REGLEMENT ICT-VOORZIENINGEN VOOR MEDEWERKERS VRIJE UNIVERSITEIT AMSTERDAM

Versie 1.4

IS VERDER KIJKEN

Reglement ICT-voorzieningen voor medewerkers Vrije Universiteit Amsterdam

Inhoudsopgave

HOOFDSTUK 1. INLEIDING

De Vrije Universiteit Amsterdam (hierna: **VU**) geeft medewerkers toegang tot haar ICT-voorzieningen zoals computers, internet, e-mail en andere applicaties. Het is van groot belang dat de ICT-voorzieningen op veilige en verantwoorde wijze worden gebruikt door medewerkers.

In dit 'Reglement ICT-voorzieningen voor medewerkers Vrije Universiteit Amsterdam' (hierna: **Reglement**) wordt beschreven welke gedragsregels gelden voor het gebruik van ICT-voorzieningen door medewerkers. Daarmee wil de VU duidelijk maken wat zij onder veilig en verantwoord gebruik verstaat en welk gedrag van medewerkers wordt verwacht. Het doel hiervan is:

- het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-Voorzieningen[1];
- het beheersbaar houden van kosten voor de VU; en
- ervoor zorgen dat de rechten en reputatie van de VU en anderen niet worden geschonden.

Daarnaast wordt in dit Reglement uiteengezet hoe de VU toezicht houdt op haar ICT-voorzieningen. De VU zorgt hierbij voor een goede verhouding tussen het bereiken van de hiervoor genoemde doelen enerzijds en het recht op eerbiediging van de persoonlijke levenssfeer van haar medewerkers anderzijds.

Logging en monitoring spelen een belangrijke rol in het toezicht op de ICT-voorzieningen. Logging en monitoring vinden geautomatiseerd plaats en zijn in principe niet gericht op individuele medewerkers. Onderzoek naar individuele medewerkers is alleen mogelijk wanneer een gerechtvaardigd vermoeden bestaat voor overtreding van de gedragsregels of een ernstig verwijtbare andere gedraging. Uitgangspunt bij gericht onderzoek is dat alleen wordt gekeken naar verkeersgegevens (ook wel 'metadata' genoemd) en niet naar inhoud van bestanden of berichten. Alleen bij zwaarwegende redenen en wanneer dit noodzakelijk is, is het mogelijk dat inhoudelijke gegevens van individuele medewerkers worden onderzocht. De voorwaarden waaronder gericht en inhoudelijk onderzoek mogelijk zijn, worden in dit Reglement uiteengezet. Daarnaast wordt beschreven voor welke andere doeleinden verkeersgegevens worden gebruikt.

Tot slot wordt vermeld hoe het toezicht op de naleving van dit Reglement is geregeld en welke slotbepalingen gelden.

HOOFDSTUK 2. ALGEMENE BEPALINGEN

Artikel 1. Begrippen

a. **Acceptabel gebruik**: gebruik van de ICT-voorzieningen waarbij de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-voorzieningen is gewaarborgd, de kosten beheersbaar zijn en de rechten en reputatie van de VU en derden niet worden geschonden.
b. **Bevoegde functionaris**: een Medewerker die vanuit zijn functie door de VU is geautoriseerd om toegang te hebben tot (bepaalde) gegevens die worden verzameld door middel van Logging en/of Monitoring.
c. **College van Bestuur**: het College van Bestuur van de VU.
d. **Datalek**: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot

[1] Deze begrippen komen uit de informatiebeveiliging en houden in dat systemen en de informatie die daarop staat toegankelijk zijn (beschikbaar), betrouwbaar zijn (integriteit) en alleen te raadplegen zijn door de juiste personen (vertrouwelijk).

doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens, zoals bedoeld in artikel 4.12 van de Algemene Verordening Gegevensbescherming (AVG).

