Netwerkreglement Wageningen University & Research

(gebruiksreglement ICT-voorzieningen)

Inhoudsopgave

Basis voor het Netwerkreglement

Wageningen University en Research[1] (WUR) stelt internet en ICT-middelen ter beschikking aan studenten, werknemers en andere gebruikers binnen WUR. Deze faciliteiten zijn noodzakelijk om het werk goed te kunnen doen of de studie goed te kunnen volgen. Aan het gebruik hiervan zijn echter risico's verbonden die het stellen van gedragsregels noodzakelijk maken. Tegen de achtergrond van deze risico's mag van alle Gebruikers een verantwoord gebruik van het beschikbare internet en de ICT-middelen van WUR worden verwacht.

Met dit Netwerkreglement wil WUR regels stellen omtrent het gewenste gebruik van de internetverbindingen (inclusief e-mailvoorziening) van WUR en de ICT-middelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van de Gebruiker.

Het gebruik van sociale media (zoals Facebook, LinkedIn en Twitter) is niet meer weg te denken, maar kan zijn weerslag hebben op WUR. Daarom wil WUR ook hier bepaalde regels aan stellen.

WUR is op grond van de Wet naast werkgever ook netwerkbeheerder en als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer. Als instelling voor hoger onderwijs is WUR op grond van de Wet bevoegd om regels te stellen met betrekking tot de goede gang van zaken in de gebouwen en terreinen van de instelling (artikel 7.57h van de wet op het hoger en wetenschappelijk onderzoek (WHW)). Dit Netwerkreglement is naast de Wet ook gebaseerd op artikelen van de CAO Nederlandse Universiteiten en de CAO Stichting Wageningen Research.

Omdat het Netwerkreglement voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van werknemers en studenten is het onderworpen aan de instemming van de centrale ondernemingsraad en de Studentenraad van Wageningen University.

Dit Netwerkreglement sluit aan op andere regelingen zoals: het Reglement bescherming persoonsgegevens, het Informatiebeveiligingsbeleid van WUR en de gebruiksvoorwaarden van SURFnet als connectiviteitsleverancier van WUR.

[1] Wageningen University & Research is een samenwerkingsverband tussen de publiekrechtelijke rechtspersoon Wageningen University en de privaatrechtelijke Stichting Wageningen Research

1 Uitgangspunten

1.1 Het Netwerkreglement stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en de internetverbinding van WUR. 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 privacygevoelige informatie van WUR waaronder verwerkte persoonsgegevens van haar medewerkers en van studenten, ouders en derden;
- bescherming van de intellectuele eigendomsrechten van WUR en derden (bijvoorbeeld respecteren van de licentie-afspraken en researchdata) van toepassing binnen WUR;
- voorkomen van bewuste en herhaalde onterechte handelingen die de goede naam van WUR schade kunnen toebrengen, zie artikel 6, "Gebruik van social media";
- kosten- en capaciteitsbeheersing.

1.2 Beperkt privégebruik van de internetverbinding en de ICT-middelen van WUR is toegestaan mits dit niet storend is voor anderen, de dagelijkse werkzaamheden, of de goede werking van het netwerk van WUR. Het gebruik voor nevenwerkzaamheden of commerciële doeleinden is te allen tijde verboden tenzij apart schriftelijk toestemming daarvoor is verkregen.

1.3 Dit Netwerkreglement geldt voor iedere Gebruiker van het internet en de ICT-middelen van WUR.

1.4 Onder Gebruiker wordt verstaan: een ieder die door middel van een ICT-werkplek of door middel van een computer, laptop/notebook, smartphone e.d., al dan niet via remote access, gebruik maakt van de ICT- of Internetvoorziening (bekabeld of draadloos) die WUR ter beschikking stelt. Tot deze gebruikers behoren in ieder geval Studenten, Werknemers, door WUR ingehuurd personeel, externen (waaronder relaties) en gasten;

1.5 Onder Student wordt verstaan: een ieder die als student staat ingeschreven dan wel onderwijs volgt bij WUR.

1.6 Onder Werknemer wordt verstaan: alle personen als bedoeld in de cao Nederlandse Universiteiten en de cao Stichting Wageningen Research en in dienst zijn van Wageningen University en stichting Stichting Wageningen Research.

