Faciliteiten en
Informatietechnologie

Informatiebeveiligingseisen

voor levering van IT dienstverlening

Instituut/Dienst	Faciliteiten en Informatietechnologie
Auteur(s)	J.P.G. Sleddens
Functie auteur(s)	Central Information Security Officer
Datum	16 augustus 2022
Versie	20220816.1

Versiebeheer

Versie	Datum	Opmerkingen
20200506.1	2020-05-06	Definitieve versie van het document 'Requirements – Informatiebeveiliging en Privacy'.
20220608.1	2022-06-08	Eerste conceptversie van herzien concept. Dit concept is geheel gebaseerd op het SURF Juridisch Normenkader (Cloud)services (JNK) waar ook het gebruikte model verwerkingsovereenkomst uit afkomstig is. Alle eisen overgenomen uit bijlage C van het JNK.
20220622.1	2020-06-22	Tweede conceptversie. Inleidende paragrafen bijgewerkt en eisen doorgenomen en afgestemd op beleid HR. Afwijkingen in de eisen t.o.v. JNK zijn in de referentiekolom aangeduid met 'HR'.
20220816.1	2020-08-16	Eerste reviewversie ter bespreking in het IT-stafoverleg.

Mededelingen

Dit document vervangt het document 'Requirements – Informatiebeveiliging en Privacy'.

Inhoudsopgave

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.

Achtergrond

Het bieden van een veilige leer- en werkomgeving is een zeer belangrijke doelstelling 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.

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.

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.

Informatiebeveiligingseisen

De eisen in dit document zijn gebaseerd op het SURF Juridisch Normenkader (Cloud)services. Op deze manier stellen we dezelfde eisen als SURF en collega onderwijsinstellingen.

Onderstaande bepalingen zijn eisen die onderdeel zijn van de aanbesteding of andersoortig inkooptraject. De Opdrachtnemer of leverancier verklaart aan de eisen in dit document te voldoen gedurende de gehele contractduur.

De eisen aangemerkt met *'HOOG'* gelden in ieder geval voor dienstverlening waarbij bijzondere persoonsgegevens verwerkt worden, in andere gevallen geeft Opdrachtgever aan of deze eisen meegenomen moeten worden. Indien de met *'HOOG'* geclassificeerde eisen in acht moeten worden genomen en er ook een eis met dezelfde nummering zonder *'HOOG'* classificatie bestaat, dan geldt de eis met de classificatie *'HOOG'*.

1. Beleid en organisatie

Een door de directie vastgesteld en uitgedragen beveiligingsbeleid is de basis van alle informatiebeveiliging. Het beleid wordt gebaseerd op een analyse van de risico's. Personeel, zowel vaste en tijdelijke werknemers als ingehuurd personeel, is zich bewust van het beleid en kent zijn verantwoordelijkheden. Voor het beheer van incidenten, inclusief datalekken, wijzigingen en beschikbaarheid is een proces ingericht.

#	Maatregel	Referentie
	Actueel informatiebeveiligingsbeleid en organisatie van informatiebeveiliging	
1.1	De directie van de leverancier heeft een Informatiebeveiligingsbeleid vastgesteld en communiceert dit aantoonbaar op regelmatige basis (jaarlijks), zowel intern als aan relevante externe partijen.	ISO 27002:2013 §5.1.1
1.2	Het informatiebeveiligingsbeleid wordt tenminste jaarlijks beoordeeld of als zich een grote verandering heeft voorgedaan.	ISO 27002:2013 §5.1.2
1.3	De leverancier heeft de verantwoordelijkheden met betrekking tot Informatiebeveiliging gedefinieerd en vastgelegd, en toegepast in de vorm van functiebeschrijvingen.	ISO 27002:2013 §6.1.1
	Risicoanalyse	
1.4	De leverancier voert ten minste iedere 3 jaar een risicoanalyse uit om de bedreigingen en kwetsbaarheden, de gevolgen daarvan voor de organisatie en de kans op die gevolgen in kaart te brengen. Op basis van de risicoanalyse worden adequate beveiligingsmaatregelen vastgesteld en ingevoerd.	ISO 27001:2013 §8.2
1.4 HOOG	De leverancier voert ten minste **ieder jaar** een risicoanalyse uit om de bedreigingen en kwetsbaarheden, de gevolgen daarvan voor de organisatie en de kans op die gevolgen in kaart te brengen. Op basis	ISO 27001:2013 §8.2