e. **Functionaris voor Gegevensbescherming (FG)**: een interne functionaris zoals bedoeld in artikel 37 e.v. van de Algemene Verordening Gegevensbescherming (AVG). De FG houdt op onafhankelijke wijze toezicht op de naleving van wet- en regelgeving met betrekking tot gegevensbescherming en het beleid van de VU met betrekking tot de bescherming van persoonsgegevens.
f. **Gedragscode**: de regels zoals opgenomen in hoofdstuk 3 van dit Reglement.
g. **Gericht Onderzoek**: onderzoek naar een individuele Medewerker of groep van Medewerkers waarbij gebruik wordt gemaakt van de Verkeersgegevens die de Medewerker(s) betreffen.
h. **ICT-voorzieningen**: alle voorzieningen die de VU gebruikt en ter beschikking stelt in het kader van haar informatie- en communicatieprocessen. Deze voorzieningen kunnen rechtstreeks door de VU of via derden met wie de VU een overeenkomst heeft ter beschikking worden gesteld. Het gaat hierbij onder meer om: netwerken, internet, computers, programma's en applicaties, printers, kopieer- en scanapparatuur, informatiedragers, opslagruimte, e-mail, (mobiele) telefoons en andere communicatiemiddelen.
i. **Inhoudelijk Onderzoek**: onderzoek naar een individuele Medewerker of groep van Medewerkers waarbij niet alleen gebruik wordt gemaakt van de Verkeersgegevens die de Medewerker(s) betreffen, maar waarbij ook naar de inhoud van bestanden of berichten van individuele Medewerker(s) wordt gekeken.
j. **Logging**: geautomatiseerde vastlegging van Verkeersgegevens.
k. **Medewerker**: degene die een dienstverband heeft met de VU, een persoon die werkzaam is onder het gezag en/of de verantwoordelijkheid van de VU zonder dienstverband (zoals een uitzendkracht, gedetacheerde, ZZP'er, stagiair(e), fellow, gastdocent en/of -onderzoeker) en andere personen die werkzaamheden verrichten ten behoeve van de VU en daarbij gebruikmaken van ICT-voorzieningen.
l. **Monitoring**: het geautomatiseerd verzamelen en analyseren van Verkeersgegevens. Monitoring vindt plaats op basis van algemene parameters en patronen en is niet gericht op individuele Medewerkers.
m. **Verkeersgegevens**: alle gegevens die samenhangen met of voortvloeien uit het gebruik van ICT-voorzieningen, die niet de inhoud van bestanden of berichten betreffen. Verkeersgegevens worden in de context van ICT-voorzieningen ook wel 'metadata' genoemd.

Artikel 2. Toepassingsbereik

2.1 Dit Reglement is van toepassing op elk gebruik van de ICT-voorzieningen door Medewerkers, ongeacht de aard van het gebruik (zakelijk of privé) en de wijze van gebruik.

2.2 Naast dit Reglement kan de VU bijzondere voorwaarden stellen aan het gebruik van (specifieke) ICT-voorzieningen door (bepaalde) Medewerkers (hierna: **Bijzondere Voorwaarden**).

Artikel 3. Doelstellingen

3.1 Het doel van dit Reglement is:
a. het bevorderen en handhaven van Acceptabel gebruik van ICT-voorzieningen door Medewerkers; en
b. het stellen van het normatief kader voor de omgang met gegevens die vastgelegd (kunnen) worden in het kader van het gebruik van ICT-voorzieningen.

HOOFDSTUK 3. GEDRAGSCODE

Artikel 4. Gedragsregels

4.1 Medewerkers maken zorgvuldig gebruik van de ICT-voorzieningen en handelen volgens de instructies die de VU hiervoor geeft.
4.2 Medewerkers houden zich bij het gebruik van de ICT-voorzieningen aan de geldende wet- en regelgeving, dit Reglement en eventuele Bijzondere Voorwaarden.
4.3 Medewerkers respecteren beveiligingsmaatregelen.
4.4 Medewerkers voorkomen onjuist of ongeoorloofd gebruik van ICT-voorzieningen en gedragen zich als een goed werknemer. Waar mogelijk zorgt de VU ervoor dat onjuist en ongeoorloofd gebruik technisch onmogelijk wordt gemaakt.
4.5 Medewerkers voorkomen dat de rechten en reputatie van de VU worden geschonden.
4.6 Medewerkers gaan zorgvuldig om met hun inloggegevens en verstrekken deze niet aan anderen.
4.7 Medewerkers bieden anderen geen toegang tot de ICT-voorzieningen[2] en lenen deze niet uit.
4.8 Medewerkers respecteren de intellectuele eigendomsrechten van de VU en die van derden.
4.9 Medewerkers behandelen vertrouwelijke informatie, waaronder persoonsgegevens waar zij in het kader van het werk toegang toe hebben, strikt vertrouwelijk.