1.7 Dit Netwerkreglement geldt ook indien als gast gebruik wordt gemaakt van netwerkvoorzieningen van andere instellingen waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (Eduroam).

1.8 WUR neemt alle redelijke maatregelen die nodig zijn om privacygevoelige data te beschermen door onder andere inzage in privacygevoelige informatie of persoonsgegevens van individuele Gebruikers zo veel mogelijk te beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen. Alle

redelijke maatregelen worden genomen om persoonsgegevens die uitgaande van de doeleinden waarvoor zij worden verwerkt en die onjuist zijn onverwijld te wissen of te rectificeren.

1.9 Door het college van bestuur is de directeur van het Facilitair Bedrijf van WUR als Toezichthouder benoemd als verantwoordelijke voor het beheer van de ICT-voorzieningen en het bewaken van bovenstaande uitgangspunten.

2 Intellectueel eigendom en vertrouwelijke informatie

2.1 De Gebruiker maakt geen inbreuk op de intellectuele eigendomsrechten van WUR en derden, en respecteert de licentieafspraken zoals die van toepassing zijn voor WUR.

2.2 De verantwoordelijkheid voor alle informatie van WUR berust bij WUR. De Gebruiker heeft geen zelfstandige zeggenschap over de informatie behalve voor zover hem die toekomt op basis van de Wet, CAO behoudens overeengekomen afwijkingen daarop, of expliciete schriftelijke toekenning door WUR.

2.3 De Gebruiker dient vertrouwelijke en/of privacygevoelige informatie, waaronder persoonsgegevens, waar hij in het kader van het werk of de studie toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid daarvan te waarborgen.

2.4 De Gebruiker besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Netwerkreglement genoemd indien in het kader van het uitvoeren van werkzaamheden of het volgen van de studie de verwerking en/of opslag van vertrouwelijke informatie buiten WUR noodzakelijk is, zoals via e-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia en eigen apparatuur (USB-apparaten, tablets, smartphones, etc.).
WUR heeft met betrekking tot informatiebeveiliging en het waarborgen van de vertrouwelijkheid voorschriften opgesteld[2]. Gebruiker zal deze voorschriften strikt naleven.

2.5 Het is de Gebruiker 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. Downloaden is in beginsel toegestaan als dit werk- of studie gerelateerd is.

2.6 Deze bepalingen gelden in het bijzonder ook voor ICT-beheerders en functioneel beheerders voor wie schending van deze bepalingen als een zeer ernstig plichtsverzuim wordt aangemerkt gezien hun bijzondere positie.

---

2 https://www.intranet.wur.nl/nl/services/ict/informatiebeveiliging/Documents/8412102050_FBIT_Flyer_Security_netwerk_NL_LR.pdf
of
www.intranet.wur.nl/security

3 Gebruik van ICT-apparatuur en netwerkfaciliteiten

3.1 ICT apparatuur en netwerkfaciliteiten worden aan Gebruikers voor uitoefening van hun functie of studie beschikbaar gesteld door middel van het verlenen van strikt persoonlijke inloggegevens. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2. Verstoring van de wireless netwerken van WUR door middel van radio activiteit dient voorkomen te worden. Gebruikers zijn verplicht mee te werken aan oplossingen ter voorkoming daarvan.

3.2 De Gebruiker dient te allen tijde zeer zorgvuldig om te gaan met aan hem toegekende persoonsgebonden inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). De Gebruiker kan zelf een derde technisch een machtiging verlenen om toegang tot zijn e-mailvoorziening (inclusief agenda) te krijgen. De derde gebruikt hiervoor zijn eigen inloggegevens. Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld of worden gebruikt voor toegang op andere niet-WUR systemen. Bij een vermoeden van misbruik van een wachtwoord kan het ICT-beheer per direct het betrokken account blokkeren.

