Acceptable Use Policy

Reglement voor ICT- en internetgebruik voor werknemers UM.

Versie 2.0

17 november 2020

Versie	Status	Datum	Door
1.1	Concept	27 juli 2020	CISO
1.2	Concept	20 augustus 2020	Privacy-Team / UM-SOC
1.3	Instemming	30 juni 2021	Lokaal Overleg
1.3	Instemming	22 september 2021	Univeriteitsraad
2.0	Vastgesteld	17 november 2020	College van Bestuur

Inhoudsopgave

Preambule

In deze Acceptable Use Policy (AUP) kun je lezen welke reglementen voor ICT- en internetgebruik het College van Bestuur van de UM heeft vastgesteld voor haar werknemers. Een AUP is noodzakelijk om aan de werknemers duidelijk te maken hoe zij de ICT-voorzieningen van de UM kunnen gebruiken voor het uitoefenen van hun werkzaamheden, zonder dat ze daarbij (wettelijke) regels en richtlijnen overtreden en zonder dat zij de veiligheid van de digitale systemen van de UM in gevaar brengen. Maar vooral ook zonder dat ze de veiligheid van andere gebruikers in gevaar brengen. Tenslotte zorgen de afspraken in de AUP er ook voor dat je rechten als werknemer worden gerespecteerd.
De AUP wordt daarom aan iedere werknemer ter beschikking gesteld. Van alle gebruikers van de ICT-faciliteiten van de UM wordt verwacht dat ze bekend zijn met de UM-reglementen en de wet en dat ze vooral ook hun "gezond verstand" gebruiken.

De gebruikers binnen de UM vormen een afspiegeling van de maatschappij. Dit betekent dat gebruikers vergissingen of fouten kunnen maken en het is zelfs denkbaar dat moedwillig ongewenste handelingen gepleegd worden. Geen enkel reglement is hier tegen bestand.
Het is natuurlijk ook denkbaar dat je als gebruiker ondanks je voorzorgsmaatregelen toch slachtoffer wordt van een phishing aanval of een virus- of malware infectie.
De nadrukkelijke bedoeling van de AUP is de verwachtingen tussen gebruikers onderling en tussen gebruikers en systeembeheerders te verduidelijken en een kader te bieden om daar onderling over te kunnen communiceren. We vragen je dan ook om dit in een open sfeer te doen. De kans op fouten, vergissingen en misverstanden wordt zo verkleind.

Voor gevallen van ongewenst gedrag voorziet de AUP in maatregelen. In de regel zal het gaan om een waarschuwing waarin wordt uitgelegd waarom onderhavig gedrag ongewenst is en wat de consequenties van (herhaling) van dat gedrag zijn. Niet uitgesloten is dat zich gevallen voordoen waarin de ernst van de situatie naar het oordeel van het CvB om een strenger ingrijpen vraagt en niet kan worden volstaan met een waarschuwing en een zwaardere sanctie gepast is.
De gebruiker krijgt in alle gevallen de gelegenheid om diens kant van het verhaal naar voren te brengen: hoor en wederhoor dus.
Juridisch taalgebruik is in een AUP onvermijdelijk. Een reglement moet namelijk maar voor één uitleg vatbaar zijn. Twijfel je over de afspraken in deze AUP, dan kun je altijd aan je lokale IT-ondersteuner, je Informatie Manager, je leidinggevende of aan de Servicedesk van ICTS vragen hoe in een bepaalde situatie te handelen.

1. Inleiding

Het gebruik van netwerkfaciliteiten en ICT-middelen, hierna te noemen: de Faciliteiten, is voor de werknemers binnen Universiteit Maastricht, hierna te noemen: de Instelling, noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn echter risico's verbonden, die dwingen tot het stellen van gedragsregels. Tegen de achtergrond van deze risico's mag van de werknemers verantwoord gebruik van de Faciliteiten worden verwacht.
Met dit ICT- en internetreglement, hierna te noemen: het Reglement, wil de Instelling regels stellen, over het gewenst gebruik van de Faciliteiten. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van de werknemer.

Het gebruik van sociale media zoals Facebook, LinkedIn, WhatsApp en Twitter is inmiddels niet meer weg te denken, maar kan ook zijn weerslag hebben op de Instelling. Daarom wil de Instelling ook hier bepaalde regels aan stellen. Deze worden in dit Reglement uitgewerkt.

