REGLEMENT GEBRUIK INTERNET- EN ICT-FACILITEITEN VOOR MEDEWERKERS VAN DE ERASMUS UNIVERSITEIT ROTTERDAM (2015)

De mogelijkheid tot gebruik van door de Erasmus Universiteit Rotterdam (hierna de “EUR”) ter beschikking gestelde internet- en ICT-faciliteiten (communicatie-, computer-, en netwerkfaciliteiten) is voor Medewerkers binnen de EUR een veelal noodzakelijke voorwaarde om hun werk goed te kunnen uitvoeren.

Aan het gebruik van deze faciliteiten kunnen echter ook risico’s verbonden zijn voor de EUR. Tegen de achtergrond van deze risico’s mag van de Medewerker verantwoord gebruik van internet en ICT-faciliteiten worden verwacht.

Met dit Reglement wil de EUR gedragsregels stellen over het gewenste gebruik van de internet- en ICT-faciliteiten. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig gebruik van internet en ICT-faciliteiten, zoals nader geconcretiseerd in dit Reglement, en de privacy van de Medewerker.

In het Reglement wordt daarnaast aandacht besteed aan het gebruik van de door de EUR ter beschikking gestelde communicatiemiddelen, zoals telefoons. Omdat ook het gebruik van social media aan belang toeneemt, zijn in dit Reglement tevens enkele gedragsregels voor het gebruik daarvan opgenomen.

De EUR is als werkgever bevoegd regels te stellen over de uitvoering van het werk en de goede orde op de werkvloer. Dit Reglement is daarnaast gebaseerd op artikel 1.2 van de cao-NU. Omdat het Reglement voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van Medewerkers, heeft de EUR Universiteitsraad (U-Raad) en het EUROPA instemmingsrecht bij de totstandkoming daarvan.

Dit Reglement treedt in werking op 1 september 2015 na instemming met dit Reglement van de Universiteitsraad d.d. 14 juli 2015 en na instemming met dit Reglement van het EUROPA d.d. 18 augustus 2015.

Artikel 1. Begripsbepalingen

In dit Reglement worden de navolgende begrippen met een hoofdletter gebruikt. Onder deze begrippen wordt het volgende verstaan:

Beheerder:	De decaan, directeur of het hoofd van het betreffende organisatieonderdeel van de EUR.
College van Bestuur:	Het College van Bestuur van de Erasmus Universiteit Rotterdam.
De EUR:	De Erasmus Universiteit Rotterdam
Gastvrijheidsovereenkomst:	Een Schriftelijke overeenkomst, tussen de EUR en een natuurlijk persoon die onder voorwaarden in de gelegenheid wordt gesteld binnen de EUR werkzaamheden te verrichten die uitsluitend of in overwegende mate in hun eigen belang zijn, en zonder dat daarbij een dienstverband wordt gesloten.
ICT-Faciliteiten:	Communicatie-, computer-, en netwerkfaciliteiten binnen de EUR, waaronder telefoonvoorzieningen, voorzieningen in de vorm van het EURnet en alle daarmee gekoppelde apparatuur en bijbehorende software, de verbindingen met andere netwerken, zoals internet, evenals computer- en audiovisuele voorzieningen die al dan niet verbonden zijn met het EURnet in zalen en ruimten binnen de EUR, evenals diensten die aan de Medewerkers worden aangeboden en die deze in staat stellen te communiceren via het EURnet en daarmee in verbinding staande netwerken.
Medewerker:	Een natuurlijke persoon die minimaal één aanstelling heeft, of heeft gehad, bij (een onderdeel van) de EUR. Voor wat betreft de reikwijdte van dit Reglement wordt aan de categorie medewerkers gelijkgesteld de natuurlijke persoon die een Gastvrijheidsovereenkomst heeft ondertekenend of: (1) valt binnen de categorieën van personen zoals benoemd in het Universitair Gegevens Model; of, (2) valt binnen de groep van personen die in de praktijk ook gebruik maken van de Gastvrijheidsovereenkomst, ofwel als irregulier personeel toegang tot ICT-faciliteiten hebben, zoals uitzendkrachten en stagiaires; of, 3) valt binnen de groep van personen die medewerker zijn van de Holding en de werkmaatschappijen.
Reglement:	Het ‘Reglement gebruik internet en ICT-faciliteiten voor Medewerkers van de Erasmus Universiteit Rotterdam (2015)’.

