



**Hogeschool
Leiden**



Reglement omgang met ICT-voorzieningen en (persoons)gegevens door medewerkers Hogeschool Leiden

Dit reglement is op 27 mei 2024 met instemming van de Ondernemingsraad vastgesteld door het College van Bestuur van Hogeschool Leiden.



Inhoud

Toelichting	3
Hoofdstuk 1 Algemene bepalingen	4
Artikel 1. Begrippen	4
Artikel 2. Reikwijdte	5
Artikel 3. Doeleinden	5
Artikel 4. Rechten van medewerkers.....	5
Hoofdstuk 2 Gebruiks- en gedragsregels voor medewerkers.....	6
Artikel 5. Informatie en (Persoons)gegevens	6
Artikel 6. E-mail en andere ICT-communicatiemiddelen	6
Artikel 7. ICT-middelen, applicaties en account	7
Artikel 8. Internet	8
Artikel 9. Afwijkingen	8
Hoofdstuk 3 ICT-beheersmaatregelen en controle.....	9
Artikel 10. Algemene bepalingen.....	9
Artikel 11. Registreren van ICT-, e-mail- en internetgebruik (logging)	9
Artikel 12. Controleren van ICT-, e-mail- en internetgebruik (monitoring)	9
Artikel 13. Gericht onderzoek naar aanleiding van overtreding van dit reglement.....	9
Artikel 14. Maatregelen in geval van andere bijzondere situaties	10
Hoofdstuk 4 Overtreding van dit reglement	12
Artikel 15. Consequenties van overtreding.....	12
Hoofdstuk 5 Slotbepaling	13
Artikel 16. Slotbepalingen.....	13

Toelichting

Het verwerken van (persoons)gegevens en het gebruik van ICT-voorzieningen (zoals laptop, smartphone, applicaties, systemen, e-mail en internet) is voor de medewerkers binnen Hogeschool Leiden noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn echter veiligheidsrisico's verbonden die nopen tot het stellen van gedragsregels. Tegen de achtergrond van deze risico's mag van de medewerkers verantwoord gebruik van (persoons)gegevens en ICT-voorzieningen worden verwacht..

Met dit reglement wil Hogeschool Leiden, hierna te noemen "de hogeschool", regels stellen omtrent het aanvaardbaar en gewenst gebruik van ICT-voorzieningen en het gebruik van (persoons)gegevens. Het streven daarbij is een goede balans aan te brengen tussen verantwoord, veilig en werkbaar gebruik van ICT-voorzieningen en (persoons)gegevens en de privacy en veiligheid van de medewerkers en studenten.

Hogeschoolmedewerkers en studenten communiceren ook met elkaar en met derden via sociale media en andere (openbare) communicatiekanalen waarover de hogeschool geen controle heeft. De gedragsregels in dit reglement op het gebied van de beschikbaarheid (continuïteit), de integriteit (betrouwbaarheid) en de vertrouwelijkheid (exclusiviteit) van gegevens gelden ook voor die kanalen voor zover de gegevens betrekking hebben op de hogeschool of op de (persoons)gegevens die onder de verantwoordelijkheid vallen van de hogeschool.

Om (persoons)gegevens en ICT-voorzieningen te kunnen beheren, optimaliseren en beveiligen is inzicht nodig in het gebruik van ICT-voorzieningen. Het registreren van activiteiten van gebruikers (logging) en het periodiek beoordelen van deze logging (monitoring) is daarbij een essentieel onderdeel. Bij dreigingen die de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens of systemen beïnvloeden of het vermoeden van activiteiten van cybercriminelen kunnen gelogde (persoons)gegevens gebruikt worden om de dreiging te onderzoeken en te verhelpen.

Bij zwaarwegende vermoedens van overtreding van dit reglement kunnen gelogde (persoons)gegevens gebruikt worden bij een onderzoek dat is gericht op een specifiek persoon. Medewerkers dienen hierover goed geïnformeerd te worden. In dit reglement is daarom tevens beschreven op welke wijze en volgens welke procedures het verzamelen van gegevens van medewerkers, de controle op naleving en gericht onderzoek plaatsvindt.