3.3 Het aansluiten van servers, lokale opslagfaciliteiten (zoals NAS) en actieve netwerkcomponenten (zoals access points en routers) is uitsluitend toegestaan met toestemming van het ICT-beheer en wanneer het de stabiliteit en/of de integriteit van de systemen van WUR niet belasten.
Het ICT-beheer kan aan deze toestemming regels verbinden ter handhaving van dit Netwerkreglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging. WUR kan het gebruik van specifieke software verbieden als daar redenen (bijvoorbeeld uit het oogpunt van beveiliging of het niet kunnen aanpassen ervan voor alle bedreigingen) voor bestaan. Het is in ieder geval verboden om software waarvan de licentie is beperkt tot privégebruik, ten behoeve van werkzaamheden voor WUR te installeren en te gebruiken.

3.4 Het aansluiten van eigen (mobiele) cliënt-apparatuur (zoals: laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. Het ICT-beheer kan conform de aansluitvoorwaarden[3] aan de toegang tot deze voorzieningen regels verbinden, zoals specifieke instellingen, wachtwoordbeveiliging, het verplicht gebruik van een virusscanner of een encryptieprogramma. De bezitter is zelf verantwoordelijk voor een up-to-date beveiliging van zijn persoonlijke apparatuur en te allen tijde verantwoordelijk voor de acties die vanaf zijn persoonlijke apparatuur ondernomen worden.

3.5 Voor mobiele privé apparatuur die op welke wijze dan ook data synchroniseert met WUR geldt dat alle informatie en alle berichten die gemaakt, opgeslagen, ontvangen of verstuurd worden en meegaan in de synchronisatie, beschouwd worden als data van WUR. Als zodanig is deze data aan dezelfde controlemaatregelen onderhevig als alle andere data en apparatuur van WUR.

3.6 Verlies of diefstal van alle apparatuur die data van WUR bevat en van mobiele apparatuur die automatisch synchroniseert met het netwerk van WUR dient altijd direct gemeld te worden bij het ICT-beheer (Servicedesk ICT), ongeacht of de apparatuur eigendom is van WUR of privé eigendom. Het nalaten van deze melding leidt tot de consequenties van overtreding genoemd in artikel 10 van dit Netwerkreglement. Het ICT-beheer zal de synchronisatie stopzetten en (indien mogelijk en noodzakelijk) de gegevens op het apparaat wissen. Op WUR rust de wettelijke plicht om datalekken onverwijld aan de Nederlandse privacy-autoriteit te melden.

[3] https://www.intranet.wur.nl/nl/services/ict/klantenservice/beleid_afspraken/Documents/Aansluitvoorwaarden_WURnet-NL.PDF

3.7 Alvorens beschadigde of defecte (privé) apparatuur die data van WUR bevat ter reparatie of afvoer binnen WUR of daarbuiten wordt aangeboden, dienen alle op het apparaat aanwezige data voor zover mogelijk grondig te zijn gewist.

3.8 Het opslaan van privé-informatie op systemen van WUR is toegestaan, mits deze door de naamgeving van de betreffende bestanden of directories, goed als zodanig herkenbaar is en dit niet leidt tot overbelasting van de opslagcapaciteit van deze systemen of een verstoring van de goede orde op de (digitale) werkvloer. WUR 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 en is niet aansprakelijk voor vermissing of beschadiging van deze informatie.

4 Gebruik van e-mail en andere ICT-communicatiemiddelen

4.1 Het e-mailsysteem en de bijbehorende mailbox en e-mailadres wordt aan de Gebruikers in het kader van hun functie, hun studie, of hun specifieke relatie met WUR beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit de functie, studie of een specifieke relatie met WUR.