Schriftelijk:	Op schrift of ‘langs elektronische weg’ als bedoeld in artikel 6:227a van het Burgerlijk Wetboek.
Systeembeheerder:	Medewerker die in het kader van beheerswerkzaamheden vanuit zijn of haar functie beschikt over verregaande bevoegdheden binnen ICT-systemen.
Toegangscode:	het samenstel van een gebruikers- of login-naam en de bijbehorende (geheime) autorisatiecode of wachtwoord.

Artikel 2. Uitgangspunten

1. Het Reglement stelt regels ten aanzien van het gebruik van internet en ICT-faciliteiten door Medewerkers. 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 die worden verwerkt binnen de EUR, zoals van Medewerkers, studenten en ouders;
    - bescherming van vertrouwelijke informatie van de EUR, van Medewerkers, of van Studenten;
    - bescherming van de intellectuele eigendomsrechten van de EUR en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de EUR;
    - voorkomen van negatieve publiciteit;
    - kosten- en capaciteitsbeheersing.
2. Beperkt privégebruik van internet en 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 de beschikbaarheid, van het netwerk of andere ICT-faciliteiten van de EUR.
3. Dit Reglement geldt voor iedereen die valt binnen de categorie ‘Medewerkers’ zoals omschreven in artikel 1 van dit Reglement. Dit Reglement is niet van toepassing op studenten die zijn ingeschreven voor een bachelor of masteropleiding aan de Erasmus Universiteit Rotterdam, of overige natuurlijke personen die gebruik maken van internet of ICT-faciliteiten van de EUR en die geen Gastvrijheidsovereenkomst hebben getekend waaronder gaststudenten of gastdocenten. Op deze laatste categorieën van personen is het ‘Reglement gebruik internet en ICT-faciliteiten voor studenten aan de Erasmus Universiteit Rotterdam (2015)’ van toepassing.

4. Dit Reglement is ook van toepassing indien gebruik wordt gemaakt van netwerkvoorzieningen van andere instellingen waarbij toegang wordt verkregen op basis van de inloggegevens van de EUR (eduroam).

5. De EUR streeft in het kader van handhaving van dit Reglement naar maatregelen die inzage in persoonsgegevens van individuele Medewerkers zo veel mogelijk beperken. De EUR zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

Artikel 3. Intellectueel eigendom en omgang met vertrouwelijke informatie

1. De Medewerker dient vertrouwelijke informatie, waaronder persoonsgegevens, waar deze in het kader van het werk toegang toe heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

2. De Medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van de EUR en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de EUR.

3. De zeggenschap over de informatie van de EUR berust bij de EUR. De Medewerker heeft geen zelfstandige zeggenschap over de informatie, behalve als hem die expliciet is toegekend door de EUR.

4. De Medewerker 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, waaronder onderzoeksgegevens en/of persoonsgegevens, buiten de EUR 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 EUR 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 de nadere voorwaarden.

5. Indien de EUR met betrekking tot het waarborgen van de vertrouwelijkheid voorschriften heeft opgesteld, zullen deze strikt worden nageleefd.

6. De bepalingen in dit artikel gelden in het bijzonder voor de Systeembeheerders, voor wie schending van deze bepalingen, gezien hun bijzondere positie, als een plichtsverzuim wordt aangemerkt.

Artikel 4. Gebruik van communicatie-, computer- en netwerkfaciliteiten

1. De communicatie-, computer- en netwerkfaciliteiten worden aan de Medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is daarom verbonden

aan taken die voortvloeien uit deze functie. Privégebruik van deze faciliteiten is alleen toegestaan zoals bepaald in artikel 2 lid 2 van dit Reglement.

2. Gebruik van de faciliteiten door een Medewerker voor commerciële doeleinden, anders dan in opdracht van, of ten behoeve van de EUR, is alleen toegestaan met Schriftelijke toestemming van de Beheerder, na overleg met de Beheerder die verantwoordelijk is voor de ICT-voorzieningen binnen de EUR.

3. De persoonlijk aan de Medewerker toegekende Toegangscode en eventuele authenticatiemiddelen - zoals smartcards en tokens - zijn strikt persoonlijk en mogen niet worden gedeeld. De Medewerker dient te allen tijde zorgvuldig om te gaan met zijn Toegangscode en eventuele authenticatiemiddelen, en is verantwoordelijk voor het (verdere) gebruik dat daarvan wordt gemaakt. De Medewerker dient alle redelijke maatregelen ter beveiliging van zijn Toegangscode en eventuele authenticatiemiddelen te treffen. De Medewerker stelt bij constatering van misbruik daarvan de Systeembeheerder hiervan onverwijld in kennis.