Naast de wet- en regelgeving is dit document gebaseerd op het Informatiebeveiligingsbeleid, het Privacy beleid, de Huisregels, Richtlijnen classificatie gegevens en applicaties en de Regeling klachtenprocedure ongewenst gedrag. Bovenstaande beleidsstukken, regelingen en richtlijnen zijn te raadplegen via de website van de hogeschool en/of de interne website [veilig online werken](#).

Bronvermelding:

Deze gedragscode voor medewerkers van Hogeschool Leiden is gebaseerd op het Model reglement voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo.

Hoofdstuk 1 Algemene bepalingen

Artikel 1. Begrippen

- **Account:** identificatie van een medewerker die hem toegang verleent tot een bepaalde applicatie, omgeving of netwerk. Bij een account hoort minimaal een gebruikersnaam en een wachtwoord.
- **Applicatie:** computerprogramma of software, al dan niet aangeboden als clouddienst.
- **Artificial intelligence (AI):** een verzamelnaam voor systemen, applicaties en software die taken kunnen doen waar eerder menselijke intelligentie voor nodig was. AI-systemen kunnen bijvoorbeeld (zelfstandig) leren, problemen oplossen of voorspellingen doen.
- **Beheerorganisatie:** is de term voor de functionarissen die bevoegd zijn ICT-voorzieningen te beheren en logging, monitoring en eventueel tracking uit te voeren. In de praktijk zal dit per implementatie verschillen en o.a. belegd zijn bij functioneel beheer, technisch beheer of een specifiek aangewezen functionaris binnen een faculteit of dienst. Aan de hand van de richtlijn die het toegangsbeleid beschrijft, is vastgesteld wie per applicatie geautoriseerd is.
- **Bronstelsel:** een aangewezen ICT-voorziening die als bron dient voor het registreren en verwerken van specifieke gegevens, die uitgewisseld worden met doelsystemen via een al dan niet geautomatiseerde koppeling.
- **(Primaire) bedrijfsprocessen:** de activiteiten van de hogeschool op het gebied van onderwijs en onderzoek.
- **Crisis:** een situatie waarin (a) de veiligheid, gezondheid en/of het welzijn van studenten, medewerkers en/of bezoekers van Hogeschool Leiden geschaad wordt, of (b) gebouwen, infrastructuur of belangen van Hogeschool Leiden worden aangetast, of (c) er verstoring van de primaire bedrijfsprocessen ontstaat, of (d) strategische belangen van de organisatie worden aangetast. In dergelijke gevallen voldoen de bestaande normale hiërarchische besluitvormingsstructuur, procedures en protocollen niet voor het beheersen en bestrijden van de situatie.
- **Datalek:** een inbreuk in verband met persoonsgegevens die een risico inhoudt voor de rechten en vrijheden van degene wiens persoonsgegevens het betreft, zoals bedoeld in artikel 4 lid 12 Algemene Verordening Gegevensbescherming.
- **Diagnostische gegevens:** geregistreerde gegevens van activiteiten van gebruikers en systemen en van gebeurtenissen in ICT-voorzieningen.
- **Doelstelsel:** een applicatie of systeem die data ontvangt van andere systemen.
- **ICT-communicatiemiddel:** alle middelen die de hogeschool beschikbaar stelt waarmee berichten kunnen worden verstuurd naar ontvangers binnen en buiten de hogeschool.
- **ICT-middel:** hardware, zoals computer, laptop, smartphone en netwerkfaciliteiten.
- **ICT-voorziening:** ICT-middelen, applicaties, (informatie)systemen en ICT-communicatiemiddelen.
- **(Informatie)stelsel:** een (informatie)stelsel is een systeem waarmee informatie over objecten of personen beheerd - verzameld, bewerkt, geanalyseerd, geïntegreerd en gepresenteerd - kan worden.
- **Logging:** het registreren van activiteiten of gebeurtenissen van gebruikers en systemen die plaats vinden in ICT-voorzieningen om het vervolg op te slaan.
- **Monitoring:** het periodiek controleren en beoordelen van de diagnostische gegevens en logging op de aanwezigheid van ongewenste gebeurtenissen en ongebruikelijke situaties zoals overtredingen van hogeschool beleid of dreigingen die de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens of ICT-voorzieningen beïnvloeden.
- **Persoonsgegevens:** informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals bedoeld in artikel 4 lid 1 van de Algemene Verordening Gegevensbescherming.
- **Sociale media:** online platformen waarbij gebruikers, al dan niet met tussenkomst van een redactie, tekst en/of (audiovisueel) beeld publiceren, kennis, meningen en ervaringen uitwisselen en de dialoog met elkaar aangaan.
- **Vertrouwelijke informatie:** informatie waarvan de medewerker de vertrouwelijkheid kent of behoort te kennen. Vertrouwelijkheid is een kwaliteitskenmerk van gegevens en staat voor de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn. Voor de classificatie van vertrouwelijkheid zie [Classificatie van gegevens](#).

