

REGLEMENT VOOR HET GEBRUIK VAN HET DIGITALE NETWERK VAN WAGENINGEN UR (WURnet)

1. Werkingssfeer van dit Reglement

- 1.1 Dit Reglement is van toepassing op een ieder die gebruik maakt van de informatie technologie (IT-)voorzieningen door middel van het WURnet van: Wageningen University (WU), stichting Dienst Landbouwkundig Onderzoek (DLO) en stichting Van Hall Larenstein (VHL), hierna te noemen als het samenwerkingsverband: Wageningen UR (University & Research centre).
- 1.2 WURnet is de verzamelnaam voor alle IT-voorzieningen van Wageningen UR, dus zowel het netwerk, personal computers, servers, telefonieapparatuur en alle andere aangesloten apparatuur met de daarop draaiende systemen.
- 1.3 Het toezicht op het gebruik van de IT-voorzieningen via het WURnet zal overeenkomstig dit Reglement worden uitgevoerd onverminderd de toepassing van andere hiervoor geldende wettelijke en/of door Wageningen UR vastgestelde interne reglementen, richtlijnen en gedragscodes. Toezichthouder namens de colleges van bestuur van respectievelijk: WU, DLO en VHL is de directeur van het facilitair bedrijf (FB) van Wageningen UR.
- 1.4 Indien er zich een situatie voordoet waarin dit Reglement niet voorziet, zal conform het arbeidsrechtelijk kader, het Studentenstatuut, de Wet Bescherming Persoonsgegevens (WBP), en indien het algemene aspecten betreft in overleg met de medezeggenschap, gehandeld worden.

2. Toepasselijkheid en doel van dit Reglement

- 2.1 Dit Reglement bevat algemene gebruiks- en gedragsregels voor alle WURnet-account gebruikers. WURnet-account gebruikers zijn:
 - a. de werknemer van Wageningen UR die vanaf een werkplek van Wageningen UR gebruik maakt van de onder artikel 1.2 genoemde WUR-net vallende IT-voorzieningen. Onder deze subcategorie worden ook begrepen: gastmedewerkers, gedetacheerden, stagiaires en uitzendkrachten;
 - b. de student die vanaf een door Wageningen UR ter beschikking gestelde werkplek gebruik maakt van de onder artikel 1.2 genoemde WUR-net vallende IT-voorzieningen;

Dit Reglement is ook van toepassing op het WURnet-account gebruik voor zover het gebruik buiten de werkplekken van Wageningen UR om plaatsvindt.

- 2.2 Dit Reglement heeft ten doel een juiste balans te creëren tussen het toezicht en de controle op verantwoord gebruik van de IT-voorzieningen en de privacy en rechtsbescherming voor de WURnet-account gebruikers. Het Reglement voorziet daarom in regels over de wijze waarop toezicht en controle op het gebruik plaatsvindt.

3. Voorwaarden en gedragsregels voor het gebruik van de IT-voorzieningen

- 3.1 De IT-voorzieningen, de opslagcapaciteit en de opgeslagen gegevens zijn eigendom van de onderscheiden rechtspersonen die Wageningen UR vormen. De toegang tot het WURnet wordt geregeld door het ter

beschikking stellen aan de gebruiker van strikt persoonlijke en niet overdraagbare identiteitsmiddelen die eigendom blijven van Wageningen UR. De combinatie van gebruikersnaam en toegangscode of een andere authenticatiefaciliteit die de gebruiker autoriseert tot gebruik van het WURnet-account, wordt door Wageningen UR aan de gebruiker verstrekt onder de verplichting van geheimhouding en onder de volgende voorwaarden en gedragsregels.