Op grond van artikel 7:660 BW is de Instelling als werkgever bevoegd regels te stellen over de uitvoering van het werk en de goede orde op de werkvloer.

Het College van Bestuur heeft dit reglement vastgesteld op 17 november 2020. Omdat het Reglement voorziet in een verwerking van persoonsgegevens en controle op gedrag van werknemers en de regeling rechten en plichten bevat voor werknemers, zijn de Universiteitsraad en het Lokaal Overleg van de Instelling instemming plichtig. De Universiteitsraad en het Lokaal Overleg hebben op 22 september 2021 resp. 30 juni 2021 ingestemd met de inhoud van dit Reglement.

Het UM Informatiebeveiligingsbeleid en nadere uitleg over beveiliging en beveiligingsmaatregelen zijn opgenomen op de beveiligingspagina's van de UM:
https://www.maastrichtuniversity.nl/informatiebeveiliging.
Voor specifieke diensten en voorzieningen kunnen specifieke reglementen, afspraken of werkinstructies van toepassing zijn. Deze worden afzonderlijk gecommuniceerd.
Bij twijfel over afspraken, richtlijnen, maatregelen etc. kan de leidinggevende toelichting geven.

2. Algemeen

In dit Reglement voor ICT- en internetgebruik van werknemers van de Instelling geeft de Instelling aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van Faciliteiten en wat dit voor de werknemers in de dagelijkse praktijk betekent. Hieronder volgen het doel van dit Reglement en de toepasselijkheid.

Artikel 1. Doel

Het Reglement stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en internet door werknemers. 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 privacy gevoelige informatie van de Instelling, waaronder persoonsgegevens van haar werknemers, (oud)studenten en andere betrokkenen;
- bescherming van vertrouwelijke informatie van de Instelling en haar werknemers, en van studenten en ouders;
- bescherming van de intellectuele eigendomsrechten van de Instelling en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de Instelling;
- voorkomen van negatieve publiciteit;
- kosten- en capaciteitsbeheersing.

Artikel 2. Toepasselijkheid

2.1. Dit Reglement geldt voor iedereen die voor de Instelling werkzaam is en gebruik maakt van de Faciliteiten, die door de Instelling ter beschikking gesteld worden. Dit Regelement geldt dus ook voor uitzendkrachten en zelfstandigen, gedetacheerden, gastdocenten en stagiaires, die ingezet zijn om werkzaamheden voor de Instelling uit te voeren. Voor gasten van werknemers geldt dit Reglement eveneens.
Het Reglement geldt niet voor (gast)studenten; hiervoor is Studentenreglement opgesteld https://www.maastrichtuniversity.nl/informatiebeveiliging.

2.2. Dit Reglement geldt ook indien u als gast gebruik maakt van netwerkvoorzieningen van andere instellingen, waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (Eduroam).

2.3. Dit Reglement wordt aan iedereen, die voor de Instelling werkzaam is, bij indiensttreding overhandigd en werknemers worden daarnaast gewezen op de vindplek van de geldende versie.

2.4. Gasten worden op dit Reglement gewezen, wanneer zij toegang krijgen op het gastennetwerk en krijgen de mogelijkheid dit Reglement desgewenst op te slaan.

2.5. Het gebruik van UM VPN[1] faciliteiten valt volledig onder de regeling van deze AUP, ongeacht het netwerk en het werkstation van waaruit de werknemer de VPN sessie heeft opgestart.

[1] VPN: Virtual Private Network: Een veilige manier om een workstation te verbinden met het Instellingsnetwerk via Internet

3. Gedragscode

Voor het uitoefenen van de werkzaamheden stelt de Instelling aan iedereen, die voor de Instelling werkzaam is, Faciliteiten ter beschikking. In dit hoofdstuk geeft de Instelling aan wat de afspraken zijn waaraan iedereen die voor de Instelling werkzaam is zich te houden heeft, wanneer er gebruik wordt gemaakt van deze Faciliteiten. De Instelling verwacht daarnaast dat werknemers hun eigen verantwoordelijkheid nemen voor het juiste gebruik van de ter beschikking gestelde middelen.

Artikel 3. Gebruik van de Faciliteiten

3.1. Om gebruik te kunnen maken van de Faciliteiten van de Instelling, ontvangt de werknemer persoonsgebonden inloggegevens (wachtwoord en gebruikersnaam) en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). De werknemer dient altijd zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen. Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan het systeembeheer per direct het betrokken account ontoegankelijk maken.