Artikel 5. Ongeoorloofd gebruik

5.1 De volgende handelingen gelden in elk geval als ongeoorloofd gebruik van de ICT-voorzieningen:
a. het verstoren, beschadigen, hinderen, vertragen of anderszins op oneigenlijke wijze beïnvloeden van de beoogde beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-voorzieningen;
b. het bewust verspreiden of bevorderen van verspreiding van virussen, trojans, spyware, malware of andere schadelijke software;
c. het bewust verspreiden of bevorderen van verspreiding van (ongevraagde) berichten voor commerciële doeleinden;
d. het omzeilen van beveiligingsmaatregelen;
e. het bewust (proberen te) verkrijgen of verlenen van hogere privileges of toegangsrechten dan voor de uitvoering van de werkzaamheden noodzakelijk is;
f. een onjuiste hoedanigheid of identiteit aannemen;
g. het bewust ter beschikking hebben, stellen of kopiëren van auteursrechtelijk of door een ander intellectueel eigendomsrecht beschermd materiaal zonder toestemming van de rechthebbende(n), waaronder illegale, vervalste of gestolen exemplaren van software;
h. elk gebruik van de ICT-voorzieningen dat ertoe leidt dat anderen gediscrimineerd, (seksueel) geïntimideerd of bedreigd worden;
i. het bewust bezoeken van websites die pornografisch of racistisch dan wel anderszins discriminerend materiaal bevatten of het (laten) plaatsen van dit materiaal op of binnen de ICT-voorzieningen, tenzij dit noodzakelijk is in het kader van de functie-uitoefening van de Medewerker;
j. het bewust opslaan, verspreiden of anderszins verwerken van materiaal waarvan het bezit strafbaar is; en
k. het bewust (laten) lekken van persoonsgegevens of andere vertrouwelijke data van de VU.

[2] Uitgezonderd de situatie waarin het de taak van een Medewerker is om andere Medewerkers toegang te bieden tot ICT-voorzieningen.

Artikel 6. Zakelijk en privégebruik

6.1 De VU stelt haar ICT-voorzieningen aan Medewerkers beschikbaar voor de uitvoering van hun taken en werkzaamheden ten behoeve van de VU. De ICT-voorzieningen zijn daarmee primair bedoeld voor zakelijk gebruik.

6.2 Beperkt privégebruik van ICT-voorzieningen binnen de kaders zoals vastgelegd in dit Reglement is toegestaan, mits:
a. dit binnen de grenzen van redelijkheid gebeurt;
b. de uitvoering van de werkzaamheden van de Medewerker daardoor niet wordt gehinderd;
c. het gebruik van ICT-voorzieningen door of de werkzaamheden van andere Medewerkers daardoor niet wordt gehinderd;
d. dit geen onevenredige technische of financiële belasting vormt van de ICT-voorzieningen van de VU; en
e. dit niet gebeurt voor commerciële doeleinden.

6.3 Medewerkers zorgen ervoor dat bestanden en berichten die privé zijn, als 'privé' worden gemarkeerd.

6.4 Medewerkers zijn zich ervan bewust dat het noodzakelijk kan zijn voor de VU om een andere Medewerker toegang te geven tot hun persoonlijke opslagruimte of mailbox.[3] Bijvoorbeeld wanneer een Medewerker langdurig afwezig is of niet meer werkzaam is bij de VU. Bestanden en berichten die gemarkeerd zijn als 'privé', zoals bedoeld in artikel 6.3, worden hierbij buiten beschouwing gelaten. Ditzelfde geldt voor geprivilegieerde informatie zoals bedoeld in artikel 10.3 (e). Toegang tot de voor de werkoverdracht relevante gedeeltes van de persoonlijke opslagruimte of mailbox is uitsluitend mogelijk wanneer:
a. dit proportioneel is, gelet op het doel dat met de toegang wordt beoogd;
b. geen redelijk alternatief beschikbaar is;
c. dit niet in strijd is met een eventuele geheimhoudingsplicht of vertrouwelijkheidsverplichting van een Medewerker zoals bedoeld in artikel 10.3 (b), (c) of (d); en
d. hiervoor schriftelijke toestemming is verkregen van de directeur bedrijfsvoering van de Faculteit of de directeur van de Dienst waar de betreffende Medewerker werkzaam is. Indien de betreffende Medewerker decaan, directeur bedrijfsvoering of directeur van een Dienst is, dient hiervoor toestemming te worden verkregen van het College van Bestuur. Indien de betreffende Medewerker lid van het College van Bestuur is, dient hiervoor toestemming te worden verkregen van de Raad van Toezicht van de VU.