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

4.3 Verboden bij elk gebruik (privé of niet) van ICT-communicatiemiddelen 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 of andere ongewenste omgangsvormen zoals genoemd in de Integriteitscode Wageningen University & Research[4];*
- *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 zoals virussen, Trojaanse paarden of spyware te versturen.*

4.4 De Gebruiker gebruikt voor privémail niet het door WUR verstrekte e-mail adres. WUR zal de toegang tot andere e-maildiensten voor privédoeleinden niet blokkeren of specifiek monitoren.

4.5 In geval van ziekte/arbeidsongeschiktheid, overlijden, langdurige afwezigheid, disfunctioneren of grove nalatigheid van de Gebruiker, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang oplevert, is WUR gerechtigd een vervanger of leidinggevende toegang tot de bestanden of de mailbox van de Gebruiker te verschaffen. Toegang wordt echter uitsluitend gegeven indien aangetoond kan worden dat toestemming verkrijgen van bedoelde Gebruiker binnen een redelijke termijn onmogelijk is of indien naar het oordeel van de directie van de organisatie-eenheid of het college van bestuur[5] het bedrijfsbelang zodanig zwaar weegt dat toestemming niet gevergd of afgewacht (spoedeisend belang) kan worden. De aanvraag voor toegang moet in laatstgenoemd geval via de Toezichthouder bij het college van bestuur worden ingediend.

4.6 In aanvulling op het bepaalde in het vorige artikel mag de vervanger/leidinggevende zich geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar, dan wel afkomstig van, een vertrouwenspersoon, bedrijfsarts of HR-consulent. Indien de in artikel 4.5 bedoelde Gebruiker dergelijke markeringen niet heeft aangebracht, zal WUR door inschakeling van een vertrouwenspersoon de betreffende informatie van de medewerker controleren om zo privé-informatie te herkennen en deze apart te plaatsen zodat de van privégegevens ontdane informatie wordt doorgezet naar de vervanger of leidinggevende .

4.7 E-mailberichten en bestanden 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 de geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

---

[4] http://www.wur.nl/nl/Over-Wageningen/Corporate-Governance.htm

[5] College van bestuur: college van bestuur van Wageningen University dan wel het college van bestuur van stichting Wageningen Research

5 Gebruik van internet

5.1 De toegang tot internet en bijbehorende faciliteiten worden aan de Gebruikers in het kader van hun functie, hun studie, of hun specifieke relatie met WUR beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit de functie, studie of specifieke relatie met WUR.

5.2 Privégebruik van deze middelen is alleen toegestaan zoals bepaald in 1.2. Gebruik van het WURnet-account, privé of ten behoeve van studie, mag niet storend zijn voor de goede orde bij WUR en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van WUR of derden of de integriteit en de veiligheid van het netwerk aantasten.

5.3 Onder storend en/of overlast veroorzakend gebruik wordt in ieder geval verstaan:

- het in openbare ruimtes raadplegen of het instellen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het verzenden van berichten met een dergelijke inhoud;
- het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven, het "minen" van bitcoins of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;
- het gebruiken van filesharing- of streaming-diensten wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen of wanneer dit anderen hindert;
- het downloaden van films, muziek, software en overig auteursrechtelijk beschermd materiaal van enige illegale bron of wanneer de Gebruiker weet of had moeten weten dat dit in strijd is met auteursrechten;
- het verspreiden (uploaden) van films, muziek, software en overig auteursrechtelijk beschermd materiaal naar derden zonder toestemming van de rechthebbende(n);
- het verspreiden of anderszins naar derden verzenden van vertrouwelijk informatie en intellectueel eigendom van WUR zonder toestemming van WUR.

5.4 Gebruikers die via het geautomatiseerd inloggen met een WUR-account buiten de gebouwen van WUR gebruik maken van computer- en netwerkfaciliteiten van WUR dienen zich aan dit Netwerkreglement te houden. Voor zover Gebruikers niet zijn ingelogd met het WUR-account maar met een privé-account de (netwerk)faciliteiten van WUR gebruiken, dient dit gebruik plaats te vinden binnen de kaders van dit Netwerkreglement. Voor het overige worden geen beperkingen opgelegd voor privégebruik buiten de gebouwen van WUR. Voor privégebruik geldt dan uitsluitend de Nederlandse wetgeving.

