of proces op de meest privacy vriendelijke instelling staan behalve als het Erasmus College daar bewust van af wil wijken. Hiermee zorgt het Erasmus College ervoor dat zo vroeg mogelijk rekening wordt gehouden met privacy beginselen en op die manier privacy risico's tijdig worden gemitigeerd.

6.5 Dataminimalisatie

Het Erasmus College verzamelt alleen gegevens die noodzakelijk zijn voor het doel dat voorafgaand aan de verwerking is vastgesteld. De verzamelde gegevens dienen toereikend, ter zake dienend en niet

bovenmatig te zijn. Hiermee voorkomt het Erasmus College dat te veel gegevens worden verwerkt. Bij de aanmelding van een leerling verzamelt het Erasmus College bijvoorbeeld alleen de informatie die nodig is om de leerling op de juiste manier in te schrijven. Denk aan naam, geboortedatum, adres en contactgegevens van ouders/verzorgers. Extra informatie, zoals het beroep van de ouders, is niet relevant voor de inschrijving en hoort daarom niet te worden verzameld. Daarnaast moet de verwerking van persoonsgegevens op de minst ingrijpende wijze plaatsvinden. Als het beoogde doel op een privacy vriendelijkere manier kan worden bereikt, dan kiest het Erasmus College hiervoor. Op deze manier voldoet het Erasmus College eveneens aan de principes van *privacy by design*.

6.6 Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Dit gebeurt in overeenstemming met het bewaar- en vernietigingsbeleid van het Erasmus College. Na het verlopen van de toepasselijke bewaartermijnen zorgt het Erasmus College ervoor dat persoonsgegevens tijdig worden vernietigd (of geanonimiseerd). Hierdoor worden persoonsgegevens beter beschermd tegen onnodige verwerking en datalekken. Zo worden bijvoorbeeld overzichten van schoolprestaties en rapporten uiterlijk tot 2 jaar na uitschrijving van een leerling bewaard. Het schooladvies wordt tot uiterlijk 5 jaar na uitschrijving van een leerling bewaard.

Het Erasmus College heeft een apart Bewaartermijnen- en retentiebeleid. Zie hiervoor <naam beleid>.

6.7 Afhandelen van datalekken

Datalekken moeten direct worden gemeld en geregistreerd in het interne register voor beveiligingsincidenten en datalekken. Het melden van (potentiële) beveiligingsincidenten en datalekken is vastgelegd in het datalek management protocol. Door toepassing van het datalek management protocol wordt telkens bepaald of een datalek moeten worden gemeld aan de Autoriteit Persoonsgegevens. En ook of het datalek moet worden gemeld aan de betrokkenen als het datalek waarschijnlijk een hoog risico voor hen oplevert. De directeur-bestuurder van het Erasmus College neemt hierover telkens een besluit. Dit gebeurt altijd in samenspraak met de Privacy Officer en de Functionaris gegevensbescherming. Deze beiden geven altijd een onderbouwd advies hierover aan de directeur-bestuurder.

Het Erasmus College heeft een apart Incident en datalek management protocol. Zie hiervoor <naam protocol>.

6.8 Data Protection Impact Assessment

Een Data Protection Impact Assesment (hierna DPIA) brengt in kaart hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar de risico's liggen en welke gevolgen dit kan hebben gerelateerd aan een verwerking van persoonsgegevens.

Voor elke nieuwe verwerking van persoonsgegevens, bijvoorbeeld een nieuw proces, technologie of applicatie, controleert het Erasmus College of de privacy beginselen en eisen en voorwaarden uit de AVG worden nageleefd. Dit vindt plaats door een zogenoemde pre-DPIA uit te voeren. Deze korte analyse van de nieuwe voorgenomen verwerking van persoonsgegevens geeft aan of een volledige DPIA noodzakelijk en wettelijk verplicht is. Op basis van de uitkomsten van de DPIA neemt het Erasmus College maatregelen om deze risico's te mitigeren, of het Erasmus College besluit om af te zien van de nieuwe voorgenomen verwerking.

6.9 Uitwisseling persoonsgegevens

Een verwerker is een partij die in opdracht van het Erasmus College persoonsgegevens verwerkt, zoals een leverancier van een leerlingadministratiesysteem. Als het Erasmus College een verwerker inschakelt om persoonsgegevens te verwerken, dan worden privacy afspraken vastgelegd in een verwerkersovereenkomst. Bepaalt het Erasmus College samen met één of meerdere partijen het doel en middelen voor de verwerking van persoonsgegevens? Dan is sprake van een zogenaamde gezamenlijke verwerkingsverantwoordelijkheid. In dat geval worden ook contractuele afspraken gemaakt rondom de zorgvuldige en veilige verwerking van gegevens.

Persoonsgegevens kunnen ook beschikbaar worden gesteld aan partijen die niet als verwerkers worden aangemerkt, maar als ‘derden’. Deze derden verwerken persoonsgegevens niet in opdracht van een verwerkingsverantwoordelijke, maar voor hun eigen doel. Een verwerkersovereenkomst is daarom ook niet nodig, maar er moet wel een grondslag bestaan om de persoonsgegevens te delen. Denk aan de situatie waarin het Erasmus College gegevens over medewerkers deelt met de Belastingdienst ten behoeve van de loonaangifte. De Belastingdienst verwerkt deze gegevens voor haar eigen wettelijke doeleinden en handelt niet als verwerker.

6.10 Gegevensverwerking buiten de EER

Schakelt het Erasmus College een verwerker in uit een land buiten de Europese Economische Ruimte (EER) dat geen passend beschermingsniveau biedt? Dan gelden aanvullende voorwaarden. Bij een gegevensdeling buiten de EER moeten namelijk (juridische, technische en organisatorische) waarborgen zijn genomen om het beschermingsniveau ook buiten de EER te laten voldoen aan de AVG, zodat de persoonsgegevens voldoende beschermd blijven. Om dit te bereiken is meer nodig dan alleen het sluiten van een verwerkersovereenkomst. In dat geval maakt het Erasmus College gebruik van de Europese modelcontracten, de zogenaamde ‘Standard Contractual Clauses’, en neemt het Erasmus College aanvullende risico gebaseerde beveiligingsmaatregelen. Ook vindt voorafgaand aan de gegevensdeling altijd afstemming plaats met de privacy officer, de CISO en de functionaris gegevensbescherming, om te beoordelen of de getroffen maatregelen voldoende zijn.

NB: De bepalingen van de meest recente versie van het convenant ‘Digitale onderwijsmiddelen en privacy’ zijn leidend bij het maken van afspraken met leveranciers, die als verwerkers in opdracht van de school persoonsgegevens verwerken.

6.11 Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG recht op controle op de verwerking van hun persoonsgegevens. Een betrokkene heeft vanuit de AVG de volgende rechten:

1. Het recht op inzage van de persoonsgegevens welke het Erasmus College verwerkt;
2. Het recht op rectificatie van de persoonsgegevens;
3. Het recht op vergetelheid, dus verwijdering en vernietiging van persoonsgegevens;
4. Het recht op bezwaar tegen een verwerking;
5. Het recht op beperking van de verwerking;
6. Het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming en profilering.

Alle betrokkene van het Erasmus College kunnen een verzoek tot uitoefening van deze rechten indienen via privacy@erasmuscollege.nl. Wanneer een verzoek wordt ingediend dan zal het Erasmus College dit verzoek afhandelen volgens het daarvoor opgestelde protocol. Het Erasmus College heeft een apart Rechten van Betrokkenen management protocol. Zie hiervoor <naam protocol>.

Alle verzoeken worden opgenomen in een wettelijk verplicht register.

Ook hebben betrokkenen het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Het Erasmus College draagt er zorg voor dat de informatie over het uitoefenen van deze rechten op een transparante manier is verstrekt aan betrokkenen via een privacyverklaring. Het Erasmus College zal binnen de wettelijke termijnen, uiterlijk binnen één maand, schriftelijk reageren op het verzoek. In uitzonderlijke situaties kan de reactietermijn worden verlengd, maar dan wordt dit wel binnen een maand gecommuniceerd. Voor AVG-verzoeken geldt een identificatieplicht, zodat de identiteit van de verzoeker kan worden vastgesteld. Hiertoe kan het Erasmus College om extra informatie verzoeken, maar zal hierbij terughoudend zijn met het verzoeken om een kopie identiteitsbewijs.

6.12 Geautomatiseerde besluitvorming en profilering

Het Erasmus College zal bij het verwerken van persoonsgegevens in alle verwerkingen, bedrijfs- en onderwijsprocessen geautomatiseerde besluitvorming en profilering op geen enkele wijze toepassen of laten plaatsvinden.
Tenzij hiervoor sluitende argumentatie bestaat waarover door zowel de CISO, Privacy Officer, de Functionaris gegevensbescherming een positief advies kan worden afgegeven. De uiteindelijke definitieve besluitvorming hierover ligt altijd bij de directeur-bestuurder.

6.13 Naleving AVG

Er vindt specifiek toezicht plaats door het Erasmus College op de naleving van de eisen en voorwaarden uit de AVG, zowel intern als extern. Van belang is dat de eerste lijn hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. Het Erasmus College besteedt in dit verband

actief aandacht aan informatiebeveiliging en privacy bij de aanstelling van medewerkers, tijdens functioneringsgesprekken en via bewustwordingscampagnes.
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan het Erasmus College de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving.

6.14 Functionaris gegevensbescherming (FG)

Voor toezicht op de naleving van de AVG vervult, de door de directeur-bestuurder extern aangestelde Functionaris gegevensbescherming, de belangrijkste rol, zoals wettelijk beschreven in artikel 39 van de AVG. Het Erasmus College, als aanstellende organisatie, zal de Functionaris gegevensbescherming in dit kader faciliteren zoals wettelijk beschreven in artikel 37 en 38 van de AVG.

Het Erasmus College heeft een apart beleidsdocument opgesteld waarin het bovenstaande onder 6.14 nader is uitgewerkt. Zie hiervoor <naam protocol>.

7 Continu verbeteren

7.1 Audits en compliance monitoring

Met regelmaat voert het Erasmus College in- en externe audits uit om te bepalen of opzet, bestaan en werking van het Informatiebeveiliging en Privacy beleid aantoonbaar voldoen aan zowel de interne en externe normen.
Het Erasmus College stelt een auditplan (inclusief frequentie, methoden, verantwoordelijkheden) vast, voert dit uit en rapporteert de resultaten. Bij het opzetten van het auditplan wordt rekening gehouden met het belang van de betrokken processen en eerdere auditresultaten.

Toewijzing verantwoordelijkheid

Voor informatie-risicomanagement en informatiebeveiliging en privacy waarborging heeft het Erasmus College afdeling Interne Audit aangewezen als verantwoordelijke voor uitvoering van de derde lijn. Deze adviseert ook de directeur-bestuurder bij bovengenoemde besluiten, vaststellingen en acceptaties voor zover deze raken aan informatiebeveiliging en privacy waarborging, en over besluiten inzake geconstateerde bevindingen en de afhandeling daarvan.
Het Erasmus College heeft het beheer over vooralsnog niet afgehandelde bevindingen en aanbevelingen inzake informatiebeveiliging neergelegd bij de CISO en inzake privacy waarborging bij de privacy officer en externe functionaris gegevensbescherming.

Audit door audits

Audits, leidende tot rapporten met conclusies, bevindingen en aanbevelingen, zijn het primaire middel waarmee auditors verbeterpunten aandragen aan auditees, de directeur-bestuurder en de Raad van Toezicht. Deze audits worden door daartoe gekwalificeerde auditors uitgevoerd conform kwaliteits- en procesvereisten die de beroepsgroepen waar zij zijn geregistreerd, dwingend opleggen.
Interne en externe auditors hebben hun eigen audit-planningen waarin hun werkzaamheden zijn geagendeerd. Van auditors mag worden verwacht dat zij bij hun planning rekening houden met de door de organisatie onderkende risico's, geaccepteerde tekorten in interne beheersing en in bevinding-oplossingsmogelijkheden, en de agenda's van te betrekken afdelingen en functionarissen.
Interne en externe auditors hebben formeel recht op toegang tot alle door hen noodzakelijk geachte informatie en personen.

7.2 Audit-proces

Auditen bestaat uit het toetsen van feitelijke situaties aan de relevante normen die de organisatie zichzelf heeft opgelegd.

Slechts bij gebreke daarvan kan een auditor voorstellen om normen van buiten te hanteren. Daarbij zal vooraf afstemming met en goedkeuring door de Raad van Toezicht en de directeur-bestuurder in samenspraak met de auditee(s) moeten plaatsvinden over het hanteren van die externe normen. De goedkeuring van de directeur-bestuurder wordt opgenomen bij het Statement of Applicability. Daarin staat per audit (externe) normen wel, en welke niet, van toepassing zijn op het Erasmus College.
Bevindingen zullen niet als tekorten in uitgevoerd werk van de auditiee(s) mogen worden beschouwd

maar als mogelijke verbeterpunten waarover opvolgende besluitvorming door of namens de Raad van Toezicht en de directeur-bestuurder nodig zijn.

7.2.1 Auditjaarplanning

De interne auditor hanteert een planning waarin, op basis van eigen risicoanalyses en op verzoek van de directie, auditobjecten en -aspecten worden ingeschaald op belangrijkheid van goede interne beheersing en voor komend jaar keuzes worden gemaakt welke audits zullen worden uitgevoerd, gegeven beperkte auditcapaciteit. De auditor houdt bij de spreiding gedurende de planning van de audits rekening met de kalender van de auditor zelf en van de auditees zodat de primaire werkzaamheden van de auditees niet onredelijk hoeven worden gestoord. Deze auditplannen worden door de Raad van Toezicht in consultatie met de directeur-bestuurder goedgekeurd.

7.2.2 Auditplanning

Per uit te voeren audit conform de planning, stelt de auditor een planning van werkzaamheden op. Hierbij betrekt de auditor de eigen capaciteit en deskundigheid en die van te betrekken collega's (ook van en voor reeds bekende externe audits). Bij het opstellen van de planning wordt rekening gehouden met samenhang gezocht met de planning en werkzaamheden van de auditees, de uit te voeren detailwerkzaamheden, de te verzamelen informatie en de te hanteren normen.

De auditor bepaalt tevens op basis van een detail-risicoanalyse per norm welke informatie nodig is om een uitspraak te kunnen doen over de kwaliteit van de getoetste interne-beheersingsmaatregelen, hoe diepgaand die informatie is, en op welke wijze de informatie dient te worden verkregen. Auditor kan daardoor per informatie-item nauwkeurig aangeven welke toetsnorm gediend is bij het hebben van dat informatie-item.

7.2.3 Auditwerkzaamheden

De auditor verzamelt de gewenste informatie die deze nodig acht om een uitspraak te kunnen doen over de effectieve opzet, bestaan en/of werking van de getoetste interne-beheersmaatregelen. Als de auditor niet kan of wil vertrouwen op reeds in de gangbare processen opgeleverde informatie omtrent die beheersmaatregelen, zal de auditor zelf onderzoek doen.
Het gereedmaken van informatie alleen ten behoeve van de auditor is geen verplichting voor de auditee noch een recht van de auditor. Slechts indien de directeur-bestuurder directe opdracht heeft gegeven tot het vervaardigen van die informatie (ook wel PBCs genaamd, Prepared By Client), behoort dat tot het werk van betrokkene als arbeidsrechtelijk opgelegde taak waarvoor impliciet en formeel de benodigde werkuren ter beschikking worden gesteld naast de reguliere werkuren van betreffende betrokkene.
Overigens zal de auditor streven naar samenwerking met auditee(s) voor het verkrijgen van de benodigde informatie, in coördinatie met de CISO, Privacy Officer en externe Functionaris gegevensbescherming.

Indien een auditor gedurende de audit bevindingen doet die een hoog risico inhouden voor bijvoorbeeld de informatieveiligheid, dan zullen deze onmiddellijk worden doorgegeven aan onder andere betreffende auditees om zo snel mogelijk risico-verminderende maatregelen te treffen.

7.2.4 Afronding van een audit

De auditor zal bij en na afronding van de werkzaamheden de initiële bevindingen ter controle op juistheid afstemmen met de auditee(s), en opmerkingen en commentaar van auditees opnemen bij de bevinding. Tevens zal de auditor in deze afstemming de haalbaarheid van en beoogde tijdspanne voor oplossing van de bevinding meenemen.

7.2.5 Rapportage

De auditor levert een concept-rapport met conclusie(s), verslag van uitgevoerde werkzaamheden en bevindingen aan de opdrachtgever (de Raad van Toezicht of de directeur-bestuurder of andere) en aan alle in het rapport genoemde verantwoordelijken voor oplossing van bevindingen. Eerst na bespreking met auditees en de directeur-bestuurder over de juistheid van de conclusie, bevindingen etc., levert de auditor aan bovenstaande een definitief rapport op.

7.2.6 Resultaten

De CISO en andere betrokkenen tot het bevindingenregister, ontvangen de bevindingen inclusief aanbevelingen en beoogde oplossingstijden, en voegt deze toe aan het register van bevindingen.
De CISO of andere betrokkenen tot het bevindingenregister bevragen ten minste elk halfjaar de respectievelijk toegewezen verantwoordelijken voor de status van oplossing van de bevinding, en escaleert indien oplossing niet binnen de beoogde termijn dreigt te slagen. Alsdan zal na overleg de directeur-bestuurder tot aanvullende oplossingsinspanning, aanpassing van de oplostermijn of acceptatie van het genoemde risico besluiten.

7.3 Directiebeoordeling en strategische evaluatie

De directeur-bestuurder beoordeelt periodiek het managementsysteem voor informatiebeveiliging en privacy waarborging van het Erasmus College op voortdurende geschiktheid, toereikendheid en doeltreffendheid.

Hierbij wordt aandacht besteed aan de status van verbeterpunten uit eerdere managementreviews, relevante veranderingen in de context en naar de behoeften en verwachtingen van belanghebbenden. Tevens worden trends in afwijkingen en corrigerende maatregelen, resultaten van monitoring en auditresultaten meegenomen. Daarnaast wordt feedback van belanghebbenden, resultaten van risicobeoordelingen en de status van het risicobehandelingsplan beoordeeld, evenals kansen voor continue verbetering.

De managementreviews resulteren in beslissingen voor continue verbetering en wijzigingen in het managementsysteem voor informatiebeveiliging en privacy waarborging, ondersteund door gedocumenteerde informatie.

7.4 Afwijkingen en corrigerende maatregelen

Het Erasmus College waarborgt het voortdurend verbeteren van het managementsysteem voor informatiebeveiliging en privacy waarborging door middel van een Plan, Do, Check, Act-cyclus.

Bij het constateren van afwijkingen reageren we adequaat en treffen passende maatregelen. Daartoe identificeren en beoordelen we deze afwijkingen en oorzaken. Vervolgens evalueren we de effectiviteit van deze corrigerende maatregelen en passen indien nodig wijzigingen toe in ons management voor informatiebeveiliging en privacy waarborging. Als bewijs leggen we de aard van de afwijkingen, de genomen maatregelen en de resultaten van de corrigerende acties vast.

8 Vaststelling en beleidsherziening

Het IBP-beleid wordt door de directeur-bestuurder van het Erasmus College minimaal eenmaal per vier jaar getoetst en indien nodig herzien. Bij een substantiële wijziging van het IBP-beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt er indien nodig een beleidswijziging.

Dit beleid is aldus vastgesteld.

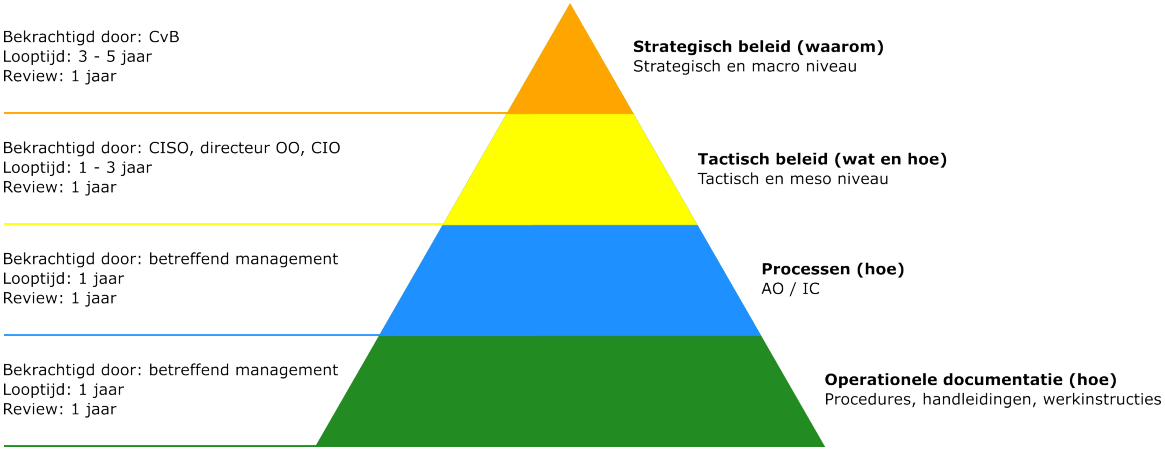
[Plaats], [Datum].

De directeur-bestuurder van het Erasmus College

[Na (her)vaststelling, ook de tabel op p.**Fout! Bladwijzer niet gedefinieerd.** bijwerken]

Bijlage 1 Beleidspiramide

De beleidspiramide van het Erasmus College bestaat uit vier lagen: strategisch beleid, tactisch beleid, processen en operationele documentatie.



Figuur 1: Beleidspiramide

Strategisch beleid

Op het eerste niveau is het strategisch beleid beschreven: het waarom. Beleid wordt formeel bekrachtigd door de directeur-bestuurder en heeft een looptijd van vier jaar.

Tactisch beleid

Op het tweede niveau zijn de beleidsondersteunende (tactische) standaarden en richtlijnen beschreven: het wat. Standaarden worden formeel bekrachtigd door de gemandateerde functionaris(sen). Dit kan / kunnen afhankelijk van het onderwerp zijn de CISO, functionaris gegevensbescherming, CIO, Directeur ICT etc. De standaarden kennen een looptijd van drie jaar.

Processen

Op het derde niveau zijn de (formele) processen beschreven: het hoe. De administratieve organisatie (AO) betreft de structuur en de processen binnen een organisatie die zorgen voor de efficiënte uitvoering van taken en de coördinatie van activiteiten. De Interne Controle (IC) betreft de systemen en processen die Erasmus College in plaats heeft om ervoor te zorgen dat de bedrijfsdoelstellingen worden bereikt, dat de risico's worden beheerd en dat de regelgeving en interne beleidsregels worden nageleefd. Deze processen worden bekrachtigd door het betreffende management. De processen kennen een looptijd van 4 jaar.

Operationele documentatie

Op het laagste niveau van de beleidspiramide zijn de operationele procedures, processen en handleidingen beschreven: het hoe. Deze worden formeel bekrachtigd door het betreffende management. Deze documenten kennen een looptijd van 2 jaar.

Review proces
Aan het einde van de looptijd worden de vastgestelde documenten in onze beleidspiramide herzien, of als hiertoe op basis van ontwikkelingen eerder aanleiding voor is. Minimaal eens per jaar worden de

documenten beoordeeld op actualiteit. Ook als er geen aanpassingen benodigd zijn wordt dit vastgelegd. De documenten worden hierbij voorzien van een nieuw versienummer.

Bijlage 2 Certificeringsschema ROSA

Het Certificeringsschema Informatiebeveiliging en Privacy ROSA is een standaard die wordt gebruikt in de Nederlandse onderwijssector. Het is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA) en biedt een kader voor het toetsen van ICT-leveranciers op het gebied van veiligheid en privacy.

Kernpunten van het schema:

- **Doelgroep:** Specifiek bedoeld voor leveranciers van ICT-toepassingen binnen het primair, voortgezet, middelbaar en hoger onderwijs.
- **Functie:** Het schema stelt instellingen in staat om aan te tonen dat persoonsgegevens veilig worden verwerkt en biedt leveranciers een uniforme manier om hun beveiligingsniveau te bewijzen.
- **Toetsingskader:** Het bevat een toetsingskader (versie 3.0) waarmee organisaties een zelfevaluatie (self-assessment) kunnen uitvoeren of extern getoetst kunnen worden.
- **BIV-classificatie:** Het helpt bij het bepalen van de benodigde maatregelen op basis van de **Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV)** van gegevens.