3.2. De Instelling kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een elektronische leeromgeving, een e-mailsysteem, (mobiele) applicaties (apps), cloudvoorzieningen of multimediadiensten. De werknemer zal voor het verzorgen van onderwijs of het uitvoeren van onderzoek alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.

3.3. Het installeren van software op de ICT-middelen en middels de netwerkfaciliteiten van de organisatie is slechts toegestaan voor zover daartoe aan de gebruiker rechten zijn verleend. Het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van het systeembeheer.

3.4. Het gebruik van de Faciliteiten van de Instelling vanuit andere netwerken of vanuit huis is alleen toegestaan via beveiligde (wifi)netwerken en de daarvoor beschikbaar gestelde beveiligde toegang (b.v. VPN of virtuele desktop) met apparatuur van de Instelling of met eigen apparatuur mits deze apparatuur voldoet aan de aanvullende eisen, zoals de installatie van virusscanners, het regelmatig updaten van het besturingssysteem, het toepassen van versleuteling en wachtwoordbeveiliging.
Meer informatie over beveiligingsmaatregelen is te vinden op:
https://www.maastrichtuniversity.nl/informatiebeveiliging.

3.5. Het gebruik van de Faciliteiten door de werknemer ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan als en voor zover de Instelling hiervoor schriftelijk toestemming heeft verleend.

3.6. Bij de uitvoering van de werkzaamheden, die aan de werknemer zijn toegekend, kan deze persoonsgegevens verwerken. Alle verwerkingen van persoonsgegevens, die de werknemer in het kader van zijn functie uitvoert, al dan niet met behulp van de Faciliteiten (waaronder voorgeschreven systemen of applicaties) van de Instelling, dienen te voldoen aan de vereisten onder de AVG en dienen te passen binnen de reguliere werkzaamheden. Zie hiervoor het UM privacy-beleid op de UM Privacy pagina.

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

4.1. Het e-mailsysteem en de bijbehorende mailbox en e-mailadres wordt aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan

taken die voortvloeien uit deze functie. Privégebruik of gebruik ten behoeve van nevenwerkzaamheden van deze middelen is alleen toegestaan zoals bepaald in artikel 7.

4.2. Het verzenden van persoonsgegevens van de Instelling via e-mail en andere ICT-middelen, in het kader van de uitvoering van de werkzaamheden, die aan de werknemer zijn toegekend, is alleen toegestaan, indien dit past binnen de reguliere werkzaamheden en getoetst is aan de AVG.

4.3. Verboden bij elk gebruik (privé of niet-privé) van elektronische communicatiemiddelen, behoudens bij specifieke functie gerelateerde opdrachten, is echter:
- 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 en phishing-mails te versturen of kwaadaardige software zoals virussen, Trojaanse paarden of spyware te versturen.

4.4. In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de werknemer, en uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is de Instelling gerechtigd een vervanger toegang tot de bestanden of mailbox van de werknemer te verschaffen. Echter (i) uitsluitend indien aangetoond kan worden dat toestemming verkrijgen van de werknemer onmogelijk is of het bedrijfsbelang zodanig zwaar is dat toestemming niet gevergd kan worden en (ii) uitsluitend nadat hiertoe aparte toestemming van het College van Bestuur is verkregen. 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, ombudsman (leden van een) medezeggenschapsorgaan[2] of het Lokaal Overleg, bedrijfsarts, of HR- of vakbondsconsulent. Indien de werknemer geen dergelijke markeringen heeft aangebracht, zal de Instelling door inschakeling van een vertrouwenspersoon de betreffende informatie van de werknemer controleren om zo privéinformatie te herkennen en apart te plaatsen alvorens de vervanger toegang krijgt.

Artikel 5. Gebruik van internet

5.1. De toegang tot internet en bijbehorende faciliteiten worden aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. Privégebruik of gebruik ten behoeve van nevenwerkzaamheden van deze middelen is alleen toegestaan zoals bepaald in artikel 7.

5.2. Het verwerken van persoonsgegevens van de Instelling op het internet, in het kader van de uitvoering van de werkzaamheden, die aan de werknemer zijn toegekend, is alleen toegestaan, indien dit past binnen de reguliere werkzaamheden en getoetst is aan de AVG.