	van de risicoanalyse worden adequate beveiligingsmaatregelen vastgesteld en ingevoerd.	
1.5	De leverancier beschrijft hoe de geïdentificeerde risico's worden behandeld en onderbouwt waarom eventuele restrisico's worden geaccepteerd.	ISO 27001:2013 §8.2
	Bewustzijn en training	
1.6	Alle werknemers van de leverancier en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, krijgen training bij indiensttreding en vervolgens regelmatig bijscholing over het Informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures.	ISO 27002:2013 §7.2.2
1.6 HOOG	Alle werknemers van de leverancier en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen training bij indiensttreding en vervolgens **tenminste jaarlijks** bijscholing over het Informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures.	ISO 27002:2013 §7.2.2
	Incidentenbeheer en datalekken	
1.7	De leverancier voert incidentenbeheer procesmatig uit. De activiteiten classificeren, prioriteren, diagnosticeren, communiceren en dossiervorming worden daarbij onderscheiden.	ISO 27002:2013 §16.1.1
1.8	De leverancier heeft functiebeschrijvingen in gebruik waarin de taken met betrekking tot incidentenbeheer zijn opgenomen.	ISO 27002:2013 §16.1.1
1.9	De leverancier hanteert een vaste werkwijze en vast format voor incidentrapportages.	ISO 27002:2013 §16.1.2
1.10	De leverancier heeft een incident classificatiekader (al dan niet geautomatiseerd) naar urgentie en impact in gebruik.	ISO 27002:2013 §16.1.4
1.11	De leverancier heeft een procedure ingericht om de opdrachtgever tijdig en adequaat te informeren over potentiële datalekken waarvan hij kennis krijgt (inclusief die bij sub-verwerkers of hulpleveranciers) en documenteert bij een incident alle stappen die zijn ondernomen in het kader van de meldplicht datalekken.	AVG, art. 28.3 Beleidsregels Meldplicht Datalekken, H2.1 – 2.4 (AP)
	Wijzigingsbeheer	
1.12	De leverancier heeft een proces ingericht voor wijzigingsbeheer, bijvoorbeeld op basis van ITIL3 of ISO 20000-1.	ISO 27002:2013 §12.1.2
1.13	De leverancier test wijzigingen in een test- of acceptatieomgeving alvorens deze in productie te brengen en legt testresultaten vast.	ISO 27002:2013 §12.1.4, §14.2.6, §14.2.9
1.14	De leverancier voert wijzigingen uit in de afgesproken servicevensters en overlegt wijzigingen met grote impact voorafgaand aan realisatie met de opdrachtgever.	
1.14 HOOG	De leverancier voert wijzigingen uit in de afgesproken servicevensters en legt wijzigingen met grote impact voorafgaand aan realisatie voor aan de *Change Advisory Board.*	
1.15	De leverancier documenteert de situatie na een wijziging in de configuratiedatabase.	ISO 27002:2013 §12.4.1
	Continuïteitsbeheer	

1.16	De leverancier heeft preventieve en correctieve maatregelen ten behoeve van de realisatie van de beschikbaarheidseisen aantoonbaar getroffen.	ISO 27002:2013 §17.2
1.17	De leverancier is bekend met de single points of failure in de infrastructuur en heeft maatregelen getroffen om storingen binnen de afgesproken termijn te kunnen verhelpen.	ISO 27002:2013 §17.2
1.18	De leverancier bewaakt de beschikbaarheid en capaciteit van applicaties en systemen continu.	ISO 27002:2013 §12.1.2 en §12.1.3
1.18 HOOG	De leverancier bewaakt de beschikbaarheid en capaciteit van applicaties en systemen continu. Overschrijdingen van drempelwaarden worden tijdig gesignaleerd en gerapporteerd aan de opdrachtgever.	ISO 27002:2013 §12.1.2 en §12.1.3
1.19	De leverancier maakt back-ups conform beschikbaarheidseisen.	ISO 27002:2013 §12.3
1.20	De leverancier bewaart back-ups beveiligd off-site. Een afstand van ten minste vijf kilometer tussen primaire opslag en backup locatie is daarbij vereist.	ISO 27002:2013 §12.3
1.21 HOOG	De leverancier heeft voor de geleverde diensten continuïteits- of disaster recoveryplannen beschikbaar, actualiseert ze regelmatig en test op regelmatige basis. Opdrachtgever wordt op de hoogte gesteld wanneer de testen zijn gepland, indien er impact op de geleverde dienst kan zijn. Indien tekortkomingen worden geconstateerd, dient er een verbeterplan of nieuw plan met duidelijk omschreven acties te worden opgesteld.	
	Geheimhouding	
1.22	De leverancier heeft een geheimhoudingsovereenkomst voor werknemers en derden in gebruik.	ISO 27002:2013 §7.1.2 (a) en §13.2.4
1.23 HOOG	Werknemers van de leverancier en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, die betrokken zijn bij verwerkingen van gegevens van Opdrachtgever, dienen een Verklaring Omtrent het Gedrag (VOG) over te leggen.	ISO 27002:2013 §7.1.1 HR

