UNIVERSITEIT VAN AMSTERDAM

REGELS VOOR VERANTWOORD GEBRUIK VAN ICT-FACILITEITEN VOOR MEDEWERKERS VAN DE UNIVERSITEIT VAN AMSTERDAM

Vastgesteld bij besluit nr. 2018-068316 van het College van Bestuur van 25 september 2018

Basis voor de Regels voor verantwoord gebruik van ICT-faciliteiten

Het gebruik van ICT-faciliteiten[1] is voor (veel van) de medewerkers van de Universiteit van Amsterdam (hierna: de "***UvA***") noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn echter risico's verbonden. Tegen de achtergrond van deze risico's mag van de medewerkers van de UvA verantwoord gebruik van de ICT-faciliteiten worden verwacht.

Met deze Regels voor verantwoord gebruik van ICT-faciliteiten (hierna: Reglement) wil de UvA regels stellen omtrent het gewenst gebruik van haar ICT-faciliteiten. Het streven daarbij is een goede balans aan te brengen tussen het inzetten van ICT-faciliteiten ten behoeve van onderwijs, onderzoek en bedrijfsvoering aan de ene kant en het verantwoord en veilig gebruik van de ICT-faciliteiten en de privacy van de medewerker aan de andere kant. De missie van de UvA is academisch onderwijs verzorgen voor de voorhoede van morgen, baanbrekend (fundamenteel) wetenschappelijk onderzoek verrichten en dit vertalen naar relevante maatschappelijke toepassingen. Het verantwoord gebruik van de ICT-faciliteiten ondersteunt medewerkers en studenten bij het realiseren van deze missie, binnen een instelling waarbij de vrijheid van handelen van medewerkers en studenten een groot goed is.

Het gebruik van social media wordt steeds belangrijker maar kan ook zijn weerslag hebben op de UvA. Daarom zijn in dit Reglement enkele gedragsregels voor het gebruik daarvan opgenomen.

De UvA is eigenaar van de aan haar medewerkers ter beschikking gestelde ICT-faciliteiten en is vanuit die hoedanigheid gerechtigd aan het gebruik daarvan voorschriften te verbinden. Medewerkers zijn daarenboven aan dit Reglement gebonden op grond van art. 125 ter Ambtenarenwet en art. 1.8(2) CAO NU (alsook, na invoering van de Wet normalisering rechtspositie ambtenaren, op grond van art. 7:611 BW).

Dit Reglement treedt in werking op 25 september 2018 na instemming met dit Reglement van de Centrale Ondernemingsraad (ex art. 27(1)(d) WOR) d.d. 30-08-2018.

Artikel 1. Uitgangspunten

1.1 Dit Reglement stelt regels ten aanzien van het gebruik van de ICT-faciliteiten. door medewerkers van de UvA. Doel van deze regels is de goede orde te bepalen ten aanzien van:
- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- bescherming van persoonsgegevens;
- bescherming van vertrouwelijke informatie;
- bescherming van intellectuele eigendomsrechten en het respecteren van licentie-afspraken;
- voorkomen van een onjuist beeld van de UvA door het verspreiden van onjuiste informatie;
- kosten- en capaciteitsbeheersing.

1.2 Beperkt privégebruik van ICT-faciliteiten is toegestaan, voor zover de werkzaamheden er niet onder lijden, het niet storend is voor anderen en het geen storende invloed heeft op de goede werking, waaronder beschikbaarheid van het netwerk of andere ICT-faciliteiten.

[1] Onder ICT-faciliteiten wordt verstaan: hardware, programmatuur en informatiesystemen.

1.3 Dit Reglement geldt voor eenieder die voor de UvA werkzaam is, dus ook voor uitzendkrachten, tijdelijke medewerkers en gasten[2]. Het Reglement geldt niet voor (gast)studenten; hiervoor is het aparte Studentenreglement opgesteld.
1.4 Dit Reglement geldt ook indien de medewerker als gast gebruiker gebruik maakt van netwerkvoorzieningen van andere instellingen, waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (Eduroam).
1.5 De UvA streeft in het kader van handhaving van dit Reglement naar maatregelen die inzage in persoonsgegevens zo veel mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren, zonder daarbij zichzelf of derden inzage te geven in gedrag van individuele personen.