6 Gebruik van sociale media

6.1 WUR ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis met vakgenoten en derden via sociale media (zoals bijvoorbeeld: Facebook, Youtube, Instagram, Skype, Twitter, Yammer of LinkedIn).

6.2 Bestuurders, managers, leidinggevenden en anderen die namens WUR kennis, 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 er bewust van dat medewerkers en ook anderen lezen wat zij schrijven. WUR heeft specifieke regels over de wijze van presentatie en communicatie[6].

6.3 Deze artikelen gelden ook indien vanaf privécomputers of -internetaansluitingen wordt deelgenomen aan sociale media, doch uitsluitend voor zover het gaat om deelname die werk gerelateerd is (of betrekking heeft op WUR).

6.4 Wanneer een social-media-account wordt opgezet dat werk gerelateerd is of betrekking heeft op WUR, maar op naam van de Werknemer persoonlijk is gesteld zullen de Werknemer en WUR bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop.

[6] Zie http://www.wur.nl/nl/Over-Wageningen-UR/goto/Social-Media.htm

7 Monitoring en controle

7.1 Controle van gebruik van de ICT-faciliteiten en internetgebruik vindt slechts plaats in het kader van handhaving van de regels uit dit Netwerkreglement voor de doelen genoemd in artikel 1 en het waarborgen van de goede werking van het internetgebruik. Bij overtreding wordt de Gebruiker door zijn leidinggevende aangesproken op zijn verantwoordelijkheden en verboden gebruik wordt zo mogelijk langs technische weg beperkt of onmogelijk gemaakt.

7.2 Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke ICT-beheerders en worden zo veel als mogelijk enkel in geanonimiseerde vorm aan de Toezichthouder beschikbaar gesteld. Op basis van deze informatie kan tot nadere technische maatregelen worden besloten.

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

7.4 WUR houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de Wet bescherming persoonsgegevens en andere relevante wet- en regelgeving. In het bijzonder beveiligt WUR 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 WUR kan uitvoeren, zijn:

- controle in het kader van systeem- en netwerkbeveiliging (o.a. malware en spam) vindt plaats op basis van filtering van de inhoud op trefwoorden.

- 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;

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

7.6 In het kader van de Helpdesk functie verschaffen ICT-beheerders zich slechts toegang tot accounts van Gebruikers of ter beschikking gestelde apparatuur als de Gebruiker daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Netwerkreglement zoals nader bepaald in dit artikel. De Gebruiker zal, indien redelijkerwijs mogelijk, in dat geval achteraf worden geïnformeerd.

8 Procedure bij gericht onderzoek

8.1 Gericht onderzoek heeft als hoofddoelen:

- het vaststellen of sprake is van oneigenlijk ICT- en Internetgebruik;
- het controleren van gemaakte afspraken;
- het controleren of vertrouwelijke informatie voldoende wordt beschermd en niet openbaar wordt of is gemaakt;
- het voorkomen van bewuste en herhaalde onterechte negatieve publiciteit over WUR via het ICT-netwerk van WUR;
- voldoen aan de verplichting op grond van wettelijke bepalingen om gegevens uit het onderzoek aan derden te verstrekken.

8.2 Van gericht onderzoek is sprake wanneer verkeers- of persoonsgegevens betreffende een Gebruiker wordt vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Netwerkreglement door die Gebruiker.

8.3 Gericht onderzoek naar verkeersgegevens vindt uitsluitend plaats na schriftelijke opdracht van de Toezichthouder en goedkeuring van het college van bestuur. Indien daartoe aanleiding bestaat wordt een afschrift van de resultaten van het onderzoek aan het college van bestuur verstrekt. De leidinggevende ontvangt in elk geval een afschrift van de resultaten. Er wordt strikt vertrouwelijk omgegaan met deze resultaten.