Artikel 2. Reikwijdte

- 2.1 Dit reglement stelt regels ten aanzien van verwerking van (persoons)gegevens en het gebruik van ICT-voorzieningen door medewerkers van Hogeschool Leiden.
- 2.2 Dit reglement informeert op welke wijze en volgens welke procedures geautomatiseerde verzameling van gegevens, de controle op naleving van dit reglement en gericht onderzoek naar individuele medewerkers plaatsvindt.
- 2.3 Tot medewerkers van Hogeschool Leiden worden in het kader van dit reglement gerekend:
 - medewerkers met een arbeidsovereenkomst;
 - personen die arbeid verrichten voor de hogeschool (in het kader van een opdracht);
 - uitzendkrachten;
 - gedetacheerden;
 - stagiaires;
 - personen die arbeid verrichten voor een organisatie die volgens een overeenkomst gebruik maakt van faciliteiten en/of (persoons)gegevens van de hogeschool;
 - overige personen die toegang hebben tot de ICT-voorzieningen en/of (persoons)gegevens van de hogeschool (niet zijnde studenten).

Artikel 3. Doeleinden

Met dit reglement worden de volgende doeleinden beoogd:

- beveiliging van ICT-voorzieningen, inclusief beveiliging tegen schade en misbruik;
- voorkomen dat de ICT-voorzieningen worden misbruikt voor seksuele intimidatie, discriminatie en ander wettelijk verboden en daarmee ongewenst gedrag;
- bescherming van de (persoons)gegevens van onze medewerkers, studenten en derden;
- bescherming van informatie van de hogeschool, haar medewerkers, studenten en derden;
- bescherming van de intellectuele eigendomsrechten van de hogeschool en derden;
- voorkomen van het al dan niet moedwillig verspreiden van foutieve en/of niet-actuele gegevens en informatie;
- beheersing van beschikbaarheid, capaciteit en kosten van de ICT-voorzieningen van de hogeschool;
- bescherming van informatie en (persoons)gegevens en ICT-voorzieningen tegen kwaadwillenden.

Artikel 4. Rechten van medewerkers

- 4.1 Informatie over de rechten van medewerkers met betrekking tot de verwerking van hun persoonsgegevens door de hogeschool is te vinden in het Privacy Statement Medewerkers, te raadplegen op de website van de hogeschool. Voor de volledigheid wordt hier ook verwezen naar de wet AVG.
- 4.2 Medewerkers kunnen ten aanzien van de verwerking van hun persoonsgegevens een verzoek indienen bij Loket Privacy (loket.privacy@hsleiden.nl) van de hogeschool. Verzoeken worden conform de procedure Behandeling verzoeken betreffende rechten van betrokkenen afgehandeld. Deze procedure is te raadplegen via Praktische Informatie.