2. Toegangsbeveiliging

Toegangscontrole is essentieel voor het bepalen en weten wie toegang heeft tot (gevoelige) data. Daartoe wordt aan iedere gebruiker een uniek login ID toegekend en, eventueel op basis van rollen, toegang verleend tot de data. Onder toegangscontrole vallen ook fysieke toegangscontrole en toegang tot mobiele apparatuur.

#	Maatregel	Referentie
	Fysieke toegangsbeveiliging en beveiliging van apparatuur	
2.1	IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. Genomen maatregelen zijn in overeenstemming met de vastgestelde risico's.	ISO 27002:2013 §11.1 en §11.2
	Logische toegangsbeveiliging	
2.2	De leverancier heeft een beleid voor toegangsbeveiliging vastgesteld en gedocumenteerd, waarin in ieder geval is bepaald dat: • gebruikers en beheerders een unieke login ID en wachtwoord combinatie hebben, • gedeelde login ID en wachtwoord combinaties niet zijn toegestaan en • toegang voor gebruikers en beheerders beperkt is tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	ISO 27002:2013 §9.1 en §9.2.4
2.3	De leverancier heeft een beleid inzake mobiele apparatuur, waarin ten minste is opgenomen dat: • het apparaat is voorzien van toetsvergrendeling of een vergelijkbaar middel, bijv. toegang via wachtwoord, • privé en zakelijk gebruik gescheiden zijn en bedrijfsdata op het device versleuteld is.	ISO 27002:2013 §6.2.1 en §11.2.8
2.4	De leverancier richt een formeel proces in voor het beheer van toegangsrechten van gebruikers en beheerders. Het toegangsbeheerproces omvat ten minste: • het registreren van gebruikers en de aan hen toegekende rechten, • het toekennen van niet meer rechten dan nodig voor de uitoefening van taken en • het wijzigen of intrekken van die rechten bij wijziging of beëindiging van het dienstverband of contract.	ISO 27002:2013 §9.2.1, §9.2.2, §9.2.3, §9.4.1 en §9.2.6
2.5	Gebruikers en beheerders worden op de hoogte gesteld van het toegangsbeveiligingsbeleid en ondertekenen een verklaring dat zij persoonlijke geheime authenticatie-informatie geheimhouden en in geval van inbreuk direct maatregelen nemen om de gevolgen te beperken.	ISO 27002:2013 §9.3.1

2.6	De leverancier controleert maandelijks of toegekende rechten juist zijn.	ISO 27002:2013 §9.2.5
2.7	Aan de hand van het toegangsbeveiligingsbeleid richt de leverancier beveiligde inlogprocedures voor systemen en toepassingen in. De inlogprocedures omvatten ten minste een sterk wachtwoord. Uit de risicoanalyse volgt of sterke authenticatie (multi-factor authentication) voor specifieke systemen of toepassingen vereist is.	ISO 27002:2013 §9.4.2, §9.4.3

3. Beheer van technische kwetsbaarheden en anti-malware

Malware kan het netwerk en systemen op diverse manieren binnendringen en misbruik maken van kwetsbaarheden. Het gebruik van antivirussoftware en het regelmatig testen van systemen en applicaties op kwetsbaarheden vermindert deze dreiging.