- 3.2 Elke gebruiker is zelf verantwoordelijk voor de juiste uitvoering van de eigen persoonlijke toegangshandelingen (inloggen) en de geheimhouding van de door Wageningen UR verstrekte of zelf gekozen codes. Het verlenen van een machtiging aan een derde voor de e-mailvoorziening en agenda is wel toegestaan, mits deze toegang geregeld wordt via het bestaande WURnet-account van deze derde.
- 3.3 Het is niet toegestaan de IT-voorzieningen te gebruiken of te exploiteren voor doeleinden anders dan die welke voortvloeien uit hoofde van de functievervulling of studie aan Wageningen UR. Het is toegestaan IT-voorzieningen te gebruiken ten behoeve van en volgens de daarvoor binnen Wageningen UR bestaande procedures goedgekeurde niet van commerciële aard zijnde nevenwerkzaamheden.
- 3.4 Gebruikers mogen de (functionaliteit van) WUR-net niet in gevaar brengen of andere gebruikers hinderen. Het gebruik van het WURnet en alle daarop aangesloten draaiende informatiesystemen dient altijd zodanig te zijn dat de continuïteit, beschikbaarheid en integriteit daarvan niet in gevaar worden gebracht.
- 3.5 Het is niet toegestaan ongewenste e-mail te versturen of authenticatiegegevens van andere gebruikers te achterhalen en/of heimelijk te gebruiken.
- 3.6 Het is zonder schriftelijke toestemming van de Toezichthouder niet toegestaan apparatuur aan het WURnet te koppelen die niet voldoet aan de aansluitvoorwaarden. Deze zijn op te vragen bij de Servicedesk IT.
- 3.7 Het is gebruiker niet toegestaan, anders dan geautoriseerd, toegang te krijgen tot het WURnet dan wel illegaal gebruik te maken van software. Gebruiker wordt geacht geconstateerde zwakke punten in het WURnet te rapporteren aan de Servicedesk IT.
- 3.8 Uitgezonderd freeware, mag software die zich op het WUR-net bevindt niet worden gekopieerd ten behoeve van gebruik op IT-systemen van derden. Het is gebruiker verboden door middel van gebruikmaking van het WURnet-account licentierechten of intellectuele en/of industriële eigendomsrechten te schenden.

4. Misbruik van de ter beschikking gestelde IT-voorzieningen

- 4.1 De gebruiker onthoudt zich bij het gebruikmaken van WUR-net van handelingen die de goede naam van Wageningen UR schade kunnen toebrengen, onrechtmatig of strafbaar zijn. Met inachtneming van de in artikel 3 genoemde voorwaarden en gedragsregels wordt in elk geval als misbruik gekwalificeerd:
 - a. gebruikmaken van WUR-net voor opslag en verwerking van onrechtmatig verkregen informatie of informatie waarvan het bezit strafbaar is;

- b. door middel van het WURnet bewust internetsites bezoeken of e-mailberichten versturen die aanstootgevend (seksueel intimiderend), agressief (racistisch), discriminerend of bedreigend materiaal bevatten;
- c. andere gebruikers via het WURnet lastig te vallen of in hun werkzaamheden te belemmeren door middel van ongewenst gedrag;
- d. niet-publieke informatie of diensten, in welke vorm dan ook opgeslagen op het WUR-net, te ontsluiten aan derden, zonder schriftelijke toestemming van de rechthebbende(n);
- e. gebruik te maken van een lek in de beveiliging van het WURnet en software zonder toestemming te verspreiden, te wijzigen of te verwijderen;
- f. gebruikmaken van het WURnet waarbij privé dan wel commercieel materiaal op het internet wordt gezet en/of bewerkingen van bestaand materiaal worden uitgevoerd die geen enkele relatie hebben met de functieervulling van gebruiker;
- g. Het WURnet voor commercieel gebruik of voor derden te gebruiken of toegankelijk te maken.

Toezichtprotocol

5. Algemeen toezicht door IT-beheerders

- 5.1 IT-beheerders¹ hebben in beginsel dezelfde rechten en plichten als andere gebruikers van het WURnet. De bijzondere positie van de IT-beheerders maakt dat deze gebruikers extra verantwoordelijkheden hebben.
- 5.2 Wageningen UR treft maatregelen ten aanzien van de positie en integriteit van de IT-beheerders en/of de afdeling systeembeheer en het toezicht daarop.
- 5.3 Het is de taak van de IT-beheerders ervoor te zorgen dat gebruikers toegang hebben tot de hardware en de software die de gebruikers nodig hebben voor hun werkzaamheden. De IT-beheerders behandelen informatie over het beheerde systeem en alle in het systeem opgeslagen informatie die tot personen herleidbaar is vertrouwelijk.
- 5.4 De IT-beheerders zijn verantwoordelijk voor de systeem- en netwerkbeveiliging van WUR-net en zorgen daarbij voor installatie en onderhoud van daartoe beschikbare software.
- 5.5 In het kader van beveiligingsincidenten kunnen IT-beheerders tijdelijk beperkingen opleggen aan het gebruik van de toegang tot WUR-net. Gebruikers dienen aanwijzingen van IT-beheerders op te volgen.

6. Controle en Registratie

- 6.1 De Toezichthouder voert ter controle op de naleving van de regels in dit Reglement geen systematische controle uit op het e-mail, netwerk- en telefoonverkeer van gebruikers, maar beperkt zich in beginsel tot het onderzoeken van de verkeersgegevens die niet herleidbaar zijn tot individuele personen. In het kader van dit technisch systeem- en netwerkbeheer vindt, in de vorm van periodieke kopieën, systeemtechnische vastlegging van gebruikers- en verkeersinformatie (log-informatie) plaats. Deze gegevens worden niet langer dan een periode van zes maanden bewaard.