5.3. Verboden bij elk gebruik (privé of niet-privé), behoudens bij specifieke functie gerelateerde opdrachten, is echter:
- sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- filesharing- of streamingdiensten (zoals internetradio of Uitzending gemist) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de Faciliteiten in gevaar kan brengen;

[2] Universiteitsraad, faculteit- en dienstraden etc.

- films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de werknemer redelijkerwijs mag aannemen 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 6. Bring your own device (BYOD)

6.1. Het is iedereen, die werkzaamheden voor de Instelling uitvoert, toegestaan hiervoor eigen apparatuur te gebruiken, mits voldaan wordt aan de hieronder gestelde beveiligingseisen. Voor bepaalde zeer gevoelige werkzaamheden, zoals systeembeheer, kunnen specifieke afspraken gelden waardoor eigen apparatuur niet gebruikt mag worden.

6.2. Het aansluiten van eigen apparatuur (zoals, laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde netwerkaansluitingen. Het systeembeheer kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners, het regelmatig updaten van het besturingssysteem, het toepassen van versleuteling en wachtwoordbeveiliging.

6.3. Iedereen die voor de uitvoering van de werkzaamheden voor de Instelling gebruik maakt van eigen apparatuur, is zelf verantwoordelijk voor het nemen van adequate beveiligingsmaatregelen. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- beveilig het apparaat met een sterk wachtwoord of pincode;
- vergrendel het apparaat bij het verlaten van de werkplek;
- sla geen persoonsgegevens waar de Instelling verantwoordelijk voor is op het eigen apparaat op; dit is niet toegestaan;
- versleutel alle gegevens met betrekking tot de Instelling, als deze, om welke reden dan ook, niet op het netwerk van de Instelling opgeslagen worden (denk hierbij aan het eigen apparaat of usb-stick);
- scheid (versleutelde) gegevens van de Instelling en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen apparaat;
- houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks);
- neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

Meer informatie over beveiligingsmaatregelen is te vinden op:
https://www.maastrichtuniversity.nl/informatiebeveiliging.

Artikel 7. Privégebruik van de Faciliteiten

7.1. De Faciliteiten worden aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

7.2. Beperkt privégebruik van de Faciliteiten is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden, de goede orde op de werkvloer of het netwerk van de Instelling.

7.3. Het opslaan van privé bestanden of informatie op systemen van de Instelling is toegestaan, mits dit niet leidt tot overbelasting van het netwerk van de Instelling of de opslagcapaciteit van deze systemen. De Instelling is echter niet verplicht van dergelijke bestanden of informatie reserve kopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.

7.4. De werknemer gebruikt voor privé mail bij voorkeur niet het door de Instelling verstrekte e-mailadres. De organisatie zal de toegang tot andere e- maildiensten niet blokkeren of specifiek monitoren.

7.5. Incidenteel privé gebruik van de door de Instelling verstrekte mobiele telefoon in het buitenland is toegestaan.

7.6. Incidenteel privé gebruik van een mobiel netwerk in het buitenland (roaming) is toegestaan.

Artikel 8. Gebruik van sociale media

8.1. Het gebruik van sociale media (zoals Facebook, YouTube, Instagram, Skype, WhatsApp, Twitter of LinkedIn) voor zaken die raken aan het functioneren of de positie als werknemer voor de Instelling is toegestaan. Wel dient de medewerker rekening te houden met de goede naam van de Instelling en iedereen die hierbij betrokken is. Ga dus op verantwoorde wijze om met het gebruik van sociale media[3].

8.2. De Instelling ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de werknemer met vakgenoten en derden via sociale media (zoals, Facebook, YouTube, Instagram, Skype, Twitter of LinkedIn).
Indien dit werk gerelateerde onderwerpen betreft, dient de werknemer ervoor te zorgen dat het profiel en de inhoud in overeenstemming is met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's en studenten.

8.3. Bestuurders, managers, leidinggevenden en anderen die namens de Instelling 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 zijn zich ervan bewust dat werknemers lezen wat zij schrijven.

8.4. Het delen of verspreiden van persoonsgegevens van anderen via sociale media vanuit de functie is alleen toegestaan, indien dit past binnen de reguliere werkzaamheden en getoetst is aan de AVG. Speciale aandacht dient daarbij geschonken te worden aan het verspreiden van beeldmateriaal (foto's en video's) waarop anderen herkenbaar in beeld zijn. Hiervoor is doorgaans expliciete toestemming van de betrokkenen noodzakelijk.