Artikel 2. Intellectueel eigendom en vertrouwelijke informatie

2.1 De medewerker dient vertrouwelijke informatie, waaronder persoonsgegevens, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.
2.2 De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten en respecteert licentieafspraken.
2.3 De medewerker heeft geen zeggenschap of beschikkingsbevoegdheid over eigendom van de UvA, behalve voor zover dat expliciet is toegekend.
2.4 Het is de medewerker niet toegestaan om grote hoeveelheden artikelen uit de bestanden van de digitale bibliotheek te downloaden of substantiële delen van de bestanden of databases in de digitale bibliotheek systematisch te kopiëren.[3]
2.5 De medewerker besteedt bijzondere aandacht aan het treffen van veiligheidsmaatregelen indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie, waaronder onderzoeksgegevens en/of persoonsgegevens, buiten de Instelling noodzakelijk is, zoals via e-mail, in niet-instellingsgebonden cloud-toepassingen, op externe opslagmedia of eigen apparatuur of opslagmedia, zoals USB-apparaten, of tablets. De UvA kan nadere voorwaarden stellen aan de toelaatbaarheid en/of wijze waarop opslag, versturen, of het delen van berichten en bestanden plaatsvindt. De medewerker dient zich te houden aan zulke nadere voorwaarden.
2.6 Deze bepalingen gelden in het bijzonder voor ICT beheerders[4], voor wie schending van deze bepalingen als een zeer ernstig plichtsverzuim wordt aangemerkt, gezien hun bijzondere positie.

Artikel 3. Gebruik van ICT-faciliteiten

3.1 ICT-faciliteiten worden aan medewerkers van de UvA voor gebruik in het kader van hun functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die daaruit voortvloeien. Privégebruik van de door de UvA ter beschikking gestelde ICT-faciliteiten is alleen toegestaan zoals bepaald in artikel 1.2.
3.2 De medewerker dient te allen tijde zorgvuldig om te gaan met persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik daarvan kan de UvA per direct het betrokken account ontoegankelijk maken.

---

[2] Personen die ten behoeve van de UvA op enigerlei wijze werkzaamheden verrichten en/of bijdragen aan onderwijs en onderzoek (zoals stagiaires, personen die in het kader van uitwisselings- of onderzoeksprogramma's verbonden zijn aan de eenheid, gedetacheerden en/of personen werkzaam op declaratiebasis).
[3] Dit artikel veronderstelt dat er auteursrechtelijke beperkingen zijn op de bestanden in de digitale bibliotheek. Gezien de ontwikkeling naar ‘open access’ wordt deze beperking minder relevant.
[4] Iedereen die op grond van zijn/haar functie een taak heeft in het beheer van ICT-systemen, waaronder ook functioneel beheer van informatiesystemen.

3.3 De UvA kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een Elektronische Leeromgeving, een emailsysteem, (Mobiele) Applicaties (Apps), Cloudvoorzieningen of multimediadiensten. De medewerker zal in die gevallen voor het delen van lesmateriaal of het uitvoeren van onderzoek alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.