Toepassing in 2026:

Het schema wordt beheerd door de werkgroep IBP binnen de Edustandaard. Voor onderwijsinstellingen is het gebruik van dit schema vaak een vereiste bij het aansluiten van applicaties via Edukoppeling.

Bijlage 3 FORA-processen

In de context van informatiemanagement en onderwijs verwijst de term FORA-processen naar de procesmodellen binnen de Funderend Onderwijs Referentie Architectuur (FORA).

Belangrijkste kenmerken van FORA-processen (2026)

- **Gestandaardiseerde werkwijze:** De FORA biedt een referentie voor de structuur en werking van onderwijsorganisaties in het primair en voortgezet onderwijs.
- **Werkgroep Processen:** Een gespecialiseerde FORA Werkgroep ontwikkelt en beheert procesmodellen die scholen helpen bij het inrichten van hun eigen organisatie.
- **Specifieke toepassingen:** In 2026 worden deze modellen onder meer ingezet voor complexe trajecten zoals het eindexamenproces, waarbij helderheid over taken, verantwoordelijkheden en benodigde informatie essentieel is.

Algemene procesindeling

Binnen organisaties, inclusief onderwijsinstellingen die de FORA gebruiken, worden processen vaak onderverdeeld in:

1. **Primaire processen:** Leveren direct waarde aan de leerling/klant (bijv. lesgeven).
2. **Ondersteunende processen:** Faciliteren de middelen en systemen (bijv. IT, HR).
3. **Besturende processen:** Geven richting en bewaken de prestaties van de organisatie.

Bijlage 4 BIV classificatie

BIV-classificatie is een methode in de informatiebeveiliging om de waarde en beveiligingsbehoeften van gegevens en systemen vast te stellen. De afkorting staat voor de drie kernpijlers van informatiebeveiliging (ook bekend als de Engelse **CIA-triade**):

- **B - Beschikbaarheid:** Garanderen dat informatie en systemen toegankelijk zijn voor geautoriseerde gebruikers op de momenten dat zij deze nodig hebben.
- **I - Integriteit:** Waarborgen dat informatie juist, volledig en actueel blijft en niet onbevoegd kan worden gewijzigd.
- **V - Vertrouwelijkheid:** Zorgen dat informatie alleen inzichtelijk is voor personen die daar expliciet recht op hebben.

Hoe werkt het?

Bij een BIV-classificatie krijgt elk aspect (B, I en V) een score, meestal op een schaal van 0 tot 3 of laag tot hoog. Deze score bepaalt welke beveiligingsmaatregelen noodzakelijk zijn:

1. **Bepalen van de impact:** Wat zijn de gevolgen als gegevens niet beschikbaar zijn, onjuist zijn of op straat liggen?
2. **Toewijzen van niveaus:** Op basis van de impact wordt een niveau toegekend (bijv. B2, I1, V3).
3. **Selecteren van maatregelen:** Hoe hoger de score, hoe zwaarder de benodigde technische en organisatorische maatregelen om de risico's te beperken.

In Nederland wordt dit model breed toegepast door organisaties zoals de Rijksoverheid en in sectoren zoals het onderwijs om te voldoen aan normen zoals ISO 27001.

Bijlage 5 Overzicht met IBP onderwerpen voor de MR

Wordt apart geleverd.

Bijlage Afkortingen

CISO	Chief information officer
EIAM	Enterprices information architecture model
EER	Europese Economische Ruimte
FG	Functionaris Gegevensbescherming
FORA	Funderend onderwijs referentie architectuur
GRC-Applicatie	Governance risk en complaince privacy control centre
IAM beleid	Identity and Access Management beleid
ICT	Informatie en communicatie technologie
MR	Medezeggenschapsraad
NEN-ISO/IEC	Nederlandse Norm, Internationale organisatie voor standaardisatie, internationaal electrotechnische commissie
Normenkader IBP-FO	Normenkader informatiebeveiliging en privacy funderend onderwijs
ROSA	Referentie Onderwijs Sector Architectuur
PDCA-aanpak	Plan-Do-Check-Act aanpak
PPIA	Preliminary Privacy Impact Assessment – onderzoek naar privacy risico's
SLA-afspraken	Service Level Agreement afspraken
SMDB	Configuratie management database
UAVG	Uitvoeringswet Algemene Verordeing Gegevensbescherming