8.5. Dit artikel geldt ook indien werknemers vanaf privé computers of - internetaansluitingen deelnemen aan sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

8.6. Wanneer werknemer een sociale-media-account opzet dat direct werk gerelateerd is, terwijl het op naam van werknemer persoonlijk is gesteld, zullen werknemer en de Instelling bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop.

Artikel 9. Intellectueel eigendom en vertrouwelijke informatie

9.1. De werknemer dient vertrouwelijke informatie, privacygevoelige informatie waaronder persoonsgegevens waar hij in het kader van het werk toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid[4] te waarborgen.

[3] Zie ook de richtlijnen mbt gebruik social media:
https://www.maastrichtuniversity.nl/nl/support/communicatiegids/social-media
[4] Deze vertrouwelijkheid geldt onverminderd het bepaalde in de "Regeling Melding Misstanden Universiteit Maastricht".

9.2. De werknemer maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Instelling.

9.3. De zeggenschap over de informatie van de Instelling berust bij Instelling. De werknemer heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling.

9.4. Het is de werknemer 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.

9.5. De werknemer besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie buiten de Instelling noodzakelijk is zoals via e-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen apparatuur (USB-sticks, Tablets, etc.). Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid, de naleving van de AVG en de bescherming van intellectueel eigendom voorschriften heeft opgesteld zal werknemer deze strikt naleven.

9.6. Deze bepalingen gelden in het bijzonder voor systeembeheerders, voor wie schending van deze bepalingen als een zeer ernstig plichtsverzuim wordt aangemerkt, gezien hun bijzondere positie.

4. Controle en maatregelen

Dit hoofdstuk beschrijft op welke manier de controle op de naleving van dit Reglement door de Instelling plaatsvindt en welke maatregelen er kunnen volgen, indien het Reglement niet nageleefd wordt.

De Instelling handelt bij de controle op het gebruik van de Faciliteiten, die door de Instelling ter beschikking worden gesteld voor de uitvoering van de werkzaamheden in het kader van de functie van de werknemer, binnen de geldende wet- en regelgeving.

De Instelling streeft in het kader van de controle en handhaving van dit Reglement naar maatregelen, die inzage in privacygevoelige informatie of persoonsgegevens van individuele werknemers zo veel mogelijk beperken. De Instelling zal daarbij uitgaan van de juiste balans tussen verantwoord gebruik van de Faciliteiten en de bescherming van de privacy van iedereen, die voor de Instelling werkzaam is. Zij zal, waar mogelijk, slechts geautomatiseerd controleren of filteren, zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

Artikel 10. Voorwaarden controle

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

10.2. Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens, die niet herleidbaar zijn tot identificeerbare personen. De gegevens, die uit een dergelijke controle voortkomen, zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten.

10.3. Bij vermoedens van overtreding van de regels kan gedurende een vastgestelde (korte) periode, gerichte controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het gebruik van de Faciliteiten, waaronder het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats. De procedure voor gericht onderzoek verloopt, zoals beschreven in artikel 12.

10.4. De Instelling 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 Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

10.5. Persoonsgegevens die zijn vastgelegd in het kader van toezicht en controle worden bewaard voor een zo kort mogelijke periode. Enkel indien er een redelijk vermoeden bestaat van onrechtmatig gebruik kan deze periode worden verlengd. Zodra een onderzoek is afgerond en niet leidt tot maatregelen tegenover een betrokkene, worden de gegevens verwijderd.

Artikel 11. Uitvoering controle

11.1. Enkele specifieke (en bij voorkeur geautomatiseerde) maatregelen ter controle die de Instelling kan voeren, zijn:

- de controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van

filtering van de inhoud op trefwoorden, ook wel content-filtering genoemd. Verdachte berichten worden automatisch teruggestuurd naar de afzender of geweigerd, verwijderd of apart gezet voor nader onderzoek;

- de 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 de adressen van internetradio en 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.
- de controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is;
- de controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het bestuur.

11.2. IT-medewerkers en systeembeheerder(s) zijn aan geheimhouding gebonden als men in het kader van de controle op dit Reglement om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

11.3. Systeembeheerders verschaffen zich slechts toegang tot accounts of UM-beheerde apparatuur van werknemers als de werknemer 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 artikel 12. De werknemer zal in dat geval achteraf worden geïnformeerd.