3.4 Ten aanzien van het gebruik van de ICT-faciliteiten is het de medewerker met name niet toegestaan:

a. zich toegang (trachten) te verschaffen tot gegevens van andere medewerkers en tot programmabestanden van computersystemen of deze te wijzigen of te vernietigen, behoudens uitdrukkelijk daartoe verleende verifieerbare toestemming;
b. zich toegang (trachten) te verschaffen tot computersystemen voor zover dit systemen betreft waarvoor geen expliciete toegangsmogelijkheid voor de medewerker is gecreëerd;
c. acties te ondernemen die de integriteit en continuïteit van de ICT-faciliteiten ondermijnen;
d. onbevoegde pogingen te ondernemen om voor de ICT-faciliteiten hogere privileges te bemachtigen dan de toegekende privileges;
e. onbevoegde pogingen te ondernemen om systeem- of gebruikers-autorisatiecodes (zoals wachtwoorden) op enigerlei wijze en in enigerlei vorm te bemachtigen;
f. voor anderen bestemde (e-mail) berichten te lezen, kopiëren, wijzigen of uit te wissen;
g. de door de UvA ter beschikking gestelde programmatuur, databestanden en documentatie te kopiëren of ter beschikking te stellen aan derden, behoudens daartoe verleende schriftelijke toestemming[5];
h. opzettelijk, of door verwijtbaar handelen of nalaten computer-"malware"[6] (of andere kwaadaardige software) op en via de ICT-faciliteiten te introduceren.

3.5 Het installeren van software op de ICT-faciliteiten van de UvA is niet toegestaan zonder toestemming van ICTS, tenzij het zelf installeren onderdeel is van de service zoals verleend door ICTS.

3.6 Het aansluiten van servers en actieve netwerkcomponenten op het UvA-netwerk (zoals access points en routers) is niet toegestaan zonder toestemming van ICTS.

3.7 Het aansluiten van eigen apparatuur (zoals laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. ICTS kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit Reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.

3.8 Het opslaan van privébestanden of -informatie op systemen van de UvA is toegestaan, mits dit niet leidt tot overbelasting van de opslagcapaciteit van deze systemen of een verstoring van de goede orde op de werkvloer. De UvA is echter niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.

3.9 Het gebruik van ICT-faciliteiten door een medewerker ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan indien en voor zover de UvA hiervoor schriftelijk toestemming heeft verleend.

Artikel 4. Gebruik van e-mail en andere ICT-communicatiemiddelen

4.1 Het e-mailsysteem en de bijbehorende mailbox en het e-mailadres wordt aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

4.2 Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

[5] In het geval van open source is dergelijke schriftelijke toestemming niet vereist. De licentievoorwaarden ('open source') worden beschouwd als de verleende schriftelijke toestemming.

[6] Malware is kwaadaardige software die gebruikt wordt om een computersysteem opzettelijk te verstoren. Het doel daarvan varieert van onbruikbaar maken tot het verzamelen van informatie.

4.3 Verboden bij elk gebruik (werkgerelateerd of niet) van ICT-communicatiemiddelen is echter het verzenden van informatie of berichten die het imago, de morele of economische belangen van de UvA kunnen schaden.[7] Voorbeelden hiervan zijn:
- het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud;
- het verzenden van berichten met een (seksueel) intimiderende inhoud;
- het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven te versturen of kwaadaardige software (malware).

4.4 De medewerker gebruikt voor privémail bij voorkeur niet het door de UvA verstrekte e-mailadres, binnen de grenzen van artikel 1.2.

4.5 In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de medewerker, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is de Instelling gerechtigd een vervanger of leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen doch uitsluitend indien aangetoond kan worden dat toestemming van de medewerker verkrijgen onmogelijk is of het bedrijfsbelang zodanig zwaar is dat toestemming niet gevergd kan worden. Deze mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar dan wel afkomstig van een vertrouwenspersoon/bedrijfsarts/HR-consulent. Indien de medewerker geen dergelijke markeringen heeft aangebracht, kan de Instelling door inschakeling van een vertrouwenspersoon de betreffende informatie van de medewerker controleren om zo privéinformatie te herkennen en apart te plaatsen alvorens de vervanger of leidinggevende toegang krijgt.