8.4 Bij gebruik in strijd met dit reglement wordt de betreffende Gebruiker zo spoedig mogelijk op zijn gedrag aangesproken door de leidinggevende of de Toezichthouder. De Gebruiker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk kan schaden.

8.5 Gericht onderzoek beperkt zich in eerste instantie tot verkeers- en persoonsgegevens van het gebruik van de ICT-faciliteiten. WUR zal terughoudendheid betrachten bij het verzamelen van deze gegevens.

8.6 Als gericht onderzoek nader bewijs oplevert kan overgegaan worden tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Er vindt dan gericht persoonsgebonden onderzoek naar de Gebruiker plaats. WUR zal zich maximaal inspannen de identiteit van de personen die de kennisneming van de inhoud van communicatie of opgeslagen bestanden uitvoeren, naar de Gebruiker toe geheim te houden.

9 Rechten van de Gebruiker met betrekking tot persoonsgegevens

9.1 De Gebruiker kan zich tot het college van bestuur wenden met het verzoek voor een volledig overzicht van zijn persoonsgegevens zoals door WUR verwerkt in het kader van dit Netwerkreglement. Aan een dergelijk verzoek wordt binnen vier weken voldaan.

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

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. Bij overtreding door studenten kunnen disciplinaire maatregelen worden getroffen op basis van artikel 7.57h Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). Studenten kunnen tegen besluiten in beroep komen bij het College van Beroep voor het Hoger Onderwijs (CBHO). Bij overtreding door werknemers van Wageningen University of Stichting Wageningen Research kunnen tevens disciplinaire maatregelen worden getroffen zoals genoemd in de regelingen op de intranetsite van WUR. Bij overtreding door Gebruikers die niet conform de CAO NU en de CAO Stichting Wageningen Research maar wel onder de verantwoordelijkheid van de colleges van bestuur werken kan de tewerkstelling bij WUR worden beëindigd. Ten aanzien van Gebruikers zoals externen en gasten zal telkens naar passende maatregelen worden gezocht. In alle gevallen zullen de maatregelen zoveel mogelijk in overeenstemming zijn met de zwaarte van de overtreding.

10.2 Disciplinaire 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. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de Gebruiker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

10.3 In afwijking/of aanvulling van het voorgaande is het mogelijk dat het college van bestuur 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 overlast kunnen disciplinaire maatregelen worden genomen.

10.4 Bij ernstige beveiligingsincidenten en calamiteiten is het ICT-beheer gerechtigd faciliteiten te beperken dan wel delen van het netwerk af te sluiten. Bij constatering van strafbare feiten zal door WUR aangifte worden gedaan bij de politie.

10.5 WUR behoudt zich het recht voor eventuele schade, ontstaan door gebruik van faciliteiten of naleving in strijd met dit Netwerkreglement op de Gebruiker te verhalen via het instellen van een privaatrechtelijke schadevergoedingsactie.

11 Slotbepaling

11.1 Dit Netwerkreglement wordt één maal per drie jaar geëvalueerd door het college van bestuur met het medezeggenschapsorgaan.

11.2 WUR kan dit Netwerkreglement met instemming van de medezeggenschap wijzigen als de omstandigheden daartoe aanleiding geven. Wijzigingen worden alleen ingevoerd nadat de studentenraad om voorafgaand advies is gevraagd. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de medewerkers/COR en aan de studenten/studentenraad bekend gemaakt. Het college van bestuur zal feedback van medewerkers en studenten in overweging nemen alvorens de wijzigingen door te voeren. De medezeggenschap van WUR heeft op 11 december 2015 ingestemd met de inhoud van dit Netwerkreglement. Dit Netwerkreglement treedt in werking op 1 januari 2016.

11.3 In gevallen waarin dit Netwerkreglement niet voorziet, beslist het college van bestuur.

11.4 Dit Netwerkreglement zal worden gepubliceerd op de inter-/intranetsite van WUR.