11.4. Door de Instelling worden in het kader van de controle op dit Reglement de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij verwerkt worden, juist en nauwkeurig zijn.

11.5. Door de Instelling worden in het kader van de controle op dit Regelement passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

Artikel 12. Procedure bij gericht onderzoek

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

12.2. Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van het College van Bestuur, waarbij mede wordt vastgelegd wie van het onderzoek en eventueel van de vastgelegde resultaten op de hoogte wordt gesteld. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

12.3. In afwijking van het vorige lid vindt gericht onderzoek naar de beveiliging of integriteit van (rand)apparatuur plaats door het systeembeheer 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 werknemer met het doel de beveiliging of integriteit van de (rand)apparatuur te verbeteren. Bij herhaling zal de procedure uit lid 2 worden gevolgd.

12.4. Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de Instelling overgaan tot

het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist schriftelijke opdracht van het College van Bestuur, welke opdracht de redenen zal noemen waarom deze wordt verleend. De Instelling zal zich maximaal inspannen de identiteit van de personen die deze kennisneming uitvoeren, geheim te houden. De vastlegging wordt onder naam van het CvB gedaan.

12.5. E-mailberichten van of naar (leden van) medezeggenschapsorganen[5] en het Lokaal Overleg, een bedrijfsarts, een vertrouwenspersoon, een ombudsman, HR- of vakbondsconsulenten en van iedereen 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.

12.6. De gerichte controle op overtreding van het verbod uit artikels 4 lid 3 en 5 lid 3 vindt door twee personen plaats door, op basis van een zwaarwegend vermoeden, (zo mogelijk steekproefsgewijs) e-mailberichten of bestanden te openen en de inhoud te raadplegen. Deze personen zijn daartoe aangewezen door het College van Bestuur en gebonden aan geheimhouding over de inhoud.

12.7. De werknemer wordt zo spoedig mogelijk schriftelijk geïnformeerd namens het CvB over de aanleiding, de uitvoering en het resultaat van het onderzoek. De werknemer 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 of hier een sterk vermoeden van is.

Artikel 13. Consequenties van overtreding

13.1. Bij het handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het bestuur, afhankelijk van de aard en de ernst van de overtreding, passende maatregelen treffen. Daarnaast kan het bestuur besluiten tot een, al dan niet tijdelijke beperking, van de toegang tot bepaalde ICT-faciliteiten.

13.2. Maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. In geval van een waarschuwing op basis van een geautomatiseerde verwerking krijgt de werknemer gelegenheid zijn zienswijze naar voren te brengen. Verder worden geen maatregelen getroffen anders dan bij herhaling van geconstateerde feiten conform artikel 13.3.

13.3. Al dan niet tijdelijke beperkingen in de toegang tot bepaalde ICT-faciliteiten en andere maatregelen kunnen door de Instelling worden opgelegd indien gehandeld wordt in strijd met dit Reglement en daarvoor al eerder een waarschuwing is uitgevaardigd met daarin opgenomen de aard van de geconstateerde handelingen en de consequenties van een eventuele herhaling. De werknemer wordt daarvoor eerst in de gelegenheid gesteld naar aanleiding van de genoemde waarschuwing zijn zienswijze naar voren te brengen.

13.4. Aanvullend op voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen aanvullende maatregelen worden genomen.

13.5. Indien er strafbare feiten worden geconstateerd die vallen onder de Wet Computer-criminaliteit, zal de Instelling aangifte doen.

[5] Universiteitsraad, faculteit- en dienstraden etc.

Artikel 14. Rechten van de werknemer met betrekking tot persoonsgegevens

14.1. De werknemer heeft alle in de AVG opgenomen rechten mbt de verwerking van persoonsgegevens, conform vastgelegd in de Privacyverklaring Werknemers UM (Intranet).

14.2. De werknemer heeft het recht op een menselijke blik bij besluiten op basis van automatisch verwerkte gegevens.

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

Artikel 15. Slotbepaling

15.1. Dit Reglement wordt jaarlijks geëvalueerd door het bestuur.

15.2. De organisatie kan dit Reglement, indien van toepassing met instemming van medezeggenschapsorganen en het Lokaal Overleg, wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de werknemers bekend gemaakt. Het bestuur zal feedback van werknemers in overweging nemen alvorens de wijzigingen in te voeren.

15.3. In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.

Bronvermelding: