Faciliteiten en
Informatietechnologie

# REQUIREMENTS - INFORMATIEBEVEILIGING EN PRIVACY

| | |
|---|---|
| *Instituut/Dienst* | Faciliteiten en Informatietechnologie |
| *Datum* | 6 mei 2020 |
| *Versie* | v20200506.1 |

# INHOUDSOPGAVE

# 1. Inleiding

In deze bijlage staan de informatiebeveiligingseisen met betrekking tot de gevraagde dienstverlening beschreven. Voordat wordt ingegaan op deze eisen wordt kort de positie van informatiebeveiliging binnen Hogeschool Rotterdam geschetst. Dit is van belang omdat u als dienstverlener deel gaat uitmaken van de informatieketen van Hogeschool Rotterdam.

## 1.1. Achtergrond

Het bieden van een veilige leer- en werkomgeving is een zeer belangrijke doelstelling van van Hogeschool Rotterdam. Hogeschool Rotterdam onderkent haar verantwoordelijkheid om de belangen van haar studenten, medewerkers en andere stakeholders goed te beschermen, en het vertrouwen wat haar gegund is waar te maken. Informatiebeveiliging, bedrijfscontinuïteit, cyber weerbaarheid en privacy maken integraal deel uit van de wijze waarop Hogeschool Rotterdam opereert.

## 1.2. Informatiebeveiligingsprincipes

Als onderdeel van het informatiebeveiligingsbeleid van Hogeschool Rotterdam is een viertal informatiebeveiligingsprincipes vastgesteld welke de basis vormen voor de wijze waarop informatiebeveiliging, bedrijfscontinuïteit en privacy binnen Hogeschool Rotterdam worden vormgegeven:

I. Wij beschermen te allen tijde, de belangen van studenten, medewerkers en andere stakeholders.
   Wij zorgen dat we op ieder moment en op iedere plek in onze processen, de informatie van de personen op transparante en aantoonbare wijze beschermen en dat die informatie alleen toegankelijk is voor bevoegden, niet verloren kan gaan en/of ongewild wordt veranderd.
II. Wij gebruiken alleen informatie waarvoor die bedoeld is en zijn daar transparant in.
   Wij gebruiken de informatie van personen niet voor andere zaken dan waar een rechtmatige grondslag voor is (zoals wettelijke grondslag of toestemming).
III. Wij hebben robuuste en betrouwbare processen en IT-systemen.
   Bij het ontwikkelen en het in standhouden van processen en IT-systemen, zorgen wij ervoor dat er afdoende maatregelen zijn genomen, die het belang van deze processen en systemen waarborgen.
IV. Wij zijn voorbereid op onverwachte verstoringen van onze dienstverlening.
   Wij zien alle verstoring die zich voordoen en hebben de organisatie voorbereid (processen, middelen en vaardigheden) om daar op een adequate wijze mee om te gaan, zodat de belangen van de stakeholders gewaarborgd zijn.

Bovenstaande principes zijn dan ook direct van toepassing op de wijze waarop de Opdrachtnemer haar werkzaamheden dient uit te voeren en moeten integraal verwerkt zijn in de werkwijze en processen van de Opdrachtnemer.

## 1.3. Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid van Hogeschool Rotterdam is gebaseerd op de NEN-ISO/IEC 27001 norm en de NEN-ISO/IEC 27002 best-practice (waarop gebaseerd set van richtlijnen en maatregelen voor hoger onderwijs in Nederland: SURF normenkaders en Baseline Informatiebeveiliging Hoger Onderwijs). Opdrachtnemer dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NENISO/ IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering.

## 1.4. Wet- en regelgeving

Hogeschool Rotterdam is, onder meer, gehouden aan alle voorschriften uit relevante regelgeving waarbij de volgende wetten het meeste raakvlak hebben met informatiebeveiliging en privacy:

- Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)
  Hogeschool Rotterdam heeft een kwaliteitszorgsysteem conform de InstellingsToets Kwaliteitszorg (ITK). Hierin is (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten gewaarborgd. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.
- Algemene Verordening Gegevensbescherming (AVG)
  Verwerking van persoonsgegevens door of in opdracht van Hogeschool Rotterdam dient te allen tijde te voldoen aan de bepalingen van de AVG.
- Wettelijke Bewaartermijnen/Archiefwet
  Hogeschool Rotterdam houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die zijn vastgelegd in specifieke wetgeving (zoals de Belastingwet en in het arbeidsrecht) en in de Archiefwet en het Archiefbesluit. Hogeschool Rotterdam hanteert daarbij het Basisselectiedocument van de sector hogescholen. Dit selectiedocument gaat over alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites en e-mail. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