4. Bij een vermoeden van misbruik kan de Systeembeheerder besluiten per direct het betrokken account ontoegankelijk te (laten) maken.

5. Ten aanzien van het gebruik van de communicatie-, computer- en netwerkfaciliteiten is het de Medewerker met name niet toegestaan:

   a. zich toegang (trachten) te verschaffen tot gegevens van andere gebruikers en tot programmabestanden van computersystemen of deze te wijzigen of te vernietigen, behoudens uitdrukkelijk daartoe verleende Schriftelijke 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 faciliteiten ondermijnen;

   d. pogingen te ondernemen voor de faciliteiten hogere privileges te bemachtigen dan de toegekende privileges;

   e. 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 EUR ter beschikking gestelde programmatuur, databestanden en documentatie te kopiëren of ter beschikking te stellen aan derden, behoudens daartoe verleende Schriftelijke toestemming;

   h. opzettelijk, of door verwijtbaar handelen of nalaten computer-"virussen" op en via de ICT-faciliteiten te introduceren.

6. De Medewerker is verplicht zich te houden aan algemene instructies die door of namens de EUR worden gegeven voor het gebruik van ICT-faciliteiten. Instructies en aanwijzingen die tijdens het gebruik van ICT-faciliteiten door de verantwoordelijke Beheerder van de ICT-voorzieningen binnen de EUR worden gegeven, dienen direct te worden opgevolgd. De EUR kan aan het gebruik van de communicatie-, computer- en netwerkfaciliteiten aanvullende gebruiksregels en voorwaarden stellen.

7. De EUR kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven. De Medewerker zal indien vereist, bij het uitoefenen van de werkzaamheden, van de voorgeschreven systemen of applicaties gebruikmaken en de daarbij gestelde beperkingen en eisen strikt naleven.

8. Het installeren van software op de ICT-faciliteiten van de EUR, of het anders inrichten of instellen van de ICT-faciliteiten, zoals het toevoegen van een routeringsfunctionaliteit, is alleen toegestaan met Schriftelijke toestemming van de betreffende Beheerder en na overleg met de Beheerder die verantwoordelijk is voor de ICT-voorzieningen binnen de EUR. Aan deze toestemming kunnen nadere voorwaarden worden verbonden. De Medewerker dient zich te houden aan de nadere voorwaarden.

9. Het aansluiten van eigen apparatuur, zoals een laptop, tablet of telefoon, is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. De beheerder verantwoordelijk voor de ICT-voorzieningen binnen de EUR kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit Reglement.

10. Het beperkt opslaan van privébestanden of- informatie op systemen van de EUR 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 EUR is echter niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van betreffende systemen.

Artikel 5. Gebruik ICT-communicatiemiddelen en toegang tot bestanden

1. Privégebruik van ICT-communicatiemiddelen, zoals e-mail en telefoon, is alleen toegestaan voor zover bepaald in artikel 2 lid 2 van dit Reglement.

2. Het e-mailsysteem, en de bijbehorende mailbox en e-mailadres worden aan de Medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld en zijn strikt persoonlijk. Gebruik is daarom verbonden aan taken die voortvloeien uit deze functie.

   Verboden bij elk gebruik van communicatiemiddelen (privé of niet) is in ieder geval:

   - het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud, berichten met een (seksueel) intimiderende inhoud, en berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;

- het versturen van ongevraagde berichten aan grote aantallen ontvangers tegelijk, kettingbrieven, of het verspreiden van kwaadaardige software (malware).

3. De Medewerker gebruikt voor privémail bij voorkeur niet het door de EUR verstrekte e-mail adres. De EUR zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.

4. In geval van ziekte, onverwacht langdurige afwezigheid, ontslag, grove nalatigheid of overlijden van de Medewerker, doch uitsluitend als dit in het licht van het belang van de EUR een zwaarwegende reden tot toegang oplevert, is de EUR gerechtigd een vervanger of leidinggevende toegang te verschaffen tot de diensten waar de (e-mail-) bestanden zijn opgeslagen, of een mailbox van de Medewerker.