Hoofdstuk 2 Gebruiks- en gedragsregels voor medewerkers

Artikel 5. Informatie en (Persoons)gegevens

- 5.1 De medewerker dient zich bewust te zijn van de classificatie van de informatie en (persoons)gegevens (laag, midden, hoog vertrouwelijk) waar hij in het kader van het werk toegang tot heeft. Deze (persoons)gegevens dienen te worden beschermd conform het niveau van de vertrouwelijkheid. De medewerker dient adequate maatregelen (zie ook artikel 5.4) te treffen om de gegevens te beschermen.
- 5.2 De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van de hogeschool en derden en conformeert zich aan de licentievoorwaarden die van toepassing zijn op de applicaties van de hogeschool.
- 5.3 De zeggenschap over informatie en (persoons)gegevens van de hogeschool berust bij de hogeschool. De medewerker heeft hierover geen zelfstandige zeggenschap behalve als hem dat expliciet is toegekend door de hogeschool, bijvoorbeeld in de arbeidsovereenkomst of in een akte van overdracht intellectuele eigendomsrechten.
- 5.4 De medewerker treft adequate maatregelen om een informatiebeveiligings- of privacy incident te voorkomen. Onder adequate maatregelen worden in ieder geval de volgende maatregelen verstaan:
 - a. Vertrouwelijke informatie en (persoons)gegevens worden alleen opgeslagen, bewaard en verwerkt in de ICT-voorzieningen van de hogeschool, die voor deze classificatie gegevens zijn bestemd. Een lijst met ICT-voorzieningen die beheerd worden door de hogeschool is te vinden op de [sharepoint-omgeving van de dienst IVT](#) en [online onderwijs](#).
 - b. De medewerker verwerkt geen vertrouwelijke informatie en (persoons)gegevens buiten de ICT-voorzieningen van de hogeschool. Het gebruik van ICT-voorzieningen voor vertrouwelijke informatie en (persoons)gegevens, wanneer deze niet onder beheer staan van de hogeschool, is niet toegestaan. Hieronder valt minimaal:
 - het gebruik van applicaties (ten tijde van het schrijven van deze richtlijnen zijn dit o.a. Google-drive, Tiktok, WeTransfer, Dropbox, Zoom, Kahoot);
 - het gebruik van AI toepassingen (ten tijde van het schrijven van deze richtlijnen zijn dit o.a. ChatGPT, Copilot, etc.);
 - het gebruik van externe opslagmedia of eigen apparatuur (USB-sticks, externe harddisks, tablets, etc.).
 - c. De medewerker past de set aan maatregelen voor de omgang met informatie en (persoons)gegevens toe. Deze set aan maatregelen wordt actueel gehouden op: [Veilig online werken](#). Voor rollen met specifieke verantwoordelijkheden (zoals beheerders, proceseigenaren en onderzoekers) gelden aanvullende maatregelen.
- 5.5 De medewerker leeft de voorschriften die de hogeschool met betrekking tot het beschermen van informatie en (persoons)gegevens heeft opgesteld, waaronder de regels in dit reglement, strikt na.

Artikel 6. E-mail en andere ICT-communicatiemiddelen

- 6.1 De hogeschool biedt medewerkers een account met toegang tot generieke ICT-communicatiemiddelen waaronder internettoegang, Office365 applicaties, een e-mailsysteem met bijbehorende mailbox en e-mailadres.
- 6.2 De hogeschool stelt ICT-communicatiemiddelen beschikbaar aan de medewerker voor gebruik in het kader van zijn functie. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. Beperkt privégebruik van ICT-communicatiemiddelen is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of voor het gebruikte communicatiemiddel van de hogeschool.
- 6.3 Verboden bij elk gebruik (privé of zakelijk) van ICT-communicatiemiddelen is echter:
 - het verzenden of plaatsen van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende, (seksueel) intimiderende of andere wettelijk verboden inhoud;
 - het versturen of plaatsen van ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven te versturen of kwaadaardige software zoals virussen, Trojaanse paarden of spyware te versturen.
- 6.4 De medewerker heeft als enige toegang tot zijn eigen hogeschool-mailbox. De enige uitzondering

hierop staat in Hoofdstuk 3 van dit reglement omschreven.

- 6.5 Voor het delen van vertrouwelijke informatie en (persoons)gegevens (zowel intern als extern) gelden de volgende regels:
- a. De medewerker verstuurt geen e-mails (of bijlagen) met daarin vertrouwelijke informatie of (persoons)gegevens.
 - b. Als informatie of (persoons)gegevens gedeeld moeten worden, verwijst de medewerker naar de (bron)systemen waar de ontvanger de betreffende vertrouwelijke informatie of (persoons)gegevens zelf kan vinden. Hiermee wordt voorkomen dat onnodig kopieën van vertrouwelijke informatie of (persoons)gegevens in de organisatie terecht komen en bewaard blijven.
 - c. Indien het verwijzen naar een (bron)systeem niet mogelijk is, dan kiest de medewerker voor een beveiligde manier van uitwisseling, zoals SURFfilesender.
 - d. De medewerker controleert altijd de link van een gedeeld bestand en het e-mailadres van de geadresseerde voor het versturen van de e-mail. Hiermee wordt voorkomen dat -per abuis- de verkeerde informatie met de verkeerde persoon wordt gedeeld.
 - e. De medewerker gebruikt bcc (blind carbon copy=verborgen adressen) als een groep aangeschreven wordt van externe personen die elkaars gegevens mogelijkwijs niet hebben of niet nodig hebben.
 - f. Als de medewerker e-mails ontvangt met vertrouwelijke informatie of (persoons)gegevens, dan verwijdert de medewerker de mail zo snel mogelijk.
 - g. De medewerker gebruikt de e-mailapplicatie niet om vertrouwelijke informatie of (persoons)gegevens te bewaren en verwijdert daarom regelmatig de betreffende e-mails.
 - h. Het delen van vertrouwelijke informatie en (persoons)gegevens in AI toepassingen is niet toegestaan.

Artikel 7. ICT-middelen, applicaties en account

- 7.1 Computer-, smartphone- en netwerkfaciliteiten (ICT-middelen) worden aan medewerkers voor gebruik in het kader van hun functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. Medewerkers dienen te allen tijde zorgvuldig om te gaan met de verstrekte ICT-voorzieningen.
- 7.2 Het aansluiten van eigen apparatuur zoals, laptops, tablets en telefoons op het netwerk is alleen toegestaan op de daarvoor beschikbaar gestelde netwerkaansluitingen. De Beheerorganisatie kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging . Ook het aansluiten van servers en netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van de Beheerorganisatie. Neem hiervoor altijd contact op met de Servicedesk.
- 7.3 Het opslaan van privébestanden of -informatie op de persoonlijke opslaglocatie van de hogeschool is toegestaan, mits dit niet leidt tot overbelasting van de ICT-voorzieningen of de goede orde op de werkvloer verstoort. Bovendien mag de inhoud van de bestanden en informatie niet in strijd zijn met wet- en regelgeving.
- De hogeschool is niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen. Het gebruiken van de persoonlijke opslaglocatie van de hogeschool voor privédoeleinden geschiedt dan ook op eigen risico.
- 7.4 De hogeschool kan voor bedrijfsprocessen, bedrijfsvoering, gegevensverwerkingen specifieke ICT-voorzieningen voorschrijven, zoals een Elektronische leer/werk omgeving, een e-mailsysteem, (mobiele) applicaties, apps, cloud-voorzieningen of multimediasdiensten. De medewerker zal voor het opslaan, bewaren en verwerken van informatie en (persoons)gegevens, alleen de daarvoor voorgeschreven ICT-voorzieningen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.
- 7.5 Het zelfstandig installeren van software op ICT-voorzieningen van de hogeschool is niet toegestaan als de Beheerorganisatie beperkingen heeft ingesteld die installatie tegenhouden.
- 7.6 Het omzeilen van beveiligingsmaatregelen op ICT-voorzieningen van de hogeschool is niet toegestaan.

- 7.7 De medewerker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende hogeschoolaccount, inloggegevens en eventuele aanvullende authenticatiemiddelen. Wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld of hergebruikt.
- 7.8 De medewerker gebruikt de aan hem uitgeleverde ICT-middelen uitsluitend zelf. Het is niet toegestaan om ICT-middelen in bruikleen aan een ander (collega's en familieleden daaronder begrepen) te geven.
- 7.9 In geval van schade, verlies of diefstal van een ICT-middel brengt de medewerker de hogeschool onmiddellijk op de hoogte door een melding te maken bij de Servicedesk. De medewerker voert zelf geen of laat geen reparaties en/of onderhoudswerkzaamheden uitvoeren. In geval van diefstal doet de medewerker aangifte bij de politie.
- 7.10 Het gebruik van ICT-voorzieningen door de medewerker ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan indien en voor zover de direct leidinggevende van de medewerker hiervoor schriftelijk toestemming heeft verleend.

Artikel 8. Internet

- 8.1 De toegang tot internet en bijbehorende faciliteiten worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. Beperkt privégebruik van internet is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of het netwerk van de hogeschool.
- 8.2 Verboden bij elk internetgebruik (privé of zakelijk) is echter:
- sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
 - filesharing- of streamingdiensten te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de ICT-voorzieningen in gevaar kan brengen;
 - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de medewerker daadwerkelijk weet dat dit in strijd met auteursrechten is;
 - films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

Artikel 9. Afwijkingen

Indien een afwijking van de artikelen uit hoofdstuk 2 noodzakelijk is voor een goede uitvoering van de bedrijfsprocessen, kan een uitzondering gemaakt worden, door de verantwoordelijke directeur, onder de volgende voorwaarden:

- In opdracht van de verantwoordelijke directeur wordt een gedegen inventarisatie en risicoanalyse uitgevoerd op de impact van de gewenste afwijking;
- De CIO Office van de dienst IVT wordt geraadpleegd om een multidisciplinair advies uit te brengen. Dit advies bevat een risico-impactanalyse van de voorgestelde afwijking, waarbij de impact op de beveiliging van de betrokken (persoons) gegevens en ICT-voorzieningen in kaart wordt gebracht. Tevens worden de (technische) beheer mogelijkheden onderzocht en wordt de afwijking getoetst op geldende wetgeving en beleidskaders. Indien relevant worden adequate maatregelen aangedragen ter verlaging van het risico en ter borging van de beveiliging van de (persoons) gegevens.
- De verantwoordelijke directeur draagt zorg voor een aantoonbare implementatie van de aangedragen maatregelen.
- De verantwoordelijke directeur accepteert aantoonbaar de eventuele restrisico's van de afwijking en geeft de betreffende medewerker(s) schriftelijk akkoord om de afwijking toe te mogen passen.
- Afwijkingen (inclusief risicobeoordeling en acceptatie) worden geregistreerd en jaarlijks geëvalueerd door het College van Bestuur als onderdeel van het hogeschool brede risicomanagementproces.

Hoofdstuk 3 ICT-beheersmaatregelen en controle

Artikel 10. Algemene bepalingen

- 10.1 De Beheerorganisatie verschaft zich slechts toegang tot het account of de ICT-middelen van een medewerker, als de medewerker daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in uitzonderlijke gevallen en volgens de procedures zoals beschreven in dit hoofdstuk.
- 10.2 Het geautomatiseerd verzamelen van gegevens over, controle op en gericht onderzoek naar gebruik van de ICT-voorzieningen en internetgebruik vindt slechts plaats in het kader van handhaving van de regels uit dit reglement voor de doelen genoemd in artikel 3. Verboden of ongewenst gebruik wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Artikel 11. Registreren van ICT-, e-mail- en internetgebruik (logging)

- 11.1 Ten behoeve van goed en efficiënt beheer en bescherming van de ICT-voorzieningen van de hogeschool worden gegevens waar mogelijk geautomatiseerd verzameld (gelogd), te weten:
- datum, tijdstip
 - gebruikersnaam/identificatie
 - werkstation/locatie informatie
 - activiteit/gebeurtenis
 - het object waarop de activiteit werd uitgevoerd
 - indien relevant, het resultaat van de activiteit
- 11.2 Deze gelogde gegevens zijn toegankelijk voor de Beheerorganisatie. De gelogde gegevens worden alleen aan andere functionarissen beschikbaar gesteld op basis van de richtlijn die het toegangsbeleid bepaalt.
- 11.3 De gelogde gegevens worden maximaal één jaar bewaard, met uitzondering van:
- Loggegevens die betrokken zijn bij (beveiligings)incidenten. Deze gelogde gegevens worden één jaar na het afhandelen van het incident bewaard om eventuele controlerende of corrigerende analyses te kunnen doen.
 - Loggegevens over inlogpogingen. Deze gegevens worden maximaal twee jaar bewaard, om op basis van inlogpogingen de oorsprong van incidenten te kunnen onderzoeken (forensisch onderzoek).

Na de vastgestelde bewaartermijn worden gelogde gegevens verwijderd.

Artikel 12. Controleren van ICT-, e-mail- en internetgebruik (monitoring)

- 12.1 Met monitoring wordt bedoeld het periodiek controleren en beoordelen van de diagnostische gegevens op de aanwezigheid van ongewenste gebeurtenissen en ongebruikelijke situaties zoals overtredingen van hogeschoolbeleid of dreigingen die de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens of ICT-voorzieningen beïnvloeden. De uitkomst van de beoordeling wordt omgezet in een signalering voor de Beheerorganisatie en mogelijk in rapportage aan relevante functionarissen.
- 12.2 Naar aanleiding van een signalering kan de Beheerorganisatie maatregelen op de ICT-voorzieningen nemen om de dreigingen weg te nemen.
- 12.3 Bij een vermoeden van misbruik van een wachtwoord, account en/of inloggegevens mag de hogeschool per direct het betrokken account ontoegankelijk maken.
- 12.4 Op basis van de uitkomsten van de monitoring kan een (gericht) onderzoek worden gestart. Dit onderzoek kan gericht zijn op de naleving van de regels van dit reglement als bedoeld in artikel 13, of in het kader van onderzoek naar een potentieel beveiligingsincident als bedoeld in artikel 14.

Artikel 13. Gericht onderzoek naar aanleiding van overtreding van dit reglement

- 13.1 Van gericht onderzoek is sprake wanneer diagnostische gegevens of persoonsgegevens betreffende een medewerker worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die medewerker.

- 13.2 Gericht onderzoek door de Beheerorganisatie vindt uitsluitend plaats na schriftelijke opdracht van de faculteits- of dienstdirecteur onder wiens verantwoordelijkheid de medewerker valt. Het College van Bestuur ontvangt een afschrift van deze opdracht en de schriftelijke resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen worden de opdracht en de resultaten direct vernietigd door de Beheerorganisatie.
- 13.3 Gericht onderzoek beperkt zich in eerste instantie tot diagnostische gegevens over het gebruik van ICT-voorzieningen. Als gericht onderzoek nader bewijs van overtreding van dit reglement oplevert, kan de Beheerorganisatie met toestemming van de opdrachtgevende directeur zoals bedoeld in 13.2 en het College van Bestuur overgaan tot het kennisnemen van de inhoud van berichten of opgeslagen bestanden indien dit noodzakelijk is voor het onderzoek. De hogeschool beperkt zich in een dergelijke situatie tot het inzien en lezen van de zakelijke e-mailberichten en bestanden. Alleen gegevens die duidelijk gemarkeerd zijn als privé zullen door de hogeschool als zodanig behandeld worden.
- 13.4 De medewerker wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur van zijn dienst of faculteit over de aanleiding, de uitvoering en het resultaat van het onderzoek. De medewerker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens (hoor en wederhoor). Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zal schaden.
- 13.5 Voor gericht onderzoek wordt uitgegaan van een meer-ogen principe bij het uitvoeren van het onderzoek. Hierbij zijn dus altijd meerdere personen betrokken.

Artikel 14. Maatregelen in geval van andere bijzondere situaties

- 14.1 Naast de in dit hoofdstuk genoemde maatregelen met betrekking tot beheer, controle en gericht onderzoek, verschaft de Beheerorganisatie zich alleen in de volgende bijzondere situaties en volgens de in dit artikel beschreven procedures toegang tot het account of de ICT-middelen van een medewerker.
- 14.2 In het geval van diefstal of verlies van ICT-middelen van een medewerker kan de beheerorganisatie na melding van de diefstal of het verlies bij de servicedesk de locatie vaststellen met behulp van digitale locatiegegevens.
- Indien het ICT-middel binnen de hogeschool wordt getraceerd, wordt dit in geval van diefstal direct door de Beheerorganisatie gemeld aan de directeur van het Facilitair Bedrijf. De conciërges kunnen vervolgens in overleg met de politie besluiten om over te gaan tot aanhouding van de verdachte(n).
- 14.3 In het geval van langdurige ziekte of onverwachte (blijvende) afwezigheid van een medewerker kan worden besloten dat aan de direct leidinggevende van de betreffende medewerker toegang wordt verschaft tot het account (zoals de e-mails en bestanden) van de medewerker, indien dit noodzakelijk is voor waarborging van de continuïteit en kwaliteit van de bedrijfsprocessen van de hogeschool.
- De hogeschool beperkt zich in een dergelijke situatie tot het inzien en lezen van de zakelijke e-mailberichten en bestanden.
- Een besluit tot het inzien en lezen van zakelijke e-mailberichten en bestanden wordt genomen door de faculteits- of dienstdirecteur onder wiens verantwoordelijkheid de medewerker valt, op verzoek van de manager van de medewerker. De directeur neemt dit besluit pas na zorgvuldige afweging van ieders belangen en inachtneming van eventuele minder verstrekkende maatregelen en – voor zover mogelijk – in overleg met de betreffende medewerker.
- Indien de medewerker wiens hogeschool-account het betreft een directeur is, wordt het besluit door het College van Bestuur genomen.
- Indien de medewerker wiens hogeschool-account het betreft lid van het College van Bestuur is, wordt het besluit genomen door een lid van de Raad van Toezicht.
- 14.4 In geval van een potentieel beveiligingsincident, kan het College van Bestuur of de crisisorganisatie toestemming verlenen aan de beheerorganisatie om zich toegang te verschaffen tot het account (zoals e-mails en bestanden) van een of meerdere medewerkers, indien dit noodzakelijk is voor waarborging van de continuïteit, beveiliging en kwaliteit van de (persoons)gegevens en/of primaire

bedrijfsprocessen van de hogeschool.

- 14.5 De medewerker wordt zo spoedig mogelijk schriftelijk geïnformeerd over de maatregelen die zijn of worden genomen op basis van dit hoofdstuk.
- 14.6 In bijzondere situaties zoals bedoeld in artikel 14.3 en 14.4, worden maatregelen genomen, die tot gevolg kunnen hebben dat gegevens en bestanden worden gelezen door anderen dan de betreffende medewerker. In deze gevallen wordt altijd een inijkprocedure gevolgd. Deze inijkprocedure gaat uit van het vierogen-principe en verloopt in hoofdlijnen als volgt:
- a) De verantwoordelijke functionaris (zoals vastgesteld in 14.3 en 14.4) verzoekt de directeur IVT om toegang te verschaffen tot de gevraagde gegevens.
 - b) Een inzageverzoek bevat een zorgvuldige afweging van ieders belangen met inachtneming van eventuele minder verstrekkende maatregelen en benoemt aan wie de toegang moet worden verschaft, inclusief de borging van het vierogen-principe en een communicatieplan richting de betrokken medewerkers.
 - d) Indien een inzageverzoek naar aanleiding van overtreding van dit reglement gegevens betreft van een medewerker van de dienst IVT, dan verzoekt de directeur IVT een mededirecteur om mee te kijken om daarmee het vierogen-principe te waarborgen. Indien de indiener van het inzageverzoek en de directeur IVT het niet eens kunnen worden over de uitvoering van het inzageverzoek, beslist het CvB.
 - e) De directeur IVT geeft een opdracht aan de beheerder(s) die het inzageverzoek afhandelen.

Hoofdstuk 4 Overtreding van dit reglement

Artikel 15. Consequenties van overtreding

Wanneer handelen in strijd met dit reglement of de algemeen geldende wettelijke regels wordt geconstateerd, kan het College van Bestuur en/of de verantwoordelijk directeur afhankelijk van de aard en de ernst van de overtreding (arbeidsrechtelijke) maatregelen treffen.

Hoofdstuk 5 Slotbepaling

Artikel 16. Slotbepalingen

- 16.1 Dit reglement wordt iedere twee jaar onder leiding van de dienst IVT geëvalueerd en waar nodig herzien.
- 16.2 Dit reglement kan met instemming van de Ondernemingsraad tussentijds worden gewijzigd als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de werknemers bekend gemaakt.
- 16.3 In gevallen waarin dit reglement niet voorziet, beslist het College van Bestuur.