# 2. Eisen aan personeel van Opdrachtnemer

De Opdrachtnemer zet personeel in voor het uitvoeren van alle voorkomende werkzaamheden zoals deze zijn onderkend. De volgende eisen worden met betrekking tot de medewerkers van de Opdrachtnemer gesteld.

| Eis | Omschrijving |
|---|---|
| IBP-2.1 | Alle medewerkers die namens/in opdracht van Opdrachtnemer participeren in de levering van de gevraagde dienstverlening moeten bekend zijn met de verantwoordelijkheid op het gebied van informatiebeveiliging en privacy die als onderdeel van zijn / haar rol van toepassing zijn. |
| IBP-2.2 | Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de gevraagde dienstverlening een geheimhoudingsovereenkomst ondertekenen en hier naar handelen. |
| IBP-2.3 | Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de gevraagde dienstverlening een Verklaring Omtrent Gedrag (VOG) of een gelijkwaardig document hebben die niet ouder is dan 12 maanden. De kosten van de VOG zijn voor rekening van de Opdrachtnemer. |
| IBP-2.4 | Bij het betreden van een Locatie van Hogeschool Rotterdam dienen medewerkers van of namens de Opdrachtnemer zich altijd te kunnen legitimeren met een wettelijk geldig legitimatiebewijs. |

# 3. Beveiliging van Diensten

## 3.1. Algemeen

Informatiebeveiliging moet als proces binnen de organisatie geborgd zijn om de informatie met de passende technische en organisatorische maatregelen te kunnen beveiligen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.1.1 | De gevraagde dienstverlening moet opgezet en geleverd worden vanuit het basis principe “Secure-by-Design”. |
| IBP-3.1.2 | Opdrachtnemer heeft informatiebeveiliging en bedrijfscontinuïteit aantoonbaar gestandaardiseerd, gestructureerd, continu en cyclus procesmatig (PDCA cyclus) in alle lagen van de organisatie en gevraagde dienstverlening ingericht. |
| IBP-3.1.3 | De gevraagde dienstverlening moet adequaat zijn beveiligd door het implementeren en onderhouden van een set van technische en organisatorische maatregelen welke de beschikbaarheid, integriteit en vertrouwelijkheid van de dienstverlening en de daarop opgeslagen en/of verwerkte informatie borgt. |
| IBP-3.1.4 | Opdrachtnemer moet een procedure hebben, uitvoeren en de resultaten rapporteren voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de gevraagde dienstverlening. |
| IBP-3.1.5 | Voor het uitvoeren van onderhoud en/of aanpassingen moet aantoonbaar een wijzigingsproces gehanteerd worden (“change management”), waarbij de nadruk ligt op het voorkomen van beveiligingsincidenten, storingen of onderbrekingen tijdens het doorvoeren van veranderingen. |
| IBP-3.1.6 | Opdrachtnemer dient zorg te dragen dat software welke gebruikt wordt als onderdeel van de gevraagde dienstverlening, altijd wordt ondersteund door de fabrikant van de software, dan wel de eigenaar van de sourcecode en functioneert binnen de werkomgeving van Hogeschool Rotterdam. |
| IBP-3.1.7 | Opdrachtnemer garandeert testgegevens, betrokken bij de Prestatie, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik. |

## 3.2. Risicoanalyses

De wendbaarheid van de gevraagde dienstverlening komt voort uit de adequate wijze waarop risico’s worden beheerst waardoor het makkelijker is om op korte termijn risico-gestuurde besluiten te nemen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.2.1 | Opdrachtnemer moet structureel risicoanalyses uitvoeren in het bouw- en implementatietraject, als onderdeel van de PDCA cyclus, bij grote onderhoudstrajecten, en bij significante wijzigingen in de gevraagde dienstverlening. |

| | |
|---|---|
| IBP-3.2.2 | Opdrachtnemer legt onderkende risico's vast in een register en deze wordt door Opdrachtnemer voorzien van de benodigde (borgings-)maatregelen ter mitigatie van de risico's. |
| IBP-3.2.3 | Opdrachtnemer moet Hogeschool Rotterdam direct op de hoogte stellen van risico's die een directe impact op Hogeschool Rotterdam kunnen vormen en waarbij de mitigerende maatregelen op onvoldoende wijze het risico beperken. |
| IBP-3.2.4 | Periodiek (minimaal eens per jaar) moet worden gerapporteerd over de status van de risico's en de bijbehorende (voortgang van de) mitigerende maatregelen. |

## 3.3. Logische toegangsbeveiliging

Logische toegangsbeveiliging richt zich op het administreren en beheren van gebruikers en resources inclusief toegangsrechten en toegangscontrole. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.3.1 | De ingezette logische toegangsbeveiligingsmiddelen moeten betrouwbare en effectieve mechanismen leveren voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, en het controleerbaar maken van het gebruik van deze middelen. |
| IBP-3.3.2 | De gevraagde dienstverlening moet afdwingen dat gebruikers alleen toegang hebben tot informatie, beheertaken en speciale bevoegdheden voor zover dat voor de uitoefening van de werkzaamheden noodzakelijk is ("need to know", "need to use", "least privilege") en ze hiervoor herleidbaar geautoriseerd zijn. |
| IBP-3.3.3 | Voor applicaties die vereisen dat een set van identiteitsinformatie van gebruikers in het systeem aanwezig is, moet gebruik worden gemaakt van automatische provisioning. Hogeschool Rotterdam is hierbij verantwoordelijk voor het vaststellen van de filtering van de accountattributen die geprovisioned worden. |
| IBP-3.3.4 | Opdrachtnemer is verantwoordelijk voor het periodiek (minimaal eens per jaar) controleren van de toegangsrechten van de eigen medewerkers die werkzaamheden uitvoeren ten behoeve van de gevraagde dienstverlening en legt hierover verantwoording af als onderdeel van de periodieke rapportage. |

## 3.4. Vulnerability management

Het tijdig informatie verkrijgen over technische kwetsbaarheden van de gebruikte informatiesystemen is van vitaal belang bij de beveiliging van de gevraagde dienstverlening. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor de mitigatie van de daarmee samenhangende risico's. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.4.1 | Het beheer van kwetsbaarheden (vulnerability management) moet procesmatig en regulier (minimaal eens per kwartaal) worden uitgevoerd op alle ICT componenten behorend bij de gevraagde dienstverlening. |

| | |
|---|---|
| IBP-3.4.2 | Voor in gebruik name van een nieuwe dienst / ICT component en bij een significante wijziging moet een kwetsbaarhedenscan uitgevoerd worden en moeten de bevindingen opgelost worden. |
| IBP-3.4.3 | Opdrachtnemer rapporteert periodiek (minimaal eens per jaar) over de resultaten van de kwetsbaarhedenscans en de daarbij behorende (voorgestelde) mitigerende maatregelen. |

## 3.5. Patch management

Patch management is het proces dat ervoor zorgt dat alle componenten (ICT-systemen) ingezet voor de gevraagde dienstverlening systematisch voorzien worden van de vereiste patches. Het zorgt voor het verwerven, testen en installeren van patches. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.5.1 | Patch management moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de gevraagde dienstverlening en borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd. |
| IBP-3.5.2 | Indien een (beveiligings)patch beschikbaar is, moeten de risico's verbonden aan de installatie van de patch worden geëvalueerd en moet de patch getest worden alvorens deze op productiesystemen wordt toegepast. |
| IBP-3.5.3 | Opdrachtnemer rapporteert periodiek (minimaal eens per jaar) over de resultaten van het patch management proces en de daarbij behorende (eventuele) afwijkingen en/of risico's. |

## 3.6. Security hardening

Security hardening is het proces dat ervoor zorgt dat alle componenten (ICT-systemen) ingezet voor de gevraagde dienstverlening op gestandaardiseerde wijze worden ingericht en structureel beheerd, waarbij de insteek is om de veiligheidsrisico's zoveel mogelijk te elimineren. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.6.1 | Security hardening moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de gevraagde dienstverlening. |
| IBP-3.6.2 | Bij het vaststellen en toepassen van de security hardening richtlijnen moet minimaal onderscheid gemaakt worden tussen de volgende ICT componenten:<br>• Applicaties;<br>• Middleware en databases;<br>• Platformen / infrastructuur;<br>• Netwerken; en<br>• Connectiviteit |
| IBP-3.6.3 | Opdrachtnemer hanteert internationaal erkende security hardening standaarden, zoals de CIS (Center of Internet Security) benchmarks, als basis voor het vaststellen van de security hardening richtlijn voor de ICT componenten. |

| | |
|---|---|
| IBP-3.6.4 | Opdrachtnemer toetst periodiek (minimaal eens per kwartaal) alle ICT componenten op basis van de vastgestelde richtlijn en rapporteert de resultaten periodiek (minimaal eens per jaar). Geconstateerde afwijkingen worden hierin, na analyse, op basis van risico inschatting benoemd. |

## 3.7. Penetratietesten

Met het uitvoeren van penetratietesten kan met een beperkte mate van zekerheid ingeschat worden in hoeverre de ICT componenten als onderdeel van de gevraagde dienstverlening kwetsbaar zijn voor inbraak. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.7.1 | Penetratietesten moeten procesmatig en procedureel, ondersteund door richtlijnen, worden uitgevoerd op alle ICT componenten van de gevraagde dienstverlening. |
| IBP-3.7.2 | Voor in gebruik name van een nieuwe dienst / ICT component of bij een significante wijziging, en minimaal jaarlijks, moet een penetratietest uitgevoerd worden en moeten de bevindingen opgelost worden. |
| IBP-3.7.3 | Opdrachtnemer rapporteert de resultaten van de uitgevoerde penetratietesten periodiek (minimaal eens per jaar). Geconstateerde bevindingen en de opvolging hiervan worden, na analyse, op basis van risico inschatting benoemd. |

## 3.8. Beveiliging webapplicaties

Het beveiligen van webapplicaties heeft tot doel om te waarborgen dat webapplicaties functioneren zoals is beoogd, ingericht zijn volgens specifieke beleidsuitgangspunten van de organisatie en voldoen aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.8.1 | Bij het ontwikkelen, implementeren en beheren van een webapplicatie moet gebruik gemaakt worden van Secure Software Development technieken om de beveiliging van de webapplicatie te borgen. |
| IBP-3.8.2 | De gevraagde dienstverlening moet voldoen aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties (September 2015)[1], dan wel de logische opvolgers daarvan. |
| IBP-3.8.3 | Opdrachtnemer moet de OWASP top tien[2] structureel hanteren om meest kritische beveiligingsrisico's binnen een webapplicatie te vermijden. |
| IBP-3.8.4 | De cryptografische beveiligingsvoorzieningen van de gevraagde dienstverlening moeten voldoen aan de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS)[3], dan wel logische opvolgers daarvan. |

[1] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
[2] https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
[3] https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

| | |
|---|---|
| IBP-3.8.5 | De cryptografische beveiligingsvoorzieningen moeten minimaal een score van 'A' behalen in de SSL Labs server test[4] en Opdrachtnemer draagt er zorg voor dat de dienstverlening hieraan blijft voldoen. |

## 3.9. Infrastructurele beveiligingseisen

De doelstelling is te waarborgen dat de infrastructuur werkt zoals beoogd, ingericht is volgens specifieke beleidsuitgangspunten, en voldoet aan de eisen ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-3.9.1 | Als onderdeel van de architectuur van de gevraagde dienstverlening moet netwerksegmentatie / zonering conform een "defense in depth" strategie worden toegepast. |
| IBP-3.9.2 | De componenten die deel uitmaken van de gevraagde dienstverlening en de diensten die hierover aangeboden worden moeten worden beschermd tegen aanvallen op de beschikbaarheid, integriteit en vertrouwelijkheid. |
| IBP-3.9.3 | In de ICT infrastructuur moeten signaleringsfuncties (registratie/logging en detectie) actief, efficiënt, effectief en beveiligd ingericht zijn. |
| IBP-3.9.4 | De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen moeten regelmatig worden gemonitord (bewaakt, geanalyseerd) en de bevindingen periodiek gerapporteerd als onderdeel van het informatiebeveiliging incidentenproces. |
| IBP-3.9.5 | De Opdrachtnemer dient voor alle Diensten Professionele maatregelen te nemen om de mogelijkheid van afluisteren van netwerkverbindingen en/of wijzigen van datastromen te verhinderen. Hiertoe worden binnen de branche gebruikelijke maatregelen toegepast. De Opdrachtnemer dient op aanvraag van Opdrachtgever inzichtelijk te maken welke maatregelen geïmplementeerd zijn en hoe deze gecontroleerd worden. |
| IBP-3.9.6 | Indien mobiele apparatuur in gebruik door personeel gegevens bevat gerelateerd aan de Prestatie die door Opdrachtgever en/of Opdrachtnemer als vertrouwelijk is geclassificeerd, dient Opdrachtnemer in ieder geval deze gegevens te versleutelen middels cryptografische toepassingen, waarbij uitsluitend algoritmes en instellingen worden gebruikt met de duiding goed uit de meest actuele versie van het Nationaal Cyber Security Centrum (NCSC) document Richtlijnen voor Transport Layer Security (TLS). |