5. Toegang tot de (e-mail) bestanden, of een mailbox zoals bedoeld in lid 4 zal uitsluitend worden verschaft nadat hiertoe aparte toestemming van het College van Bestuur is verkregen. De vervanger of leidinggevende mag zich 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 of personen die zich op grond van de wet op vertrouwelijkheid kunnen beroepen. Indien de Medewerker geen dergelijke markeringen heeft aangebracht, zal de EUR daar waar mogelijk de betreffende informatie van de Medewerker laten controleren door een onafhankelijke vertrouwenspersoon om zo privéinformatie te herkennen en apart te plaatsen alvorens de vervanger of leidinggevende toegang krijgt. Bij de toegang zal tegelijkertijd, naast de vervanger of leidinggevende, altijd een tweede door de leidinggevende aangewezen persoon aanwezig zijn om de zorgvuldigheid van handelen bij de inzage van bestanden en berichten te borgen. In alle situaties waarin toegang wordt verschaft tot de (e-mail) bestanden of mailboxen van een Medewerker, wordt een onafhankelijke vertrouwenspersoon daar waar mogelijk geïnformeerd.

6. E-mailberichten van bedrijfsartsen, HR-consulenten, leden van de Universiteitsraad onderling, en van een ieder die zich op grond van de wet mag beroepen op vertrouwelijkheid, worden niet gecontroleerd. Deze beperking geldt niet voor geautomatiseerde controle op de veiligheid van de internet- en ICT-faciliteiten.

7. De EUR behoudt zich het recht voor om de toegang tot bepaalde telefoonnummers te beperken. Nummers waaraan hoge kosten verbonden zijn, kunnen worden geweerd.

8. Het gebruik van telefoons die beschikbaar zijn gesteld door de EUR wordt vastgelegd. Deze registratie geschiedt in het kader van het doorberekenen van de kosten voor telefoongebruik binnen de EUR, en om het beheer, de continuïteit, de integriteit, en de beschikbaarheid van de technische infrastructuur of de dienst te waarborgen. De inhoud van gesprekken wordt hierbij niet vastgelegd.

9. Ingeval van opvallend hoge kosten behoudt de EUR zich het recht voor achteraf controle uit te oefenen op het gebruik dat van de telefoonaansluiting is gemaakt. Daartoe kunnen per aansluiting de lijsten van nummers, en de duur van de gevoerde telefoongesprekken worden opgevraagd. Op basis van de uitkomsten kan een gericht onderzoek worden uitgevoerd zoals bedoeld in artikel 9 van dit Reglement.

Artikel 6. Gebruik van internet

1. De toegang tot internet en bijbehorende faciliteiten worden aan de Medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is daarom verbonden aan taken die voortvloeien uit deze functie.
2. Privégebruik van deze faciliteiten is alleen toegestaan zoals bepaald in artikel 2 lid 2 van dit Reglement.
3. Verboden bij elk gebruik (privé of niet) is in ieder geval:
    - sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten, of dit soort materiaal te downloaden;
    - filesharing- of streamingdiensten te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het een storende invloed heeft op de goede werking, waaronder de beschikbaarheid, van het netwerk of andere ICT-faciliteiten van de EUR;
    - 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 naar derden dan wel ter beschikking te stellen zonder toestemming van de rechthebbenden;
    - zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet;
    - opzettelijk en zonder toestemming informatie waartoe men via internet toegang heeft verkregen te veranderen of te vernietigen.

Artikel 7. Gebruik van social media

1. De EUR onderkent de mogelijkheden voor een open dialoog en uitwisseling van ideeën en het delen van kennis van de Medewerker met vakgenoten en derden via social media. Bij werkgerelateerde onderwerpen zal de Medewerker bij gebruik van social media, de EUR, naam en functie bij de EUR aangeven, alsmede dat het een persoonlijk standpunt betreft dat niet overeen hoeft te komen met dat van de EUR. De Medewerker heeft de plicht zich bij gebruik van, en uitingen via, social media als een goed werknemer gedragen.
2. Bestuurders, managers, leidinggevenden en anderen die namens de EUR beleid of strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik van social media, met name als de inhoud verband houdt met hun werk.

3. Dit artikel geldt ook indien de Medewerker vanaf privécomputers of -Internetaansluitingen deelneemt aan social media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

4. Indien een Medewerker een social media-account opzet en/of beheert dat direct aan het werk bij de EUR gerelateerd is, terwijl het op naam van de Medewerker persoonlijk is gesteld, zullen de Medewerker en de EUR bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel en/of de informatie en contacten daarop.