Artikel 7. Melding incidenten

7.1 Een Medewerker meldt een incident met betrekking tot de ICT-voorzieningen direct - zonder enige vertraging - bij de IT Servicedesk via servicedesk.it@vu.nl of 020-5980000.

7.2 Onder een incident wordt in elk geval verstaan (een vermoeden van):
a. verlies of diefstal van inloggegevens;
b. verlies of diefstal van ICT-voorzieningen, zoals een computer, telefoon of USB-stick;
c. ongeautoriseerde toegang tot ICT-voorzieningen;
d. ongeoorloofde of onopzettelijke vernietiging, openbaarmaking of wijziging van dan wel onbedoelde toegang tot persoonsgegevens of anderszins vertrouwelijke of gevoelige (bedrijfs- of onderzoeks)gegevens;
e. aanwezigheid van schadelijke software, zoals een virus, trojan, spyware, malware; of
f. een phishing-aanval.

[3] Medewerkers worden geacht om werkgerelateerde bestanden en berichten zoveel mogelijk op te slaan op voor (directe) collega's toegankelijke plekken, zoals de G-schijf. Op die manier is het overdragen van werk bij (langdurige) afwezigheid mogelijk zonder dat een collega toegang hoeft te hebben tot de persoonlijke opslagruimte of mailbox van de afwezige Medewerker.

HOOFDSTUK 4. LOGGING EN MONITORING

Artikel 8. Logging

8.1 Medewerkers moeten zich bij het gebruik van ICT-voorzieningen bewust zijn van het feit dat bepaalde gegevens, waaronder persoonsgegevens, vastgelegd kunnen worden. In sommige gevallen is dit een bewuste, gegronde keuze en in andere gevallen is dit een technisch-functionele noodzaak of onvermijdelijkheid.

8.2 De VU zal zich inspannen om zowel het aantal categorieën als de totale hoeveelheid van de gegevens die in het kader van het gebruik van ICT-voorzieningen worden verzameld, te minimaliseren. De verzamelde gegevens worden zoveel mogelijk geanonimiseerd c.q. gepseudonimiseerd.

8.3 De volgende gebeurtenissen worden in ieder geval gelogd[4]:

a. handelingen van Medewerkers, zoals inlogpogingen, systeemtoegang, e-mailgebruik, telefoongebruik, toegang tot bestanden en bezoek websites;
b. het gebruik van technische beheerfuncties, zoals het wijzigen van configuratie of instellingen, het uitvoeren van een systeemcommando, starten en stoppen van services, uitvoering van een back-up of restore;
c. gebruik van functies voor functioneel beheer, zoals het wijzigen van configuraties en instellingen, release van nieuwe functionaliteiten, ingrepen in gegevenssets (waaronder databases);
d. handelingen in beveiligingsbeheer, zoals het opvoeren en afvoeren van gebruikers, toekennen en intrekken van rechten en wachtwoordwijzigingen;
e. beveiligingsincidenten, zoals de aanwezigheid van malware, testen op (potentiële) zwakheden, inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet-operationele systeemservices, het starten en stoppen van beveiligingsbeheer; en
f. verstoringen in het dagelijks proces, zoals systeemfouten, afbreken tijdens het uitvoeren van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of -systemen.

8.4 De VU zorgt ervoor dat de gegevens die worden verzameld door middel van Logging goed zijn beschermd. Dit betekent in ieder geval dat:

a. de logfaciliteiten en informatie in logbestanden zijn beschermd tegen inbreuk en onbevoegde toegang;
b. het (automatisch) aanpassen, overschrijven en verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log; en
c. de logbestanden alleen kunnen worden geraadpleegd door Bevoegde functionarissen. De toegang is beperkt tot leesrechten.

Artikel 9. Monitoring

9.1 De VU past Monitoring uitsluitend toe indien dit strikt noodzakelijk is om één of meerdere gerechtvaardigde doelen te bereiken zoals vermeld in artikel 9.2. Indien alternatieven beschikbaar zijn met minder (privacy)risico's, zal de VU de voorkeur geven aan deze alternatieven of uitleggen waarom deze niet toegepast kunnen worden.

[4] De Verkeersgegevens die worden verzameld door middel van Logging worden alleen gebruikt voor de in artikel 14.2 vermelde doeleinden. De gegevens worden niet gebruikt om het individuele functioneren van (bepaalde groepen) Medewerkers te beoordelen, tenzij hiertoe een schriftelijk besluit is genomen door het College van Bestuur en de Ondernemingsraad hiermee heeft ingestemd. Zie artikel 14.3.

9.2 De VU past Monitoring uitsluitend toe voor de volgende doelen:
a. het voorkomen, signaleren en oplossen van capaciteits-, performance- of beschikbaarheids-problemen van de ICT-voorzieningen;
b. controle of de ICT-voorzieningen correct worden gebruikt, goed worden beheerd en naar behoren functioneren;
c. het voorkomen, signaleren en oplossen van beveiligingsincidenten, in het bijzonder een Datalek;
d. het creëren van 'bewijs' (audit trail) ter waarborging van de bedrijfsvoering, naleving van wet- en regelgeving en om intern en extern verantwoording af te kunnen leggen over het gebruik en de beveiliging van de ICT-voorzieningen. Denk bij dit laatste aan de accountantscontrole, externe of interne audits en de informatievoorziening voor toezichthouders zoals de Autoriteit Persoonsgegevens;
e. het verschaffen van managementinformatie met betrekking tot de beschikbaarheid, integriteit, vertrouwelijkheid en kosten van de ICT-voorzieningen;
f. het verbeteren van (de toegankelijkheid tot) de ICT-voorzieningen;
g. wetenschappelijke of statistische doeleinden, voor zover privacywetgeving dit toestaat; en
h. controle op naleving van dit Reglement.

9.3 Indien Monitoring noodzakelijk is en geen redelijke alternatieven beschikbaar zijn, is Monitoring uitsluitend mogelijk met inachtneming van de volgende voorwaarden:
a. de Monitoring vindt zoveel mogelijk systeembreed plaats op basis van algemene parameters en patronen. Er wordt in beginsel géén onderscheid gemaakt per individuele Medewerker; en
b. de Monitoring wordt zoveel mogelijk voorafgaand kenbaar gemaakt in het kader van de informatievoorziening rondom die specifieke ICT-voorziening, bijvoorbeeld via VUnet of via specifieke werkinstructies.

HOOFDSTUK 5. INDIVIDUEEL ONDERZOEK

Artikel 10. Gericht en inhoudelijk onderzoek

10.1 Bij onderzoek naar een individuele Medewerker is Gericht Onderzoek het uitgangspunt. Alleen wanneer duidelijk is dat Gericht Onderzoek ontoereikend is om de vermoede gedraging voldoende te kunnen onderzoeken, kan Inhoudelijk Onderzoek plaatsvinden.

10.2 Gericht onderzoek en Inhoudelijk Onderzoek zijn uitsluitend mogelijk wanneer voldaan wordt aan de volgende voorwaarden:
a. er is sprake van een gerechtvaardigd vermoeden van:
- overtreding van de Gedragscode;
- ongewenst gedrag zoals bedoeld in de regeling Ongewenst Gedrag van de VU; of
- een (andere) ernstig verwijtbare gedraging van een Medewerker;
b. het gericht onderzoek vindt plaats door twee Bevoegde functionarissen (vier-ogenprincipe) onder strikte geheimhouding;
c. een daartoe bevoegde persoon schriftelijk opdracht heeft gegeven tot het onderzoek. In de opdracht wordt vermeld wat het gerechtvaardigd vermoeden is zoals bedoeld in artikel 10.2 (a) en indien het Inhoudelijk onderzoek betreft waarom niet met Gericht onderzoek kan worden volstaan. De opdracht wordt gegeven door de directeur bedrijfsvoering van de Faculteit of de directeur van de Dienst waar de betreffende Medewerker werkzaam is, met dien verstande dat in de volgende gevallen alleen het College van Bestuur de opdracht mag geven:
- de betreffende Medewerker is een decaan, directeur bedrijfsvoering of directeur van een Dienst;
- de betreffende Medewerker heeft een geheimhoudingsplicht zoals bedoeld in artikel 10.3 (b) of (c) dan wel een vertrouwensfunctie zoals bedoeld in artikel 10.3 (d); of

- het onderzoek vindt plaats op verzoek van de klachtencommissie bedoeld in de regeling Ongewenst Gedrag;

Het College van Bestuur, of als het College zelf de opdrachtgever is de Raad van Toezicht, ontvangt gelijktijdig een afschrift van de betreffende opdracht. Indien de betreffende Medewerker lid is van het College van Bestuur, heeft de Raad van Toezicht van de VU de opdracht gegeven; en

d. de betreffende Medewerker wordt zo spoedig mogelijk geïnformeerd over de aanleiding, de uitvoering en de resultaten van het onderzoek en in de gelegenheid gesteld om nadere uitleg te geven. Het verstrekken van informatie aan de Medewerker kan worden uitgesteld indien het onderzoek daardoor zou kunnen worden geschaad. De opdrachtgever wordt van dit uitstel en de gronden ervoor op de hoogte gesteld.

10.3 Voor Inhoudelijk Onderzoek gelden de volgende aanvullende regels:

a. bestanden en berichten die als 'privé' zijn gemarkeerd worden buiten beschouwing gelaten, tenzij een gerechtvaardigd vermoeden bestaat dat zij informatie bevatten over de (vermoede) ongewenste gedraging van de Medewerker;
b. indien de Medewerker een wettelijke geheimhoudingsplicht heeft, worden alle bestanden en berichten die betrekking hebben op de werkzaamheden van deze Medewerker in die hoedanigheid buiten beschouwing gelaten;[5]
c. indien de Medewerker een geheimhoudingsplicht heeft op basis van een reglement van de VU, worden alle bestanden en berichten die betrekking hebben op de werkzaamheden van deze Medewerker in die hoedanigheid buiten beschouwing gelaten, tenzij:
   - een gerechtvaardigd vermoeden bestaat dat zij informatie bevatten over de (vermoede) ongewenste gedraging van de Medewerker; en
   - het onderzoeksbelang in dat geval zwaarder weegt dan het belang dat gediend wordt met de geheimhoudingsplicht in het betreffende reglement;[6]
d. indien de Medewerker een vertrouwensfunctie heeft die niet valt binnen de categorieën zoals bedoeld in artikel 10.3 (b) of (c), worden alle bestanden en berichten die betrekking hebben op werkzaamheden van deze Medewerker in die hoedanigheid buiten beschouwing gelaten, tenzij een gerechtvaardigd vermoeden bestaat dat zij informatie bevatten over de (vermoede) ongewenste gedraging van de Medewerker[7];
e. geprivilegieerde informatie die betrekking heeft op de Medewerker - waaronder communicatie met een bedrijfsarts, psycholoog, de Functionaris voor Gegevensbescherming (FG), de Ombudsman, vertrouwenspersonen en/of commissieleden zoals bedoeld in artikel 10.3 (c), de Ondernemingsraad (OR), de Onderdeelcommissie (ODC), vakbondsconsulent en een advocaat - worden buiten beschouwing gelaten, tenzij de (vermoede) ongewenste gedraging van de Medewerker direct betrekking heeft op het contact met één of meer van de hiervoor bedoelde personen en instanties.

10.4 Het gerechtvaardigd vermoeden zoals bedoeld in artikel 10.2 (a) kan gebaseerd zijn op de resultaten van Monitoring, Logging, eigen waarneming van de VU en/of een melding door een derde.

10.5 De verzamelde gegevens en resultaten van het Gericht Onderzoek en/of Inhoudelijk Onderzoek zijn uitsluitend - onder strikte geheimhouding - toegankelijk voor de leidinggevende van de betreffende Medewerker, de directeur van de Faculteit of Dienst waar de betreffende Medewerker werkzaam is, het College van Bestuur, de leden en de ambtelijk secretaris van de klachtencommissie zoals bedoeld in de regeling Ongewenst Gedrag voor zover het onderzoek is verricht op verzoek van deze commissie, en

[5] Medewerkers met een wettelijke geheimhoudingsplicht zijn in ieder geval: bedrijfsartsen, (studenten)psychologen en de Functionaris voor Gegevensbescherming (FG).

[6] Medewerkers met een reglementaire geheimhoudingsplicht zijn ieder geval: de ombudsmannen voor personeel en studenten, alsmede vertrouwenspersonen en commissieleden in het kader van de Regeling ongewenst gedrag, de Klokkenluidersregeling en de Klachtenregeling wetenschappelijke Integriteit VU-VUmc.

[7] Medewerkers met een dergelijke vertrouwensfunctie zijn in ieder geval: leden van de Ondernemingsraad (OR), leden van de Onderdeelcommissie (ODC), vakbondconsulenten, studentdecanen, studieadviseurs, bedrijfsmaatschappelijk medewerkers en redacteuren van Advalvas.

eventueel de ter ondersteuning betrokken HR-adviseur en/of (arbeids)jurist. Indien de betreffende Medewerker directeur of decaan is, zijn de verzamelde gegevens en resultaten uitsluitend - onder strikte geheimhouding - toegankelijk voor het College van Bestuur, de leden en de ambtelijk secretaris van de klachtencommissie zoals bedoeld in de regeling Ongewenst Gedrag voor zover het onderzoek is verricht op verzoek van deze commissie, en eventueel de betrokken HR-adviseur en/of (arbeids)jurist. Indien de betreffende Medewerker lid is van het College van Bestuur, zijn de verzamelde gegevens en resultaten uitsluitend - onder strikte geheimhouding - toegankelijk voor de Raad van Toezicht, de leden en de ambtelijk secretaris van de klachtencommissie zoals bedoeld in de regeling Ongewenst Gedrag voor zover het onderzoek is verricht op verzoek van deze commissie, en eventueel de ter ondersteuning betrokken HR-adviseur en/of (arbeids)jurist.

10.6 De resultaten van Gericht onderzoek en/of Inhoudelijk onderzoek worden onmiddellijk vernietigd indien het vermoeden van overtreding van de Gedragscode en/of een ernstige verwijtbare gedraging onterecht blijkt. Zodra geen noodzaak meer bestaat om de resultaten te bewaren, worden deze vernietigd. De resultaten van Gericht onderzoek en/of Inhoudelijk onderzoek kunnen (langer) worden bewaard indien noodzakelijk voor bepaalde bewijsvoering in rechte of in het belang van een strafrechtelijk onderzoek of aangifte.

Artikel 11. Bezwaar onderzoek

11.1 De Medewerker die onderwerp is van Gericht onderzoek en/of Inhoudelijk onderzoek, zoals bedoeld in artikel 10, kan daartegen schriftelijk en gemotiveerd bezwaar aantekenen bij het College van Bestuur binnen vier weken nadat hij is ingelicht over het onderzoek.

11.2 Het College van Bestuur neemt zo spoedig mogelijk en in ieder geval binnen vier weken na ontvangst van het bezwaar een schriftelijk en met redenen omkleed besluit. Indien het bezwaar gegrond wordt verklaard, worden de door middel van Gericht onderzoek en/of Inhoudelijk onderzoek verkregen gegevens terstond vernietigd. Daarnaast worden eventuele maatregelen ingetrokken indien deze ten onrechte zijn genomen.

11.3 Het aantekenen van bezwaar laat onverlet dat de VU maatregelen kan treffen zoals bedoeld in artikel 12.

Artikel 12. Maatregelen

12.1 De VU behoudt zich het recht voor om Medewerkers die in strijd handelen of hebben gehandeld met de Gedragscode de toegang tot bepaalde ICT-voorzieningen te ontzeggen of deze te beperken.

12.2 Wanneer blijkt dat een Medewerker in strijd heeft gehandeld met de Gedragscode kan het College van Bestuur afhankelijk van de aard en ernst van de overtreding jegens hem passende maatregelen treffen, waarbij ontslag (op staande voet) de meest vergaande maatregel is.