#	Maatregel	Referentie
	Kwetsbaarhedenbeheer	
3.1	De leverancier richt een proces in ter voorkoming van het benutten van technische kwetsbaarheden. Het proces omvat in ieder geval: • het regelmatig up-to-date houden van systemen en software (patching), • het tijdig vergaren van informatie over nieuwe kwetsbaarheden (intelligence), • het controleren van netwerk en systemen op kwetsbaarheden (vulnerability assessment), • het testen van webapplicaties, op regelmatige basis, op kwetsbaarheden (Web application scanning), • het gebruik van antivirussoftware die dagelijks wordt geactualiseerd, • beperkingen op het installeren van (ongeautoriseerde) software.	ISO 27002:2013 §12.2, §12.6.1, §12.6.2
3.1 HOOG	De leverancier richt een proces in ter voorkoming van het benutten van technische kwetsbaarheden. Het proces omvat in ieder geval: • het regelmatig up-to-date houden van systemen en software (patching), • het tijdig vergaren van informatie over nieuwe kwetsbaarheden (intelligence), • het *geautomatiseerd* controleren van programmapakketten en infrastructurele programmatuur op bekende zwakheden, • het *continu* testen van webapplicaties op kwetsbaarheden (Web application scanning) *en het uitvoeren van een penetratietest ten minste eenmaal per jaar*, • het gebruik van *anti-malware (inclusief anti-virus) software van verschillende aanbieders met verschillende engines* die dagelijks worden geactualiseerd, • beperkingen op het installeren van (ongeautoriseerde) software.	ISO 27002:2013 §12.2, §12.6.1, §12.6.2

	Intrusion Detection	
3.2	De leverancier inspecteert gegevensverkeer vanuit externe of nietvertrouwde netwerken real-time.	ISO 27002:2013 §13.1.2
3.3 HOOG	De leverancier heeft een Intrusion Detection/Prevention Systeem dat netwerk gebaseerde aanvallen herkent op basis van signatures, protocol validatie en anomaly detection.	ISO 27002:2013 §13.1.2
3.4 HOOG	De leverancier verwijdert alle niet voor de dienst(en) noodzakelijke services op systemen en/of zet ze uit (disabled), of – indien de systeemsoftware dit niet toelaat – blokkeert de dienst(en) via gedocumenteerde filters op de meest nabijgelegen netwerkcomponent die deze filtering kan verschaffen.	

4. Vertrouwelijkheid en integriteit van gegevens, privacy

Wanneer een aanvaller de toegangscontrole weet te omzeilen moet de data goed beschermd zijn. Dit geldt zowel voor data in rust als voor data in transit. Voor de bescherming van privacygevoelige data zijn extra maatregelen gewenst.

#	Maatregel	Referentie
	Bescherming persoonsgegevens	
4.1	De leverancier beschikt over een privacybeleid of een privacyreglement dat niet ouder is dan drie jaar en voldoet aan de eisen uit de AVG.	ISO 27002:2013 §18.1.1
4.2	De leverancier heeft een privacyfunctionaris benoemd en deze is in functie.	AVG, art. 37, 38 en 39
	Versleuteling	
4.3	De leverancier versleutelt vertrouwelijke gegevens, waaronder privacygevoelige informatie, in rust in ieder geval in de volgende situaties: • op verwijderbare media (zoals extern opgeslagen back-up tapes, DVD's, geheugenkaarten en USB-sticks); • in het opslaggeheugen van mobiele apparatuur (zoals het in- en externe geheugen van laptops, smartphones en tablets).	ISO 27002:2013 §10.1, §13.2, §14.1.2 CBP Richtsnoer *beveiliging persoonsgegevens*, pag. 25
4.3 HOOG	De leverancier versleutelt vertrouwelijke gegevens, waaronder privacygevoelige informatie, in rust *te allen tijde*.	
4.4	End-to-end encryptie is altijd noodzakelijk, indien data die als gevoelig of kritiek is geclassificeerd getransporteerd wordt (zoals tijdens back-up). De leverancier versleutelt vertrouwelijke gegevens, waaronder privacygevoelige informatie, in beweging in ieder geval in de volgende situaties: • beheersessies over het eigen netwerk (met encryptievoorzieningen binnen de beheertools of gebruikte protocollen); • draadloze datacommunicatie; • wachtwoorden, die worden opgeslagen of verzonden.	
4.4 HOOG	End-to-end encryptie is altijd noodzakelijk, indien data getransporteerd wordt. De leverancier versleutelt vertrouwelijke gegevens, waaronder privacygevoelige informatie, in beweging *te allen tijde*.	
4.5	De leverancier maakt gebruik van verbindingsencryptie en hashing algoritmen die voldoen aan de eisen van de tijd en voldoen aan de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS)[1],	Beleidsregels Meldplicht Datalekken, H7.2.3 HR