Artikel 8. Monitoring en controle

1. Controle van gebruik van de internet- en ICT-faciliteiten kan slechts plaats vinden in het kader van de doelen genoemd in artikel 2 van dit Reglement. Eventueel verboden gebruik van de internet en ICT-faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

2. Ten behoeve van controle op de naleving van de regels kunnen geautomatiseerd gegevens worden verzameld. Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke Systeembeheerder en worden in beginsel alleen in geanonimiseerde vorm aan overige Beheerders en andere verantwoordelijken beschikbaar gesteld om tot nadere technische maatregelen te kunnen besluiten.

3. Bij vermoeden(s) van overtreding van de regels door een Medewerker of een groep Medewerkers, beperkt controle zich in beginsel tot het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

4. Specifieke maatregelen die de EUR kan nemen ter controle, zijn bijvoorbeeld:

    - controle ter voorkoming van negatieve publiciteit, seksuele intimidatie, of controle in het kader van systeem- en netwerkbeveiliging. Deze controle vindt in beginsel 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. Deze controle 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;

    - controle op basis van klachten of meldingen van derden bijvoorbeeld bij gebruik van auteursrechtelijk beschermd beeldmateriaal, of steekproefsgewijs bij openbaar beschikbaar beeldmateriaal.

Artikel 9. Procedure bij gericht onderzoek

1. Van gericht onderzoek is sprake wanneer verkeersgegevens of andere (persoons-) gegevens betreffende een specifieke Medewerker worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van de voorwaarden en/of uitgangspunten zoals beschreven in dit Reglement door de betreffende Medewerker.

2. Gericht onderzoek vindt uitsluitend plaats na Schriftelijke opdracht van de Beheerder. Het College van Bestuur ontvangt 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.

3. In afwijking van het vorige lid vindt gericht onderzoek naar de beveiliging of integriteit van randapparatuur plaats door Systeembeheerder op basis van concrete aanwijzingen. Een aparte Schriftelijke opdracht van de Beheerder is in dit geval niet nodig. De resultaten van dit onderzoek worden alleen gedeeld met de Medewerker met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit het tweede lid van dit artikel worden gevolgd.

4. Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de internet en ICT-faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de EUR overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist Schriftelijke en met redenen omklede toestemming van het College van Bestuur.

5. Specifieke persoonsgebonden maatregelen die de EUR ter controle kan nemen, zijn bijvoorbeeld:

    - controle op het uitlekken van vertrouwelijke Informatie. Deze controle vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het College van Bestuur;
    - dat de controle op overtreding van het verbod uit artikel 5 lid 3 van dit Reglement plaatsvindt door twee personen, op basis van een specifieke klacht of steekproefsgewijs, e-mailberichten te laten openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud.

6. De Medewerker wordt zo spoedig mogelijk Schriftelijk geïnformeerd door de betreffende Beheerder 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 is alleen toegestaan als informeren het onderzoek daadwerkelijk zou schaden.

7. Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van Medewerker als de Medewerker daarvoor vooraf zijn toestemming heeft gegeven. Toegang zonder toestemming van de Medewerker is slechts toegestaan in dringende gevallen, in geval van een duidelijk vermoeden van schending van dit Reglement, zoals

nader bepaald in dit artikel, of na Schriftelijke toestemming van het College van Bestuur. De Medewerker zal in dat geval achteraf worden geïnformeerd.

Artikel 10. Consequenties van overtreding

1. Bij het niet opvolgen van instructies of aanwijzingen op basis van dit Reglement, 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 in ieder geval een waarschuwing, berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst. Daarnaast kan het College van Bestuur besluiten tot een al dan niet tijdelijke beperking in de toegang tot bepaalde EUR ICT-faciliteiten en toepassingen.

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

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).

4. In aanvulling op het voorgaande is het mogelijk dat de EUR 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 disciplinaire maatregelen worden genomen.

Artikel 11. Intrekking van het oude Reglement

Dit Reglement treedt in plaats van het ‘Reglement voor gebruik van computer- en netwerkfaciliteiten van de Erasmus Universiteit Rotterdam (EUR)’.

Artikel 12. Slotbepaling

1. Dit Reglement treedt in werking op 1 september 2015.
2. Dit Reglement kan door het College van Bestuur worden gewijzigd. Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer de EUR door omstandigheden van buitenaf gedwongen is tot een snellere invoering.
3. De EUR kan dit Reglement wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden zoveel mogelijk voorafgaand aan de invoering aan

de Medewerkers bekend gemaakt. Het College van Bestuur zal feedback van Medewerkers mee in overweging nemen alvorens de wijzigingen in te voeren.

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