4.6 E-mailberichten van leden van het medezeggenschapsorgaan onderling, van bedrijfsartsen, van HR-consulenten en van een ieder die zich op grond van de wet op vertrouwelijkheid mag beroepen, worden niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

Artikel 5 Gebruik van internet

5.1 De toegang tot internet en bijbehorende ICT-faciliteiten wordt aan de medewerker in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

5.2 Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

5.3 Verboden bij elk gebruik (werkgerelateerd of niet) is echter:
- internetpagina's te bezoeken die het imago, de morele of economische belangen van de UvA kunnen schaden, zoals internetpagina's die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten[8] [9];
- zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet;

5.4 Onderdeel van de ICT-faciliteiten die de medewerker ter beschikking gesteld worden zijn filesharing- of streamingdiensten. In het geval dat het gebruik van deze diensten overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de ICT-faciliteiten in gevaar brengt, dan kan de UvA hier tegen optreden.

---

[7] Er wordt actie ondernomen op basis van klachten door medewerkers en studenten of andere bronnen (derden). Klachten worden beoordeeld aan de hand van wet- en regelgeving.

[8] De sites genoemd in dit Artikel kunnen ook onderwerp zijn van wetenschappelijk onderzoek en onderwijs. Dit onderzoek en onderwijs is natuurlijk mogelijk en wordt beoordeeld binnen de (ethische) afwegingen van het onderzoek en onderwijs.

[9] Er wordt actie ondernomen op basis van klachten door medewerkers en studenten of andere bronnen (derden). Klachten worden beoordeeld aan de hand van wet- en regelgeving.

Artikel 6. Gebruik van sociale media

6.1 De UvA ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de medewerker met vakgenoten en derden via sociale media Medewerkers zijn 24/7 UvA medewerker en uitingen op social media kunnen soms onvoorziene gevolgen hebben.. Alle medewerkers vertegenwoordigen de UvA, zeker als de UvA als werkgever wordt vermeld. De medewerker draagt zorg bij gebruik van, en uitingen via, social media voor een waardevolle en toegevoegde bijdrage, waarbij duidelijk wordt gemaakt dat het een persoonlijk standpunt betreft dat niet overeen hoeft te komen met dat van de UvA. Bijlage 1 van de social-mediarichtlijnen geeft een handleiding voor alle medewerkers voor het goed gebruik van social media. Zie hiervoor de website van de UvA[10].

6.2 Bestuurders, managers, leidinggevenden en anderen die namens de UvA beleid of strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, ook als de inhoud niet direct verband houdt met hun werk. Op grond van hun positie moeten zij nagaan of zij op persoonlijke titel kunnen publiceren. Zij dienen zich ervan bewust te zijn dat medewerkers lezen wat zij schrijven.

6.3 Dit artikel geldt ook indien medewerkers vanaf privécomputers of -internetaansluitingen deelnemen aan sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

6.4 Wanneer een medewerker een sociale-media-account heeft opgezet dat direct gerelateerd is aan zijn of haar werkzaamheden bij de UvA zullen medewerker en de UvA bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop.

Artikel 7. Monitoring en controle

7.1 Controle van gebruik van de ICT-faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement voor de doelen genoemd in artikel 1. Verboden gebruik van ICT-faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

7.2 Ten behoeve van controle op het functioneren van het systeem en op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke ICT beheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld.

7.3 Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

7.4 De UvA houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de Algemene Verordening Gegevensbescherming (AVG) en andere relevante wet- en regelgeving. In het bijzonder beveiligt de UvA de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

7.5 Enkele specifieke maatregelen ter controle die de UvA kan voeren, zijn:

- controle ter voorkoming van b.v. uitlekken van vertrouwelijke informatie en controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van filtering van de inhoud op trefwoorden. Verdachte berichten worden automatisch teruggestuurd naar de afzender;
- controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag (zoals bv. adressen van videosites). Als deze websites tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;

[10] De richtlijn is te vinden op: https://medewerker.uva.nl/content-secured/az/social-media/social-media.html.

- controle op het gebruik van auteursrechtelijk beschermd beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.