[1] https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

	dan wel logische opvolgers daarvan, en daarin minimaal als 'voldoende' zijn geclassificeerd.	
4.6	De leverancier gebruikt hardware oplossingen (zoals smart cards en Hardware Security Module producten) die zijn gecertificeerd volgens daartoe strekkende standaards.	
4.7	De leverancier verwijdert data van af te danken apparatuur en verwijderbare media middels een secure erase alvorens af te voeren.	ISO 27002:2013 §11.2.7
4.8 HOOG	Authenticatie van gebruikers op basis van cryptografische techniek, hardware tokens of challenge/response protocollen (sterke authenticatie) vindt in ieder geval plaats in de volgende situaties: • wanneer Single Sign-On wordt toegepast; • bij toegang vanuit een onvertrouwd netwerk; bij beheer van kritische beveiligingsvoorzieningen (zoals firewalls, Intrusion Detection and Prevention Systems en routers).	ISO 27002:2013 §10.1.1
4.9 HOOG	De leverancier stemt de geldigheidstermijn van cryptografische sleutels en certificaten af op het kritische gehalte van de toepassing met een maximum van 1 jaar.	ISO 27002:2013 §10.1.2
4.10	De cryptografische beveiligingsvoorzieningen moeten minimaal een score van 'A' behalen in de SSL Labs server test en de leverancier draagt er zorg voor dat de dienstverlening hieraan blijft voldoen.	HR

5. Controle en logging

Logging en het bijhouden van gebruikersactiviteit is essentieel bij het voorkomen, detecteren of minimaliseren van de impact van een inbreuk.

#	Maatregel	Referentie
	Controle en logging	
5.1	De leverancier legt activiteiten die gebruikers uitvoeren op (persoons) gegevens vast in logbestanden en registreert goedgekeurde en geweigerde pogingen om toegang te verkrijgen tot bronnen van informatie.	ISO 27002:2013 §12.4.1
5.2	De leverancier beschermt logfaciliteiten en informatie in logbestanden tegen vervalsing en onbevoegde toegang.	ISO 27002:2013 §12.4.2 AVG, art. 5.1 (e)
5.3	De leverancier legt activiteiten van systeembeheerders en -operators vast en beoordeelt ze regelmatig.	ISO 27002:2013 §12.4.3
5.4	De leverancier gebruikt één referentietijdbron waarmee alle relevante informatie verwerkende systemen worden gesynchroniseerd, zodat de nauwkeurigheid van logbestanden gewaarborgd is.	ISO 27002:2013 §12.4.4
5.5	De leverancier levert aan de opdrachtgever maandelijks een rapportage waarin ten minste zijn opgenomen: • aantallen geslaagde en mislukte inlogpogingen; • data en tijden van niet succesvolle inlogpogingen; • gevraagde en verleende toegang tot gedeelde bestanden/informatie buiten de regulieren gebruikstijden; • activiteiten van beheerders; • significante gebruikershandelingen (zoals mutaties aan autorisaties, configuratieparameters en stamgegevens; afhankelijk van applicatie); gedetecteerde malware (wormen/virussen/spyware e.d.) en storingen in de dienstverlening.	ISO 27002:2013 §15.2.1
5.6	De leverancier bewaart alle informatie in de logbestanden tenminste 3 maanden en ten hoogste 12 maanden, tenzij wettelijke verplichtingen anders voorschrijven of de logbestanden nodig zijn voor onderzoek in het kader van een (vermoed) beveiligingsincident. Gedurende die periode kan deze informatie worden ingezien door de opdrachtgever.	AVG, art. 5.1 (e)