12.3 Indien sprake is van (een gerechtvaardigd vermoeden van) een strafbaar feit, kan de VU aangifte doen.

Artikel 13. Rapportage Ondernemingsraad

13.1 Het CvB rapporteert jaarlijks aan de Ondernemingsraad over het aantal individuele onderzoeken dat in een bepaald jaar heeft plaatsgevonden en de algemene uitkomsten hiervan. Hierbij zullen geen tot personen herleidbare gegevens worden gedeeld.

HOOFDSTUK 6. GEBRUIK VERKEERSGEGEVENS EN BEWAARTERMIJN

Artikel 14. Gebruik Verkeersgegevens

14.1 De VU gebruikt Verkeersgegevens alleen overeenkomstig dit Reglement.

14.2 De VU gebruikt Verkeersgegevens voor:

a. Logging zoals beschreven in artikel 8;
b. Monitoring zoals beschreven in artikel 9;
c. individueel onderzoek zoals beschreven in hoofdstuk 5; en
d. het volgen van werkprocessen. Denk hierbij aan een (automatische) herinnering die wordt verstuurd naar een Medewerker wanneer hij een taak in VUnet niet of te laat uitvoert.

14.3 De VU gebruikt Verkeersgegevens niet om het individuele functioneren van (bepaalde groepen) Medewerkers te beoordelen, tenzij hiertoe een schriftelijk besluit is genomen door het College van Bestuur en de Ondernemingsraad hiermee heeft ingestemd.

Artikel 15. Bewaartermijn

15.1 De gegevens die worden verzameld en verwerkt in het kader van Logging en Monitoring worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor deze zijn verzameld en (verder) worden verwerkt.

15.2 De VU houdt zich aan de wettelijke bewaartermijnen die gelden voor persoonsgegevens en andere gegevens. Voor zover geen sprake is van een wettelijke bewaartermijn, heeft de VU bewaartermijnen vastgesteld. Deze zijn te vinden op VUnet.

HOOFDSTUK 7. SLOTBEPALINGEN

Artikel 16. Toezicht

16.1 De Functionaris voor Gegevensbescherming (FG) van de VU is belast met het toezicht op de naleving van dit Reglement. De FG van de VU wordt door de VU in staat gesteld zijn toezichthoudende taak onafhankelijk en naar behoren uit te oefenen. Dit betekent dat hij wat betreft de uitoefening van zijn functie geen aanwijzingen kan ontvangen van (het CvB van) de VU en dat hij geen nadeel ondervindt van de uitoefening van zijn functie. De FG van de VU heeft een adviserende rol ten opzichte van het CvB.

16.2 Alle Medewerkers zijn verplicht aan de FG alle medewerking te verlenen die de FG redelijkerwijs bij de uitoefening van zijn bevoegdheden kan vragen, tenzij een wettelijke geheimhoudingsplicht daaraan in de weg staat. Voor zover een geheimhoudingsplicht een Medewerker in de weg staat om medewerking te verlenen, zal de Medewerker de FG daarvan onverwijld op de hoogte stellen.

Artikel 17. Implementatie nieuw IT-systeem

17.1 Voordat het College van Bestuur overgaat tot de implementatie van een nieuw, belangrijk IT-systeem, overlegt het College van Bestuur met de Ondernemingsraad over de implicaties hiervan in het licht van het bepaalde in dit Reglement. In dit kader kan de Ondernemingsraad een advies- en/of instemmingsrecht hebben, een en ander zoals bepaald in de Wet op de ondernemingsraden (WOR).

Artikel 18. Slotbepalingen

18.1 In gevallen waarin dit Reglement niet voorziet beslist het CvB.
18.2 De Ondernemingsraad heeft ingestemd met dit Reglement.
18.3 Dit Reglement wordt gepubliceerd op de website van de VU en intranet (VUnet).
18.4 Dit Reglement is vastgesteld door het CvB en is in werking getreden per juli 2019.
18.5 De toepassing van dit Reglement wordt twee jaar na de inwerkingtreding ervan geëvalueerd en besproken met de Ondernemingsraad.

***