Artikel 8. Procedure bij gericht onderzoek

8.1 Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende een specifieke medewerker worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die medewerker.

8.2 Gericht onderzoek naar verkeersgegevens of andere persoonsgegevens vindt uitsluitend plaats na schriftelijke opdracht van, de decaan voor faculteiten en de directeur van de betreffende afdeling voor overige eenheden, na consultatie van de Functionaris Gegevensbescherming (FG) en goedkeuring van de directeur ICTS. Het College van Bestuur en de Functionaris Gegevensbescherming (FG) ontvangen een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

8.3 In afwijking van het vorige lid vindt gericht onderzoek naar de beveiliging of integriteit van de ICT-faciliteiten plaats door ICTS op basis van concrete aanwijzingen. Aparte toestemming van de in lid 2 bedoelde instantie is niet nodig. De resultaten van dit onderzoek worden alleen gedeeld met de medewerker met het doel de beveiliging of integriteit van de ICT-faciliteiten te verbeteren. Bij herhaling zal de procedure uit lid 2 worden gevolgd.

8.4 Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de ICT-faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de UvA overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist schriftelijke toestemming van het College van Bestuur, welke toestemming de redenen zal noemen waarom deze wordt verleend.

8.5 Enkele specifieke persoonsgebonden maatregelen ter controle die de UvA kan voeren, zijn:
- controle op het uitlekken van vertrouwelijke informatie vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het College van Bestuur;
- controle op overtreding van het verbod uit artikel 4 lid 3 vindt plaats door twee personen op basis van een specifieke klacht e-mailberichten te openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud.

8.6 De medewerker wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur van de betreffende afdeling 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. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

8.7 Geautoriseerde ICTS medewerkers verschaffen zich slechts toegang tot accounts of computers van een medewerker als de medewerker daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit artikel. De medewerker zal in dat geval achteraf worden geïnformeerd.

Artikel 9. Rechten van de medewerker m.b.t. persoonsgegevens

9.1 De medewerker kan zich tot het bestuur wenden met het verzoek voor een volledig overzicht van zijn persoonsgegevens zoals door de Instelling verwerkt in het kader van dit Reglement. Aan een dergelijk verzoek wordt binnen vier weken voldaan.

9.2 De medewerker kan het bestuur verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift zijn. Op een dergelijk

verzoek wordt binnen vier weken gereageerd. Een weigering is met redenen omkleed. Een toegewezen verzoek zal zo spoedig mogelijk worden uitgevoerd.

9.3 De medewerker kan verder verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met zwaarwegende persoonlijke omstandigheden. Het bestuur oordeelt binnen vier weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien het bestuur het verzet gerechtvaardigd acht, beëindigt zij terstond de verwerking.

9.4 Het bestuur zal de medewerker geen opdrachten of dienstbevelen geven ten aanzien van privacygevoelige informatie en persoonsgegevens die in strijd zijn met dit Reglement.

Artikel 10. Consequenties van overtreding

10.1 Bij handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het College van Bestuur afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, overplaatsing, schorsing en beëindiging van de aanstelling. Daarnaast kan het College van Bestuur besluiten tot een al dan niet tijdelijke beperking in de toegang tot bepaalde ICT-faciliteiten.

10.2 Er worden geen disciplinaire maatregelen getroffen zonder dat de Medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

10.3 Behalve een waarschuwing kunnen geen disciplinaire maatregelen worden opgelegd indien de controle slechts heeft plaatsgevonden op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens (zoals een constatering op basis van een automatisch filter of een blokkade).

10.4 In aanvulling op het voorgaande is het mogelijk dat de UvA bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende ICT-faciliteit invoert. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

Artikel 11. Slotbepaling

11.1 In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur. Het CvB wint, afhankelijk van het onderwerp, advies in bij de Chief Security Officer (CSO) en/ of de Chief Information Security Officer (CISO) en/of de Functionaris Gegevensbescherming (FG).