## 3.10. Cloud

De veiligheid van gegevens van Hogeschool Rotterdam is van kritiek belang bij het gebruik van dienstverlening die vanuit "de Cloud" wordt aangeboden, waarbij er in dezen vanuit wordt gegaan dat vertrouwelijke informatie en/of persoonsgegevens onderdeel zijn van deze gegevens. Het is dan ook belangrijk om naast de al gestelde eisen, een aantal specifieke eisen voor Cloud leveranciers te stellen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

[4] https://www.ssllabs.com/ssltest

| Eis | Omschrijving |
|---|---|
| IBP-3.10.1 | Verwerking van data moet uitsluitend plaatsvinden binnen de Europese Economische Ruimte (Europese Unie, Noorwegen, Liechtenstein, IJsland). |
| IBP-3.10.2 | Alle koppelingen tussen applicaties (interoperabiliteit) moet op basis van open standaarden plaatsvinden en worden standaard via de koppelpunten van Hogeschool Rotterdam geleid. |
| IBP-3.10.3 | Opdrachtnemer moet garanderen en aantonen dat de gegevens van Hogeschool Rotterdam logisch en functioneel gescheiden zijn van de overige afnemers. |
| IBP-3.10.4 | De gevraagde dienstverlening biedt een oplossing om vertrouwelijke en/of gevoelige gegevens versleuteld op te slaan waarbij gebruik gemaakt wordt van de geldende 'best practices' (afhankelijk van de stand der techniek) m.b.t. versleuteling. |
| IBP-3.10.5 | De encryptie sleutels die gebruikt worden voor het versleutelen van de gegevens moeten adequaat beheerd worden door de Opdrachtnemer waarbij Hogeschool Rotterdam inzicht wil hebben in het beheer en gebruik van de encryptiesleutels. De bij de Opdrachtnemer toegepaste encryptie sleutels moeten per direct ingetrokken of onbruikbaar kunnen worden gemaakt. |
| IBP-3.10.6 | In het kader van dataportabiliteit moet de Opdrachtnemer de volgende voorzieningen direct ter beschikking stellen voor het exporteren van data (na beëindiging van de dienstverlening):<br>• SaaS – Data moet beschikbaar zijn in een voor Hogeschool Rotterdam bruikbaar format zoals CSV, Excel (xlsx) en/of PDF (1.7). In het geval er sprake is van aanlevering van documenten tijdens gebruik van de dienst, dan moet het "originele / oorspronkelijke" format van het document (inclusief mappenstructuren) beschikbaar zijn. |

# 4. Privacy

De Algemene Verordening Gegevensbescherming (AVG) beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens. In dit overzicht zijn niet de eisen herhaald die zowel van toepassing zijn op privacy als op informatiebeveiliging; deze zijn reeds opgenomen in hoofdstuk 3. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-4.1 | De gevraagde dienstverlening moet gedurende de gehele looptijd van de Raamovereenkomst voldoen aan de algemene vigerende wet- en regelgeving van de Nederlandse overheid, waaronder de AVG (Algemene Verordening Gegevensbescherming). |
| IBP-4.2 | In lijn met Verwerkersovereenkomst moet Opdrachtnemer de van Hogeschool Rotterdam ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van Hogeschool Rotterdam verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die partijen zijn overeenkomen, en zal Opdrachtnemer de persoonsgegevens dus niet gebruiken voor:<br>• Het uitvoeren van testen; en<br>• Het uitvoeren van data-analyses. |
| IBP-4.3 | Daar waar Hogeschool Rotterdam geen volledige toegang heeft tot de persoonsgegevens moet Opdrachtnemer Hogeschool Rotterdam ondersteunen bij verzoeken tot inzage, correctie en eventueel het wissen van persoonsgegevens. |
| IBP-4.4 | De gevraagde dienstverlening moet de mogelijkheid bieden om gegevenselementen die niet strikt noodzakelijk zijn voor latere verwerkingen of waarvoor geen doelbinding/rechtsgrond aanwezig is te verwijderen of te verbergen. |
| IBP-4.5 | Encryptie moet door Opdrachtnemer worden toegepast als een van de Privacy by design maatregelen indien er sprake is van:<br>1. Transport van persoonsgegevens over openbare of semiopenbare infrastructuur (internet, e-mail, extranet, etc.).<br>2. Opslag en/of transport van persoonsgegevens op locaties en/of media waarbij de fysieke en/of logische beveiligingsmaatregelen ontoereikend worden geacht. |
| IBP-4.6 | Bij het toepassen van data-protection-by default moet bij het inrichten van autorisatierollen rekening gehouden worden met privacy en worden alleen die persoonsgegevens getoond die een medewerker nodig heeft voor zijn of haar functie. |
| IBP-4.7 | De Opdrachtnemer dient de integriteit en vertrouwelijkheid van het over zijn netwerk getransporteerde gesprek/verkeer van Hogeschool Rotterdam te waarborgen. |

# 5. Uitvoeringsaspecten

## 5.1. Beveiligingsincidenten

Een beveiligingsincident is iedere handeling in strijd met het vastgestelde informatiebeveiligingsbeleid (van Opdrachtnemer en/of Hogeschool Rotterdam), of een gebeurtenis, met (mogelijk) nadelige gevolgen voor de beschikbaarheid, integriteit en/of vertrouwelijkheid van systemen en/of informatie, die vallen onder de verantwoordelijkheid en/of het beheer van Hogeschool Rotterdam en/of Opdrachtnemer. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-5.1.1 | Opdrachtnemer meldt informatiebeveiligingsincidenten onverwijld per email via het emailadres cert@hr.nl |
| IBP-5.1.2 | In het geval van een informatiebeveiligingsincident moet de Opdrachtnemer redelijkerwijs maatregelen treffen om de gevolgen en de schade te beperken voortkomend uit het incident. |
| IBP-5.1.3 | Opdrachtnemer moet volledige medewerking geven bij het onderzoeken en oplossen van het informatiebeveiligingsincident en stelt, indien gevraagd, alle informatie met betrekking tot het incident ter beschikking aan Hogeschool Rotterdam. |

## 5.2. Controle en audits

Ter ondersteuning van de eisen die Hogeschool Rotterdam stelt aan haar Opdrachtnemer, moet gedurende de looptijd van de Raamovereenkomst met de Opdrachtnemer een aantal controles en/of audits uitgevoerd worden. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-5.2.1 | Hogeschool Rotterdam heeft het recht om bij Opdrachtnemer een onderzoek (of audit ) in te stellen met betrekking tot de naleving van de in het Beschrijvend document, de Raamovereenkomst, de Wachtkamerovereenkomst en de Bijlagen opgenomen verplichtingen aangaande de gevraagde dienstverlening. De audit wordt altijd door een onafhankelijke derde partij (auditor) uitgevoerd en kosten zijn voor rekening van Hogeschool Rotterdam. |
| IBP-5.2.2 | Minimaal jaarlijks levert Opdrachtnemer een recente formele audit-verklaring die past bij de aard van de gevraagde dienstverlening (zoals een ISAE 3000 rapportage op basis van één of meerdere SOC2 – Trusted Services Principes, of gelijkwaardig) op, die is afgegeven door een onafhankelijke geaccrediteerde auditor en waarmee de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de gevraagde dienstverlening wordt aangetoond. |

## 5.3. Overleg & rapportage

Als onderdeel van de besturing van de door Opdrachtnemer geleverde dienstverlening vindt regulier overleg plaats tussen Hogeschool Rotterdam en Opdrachtnemer en levert Opdrachtnemer periodiek rapportages op. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

| Eis | Omschrijving |
|---|---|
| IBP-5.3.1 | Opdrachtnemer stelt een vaste contactpersoon aan die voor de gevraagde dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy. |
| IBP-5.3.2 | Gestructureerd en periodiek (minimaal eens per jaar) moet overleg tussen Opdrachtnemer en Hogeschool Rotterdam plaatsvinden om zowel de rapportages als (eventuele) issues te bespreken. |
| IBP-5.3.3 | Opdrachtnemer moet zorgen voor een rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligingsmaatregelen en het gerealiseerde beveiligingsniveau (inclusief privacy) binnen de scope van de geleverde dienstverlening. |