¹ Hieronder valt ook het telecom expense management

- 6.2 In geval van een gerechtvaardigd vermoeden van niet toegestaan gebruik, kan de verkeers- en gebruiksinformatie (gegevens over afzenders, bestemming, datum, tijd, hoeveelheid en omvang), worden bewaard totdat de noodzaak daartoe is vervallen. Op grond van de WBP wordt hiervan melding gedaan bij het College Bescherming Persoonsgegevens.
- 6.3 De Toezichthouder kan in geval van beveiligingsincidenten (malware en spam), niet zijnde technische storingen, IT-beheerders opdragen om specifieke informatie (bestanden, programma's) aan een nader onderzoek te onderwerpen om zo geconstateerde problemen op te kunnen lossen.
- 6.4 Indien het bedrijfsbelang dit vereist en enkel in omstandigheden waar normale toegang tot bestanden via de gebruiker (werknemer) niet mogelijk is, kan de Toezichthouder na schriftelijke opdracht daartoe door het college van bestuur, de in het kader van de functievervulling ontstane bestanden veilig stellen.

7. Gericht onderzoek

- 7.1 Bij gerechtvaardigde vermoedens van handelen in strijd met dit Reglement of geconstateerd misbruik zoals (niet uitputtend) omschreven in dit Reglement, behoudt het college van bestuur van respectievelijk WU, DLO en VHL zich het recht voor door middel van een schriftelijke opdracht aan de Toezichthouder gerichte controle uit te laten voeren op het e-mail, netwerk- en telefoonverkeer van individuele gebruikers.
- 7.2 In gevallen bedoeld in artikel 7.1 zal de Toezichthouder gericht onderzoek doen dat zich in eerste instantie beperkt tot de verkeersgegevens van het gebruik van e-mail, internet en telefoon met als doel:
 - a. Het tegengaan van oneigenlijk en bovenmatig gebruik van IT-voorzieningen;
 - b. Controle op het naleven van gemaakte afspraken over het (verboden) gebruik van IT-voorzieningen;
 - c. De beveiliging van het WURnet en controle of bedrijfsinformatie voldoende wordt beschermd en niet openbaar is gemaakt.De controle op persoonsgegevens over e-mail, internet- en telefoongebruik is een verwerking van persoonsgegevens in de zin van de WBP.
- 7.3 Gebruikers van het WUR-net ten aanzien van wie door de Toezichthouder wordt geconstateerd dat zij zich niet aan dit Reglement houden en/of zich aan misbruik schuldig maken, worden zo spoedig mogelijk door hun leidinggevende of onderwijseenheid op hun gedrag aangesproken en indien van toepassing, schriftelijk gewezen op de consequenties bij voortzetting van het geconstateerde gedrag of misbruik.
- 7.4 Alleen bij zwaarwegende redenen kan de Toezichthouder, na schriftelijke opdracht van het college van bestuur, gericht onderzoek doen naar inhoud van e-mails.
- 7.5 De Toezichthouder zal kennis over de inhoud, vorm en strekking van de berichten en/of bestanden van gebruikers, voor zover niet strijdig met de bedrijfsbelangen van Wageningen UR en behoudens de bedoelde medewerking onder artikel 7.7, niet openbaar maken.
- 7.6 De betrokkene naar wie een onderzoek als bedoeld in artikel 7.2 en 7.4 plaatsvindt, wordt onmiddellijk schriftelijk door het college van bestuur

geïnformeerd over de aanleiding, uitvoering en het resultaat van het onderzoek. De betrokkene wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Het verstrekken van informatie aan de betrokkene wordt uitgesteld als vervolgonderzoek noodzakelijk blijkt te zijn.

- 7.7 Op grond van wettelijke bepalingen kan Wageningen UR worden verplicht medewerking te verlenen aan verstrekking van informatie aangaande gebruik van de IT-voorzieningen door individuele gebruikers van het WUR-net.

8 MAATREGELEN

- 8.1 Bij handelen van een werknemer in strijd met deze regeling kan het college van bestuur één of meer van de volgende maatregelen opleggen:
- Een tijdelijke beperking in de toegang tot bepaalde IT-voorzieningen;
 - Een tijdelijk of definitief verbod op het gebruik van bepaalde IT-voorzieningen;
 - Overige disciplinaire maatregelen als bedoeld in de van toepassing zijnde Cao's.
- 8.2 Indien een persoon bedoeld in artikel 2.1 sub a, niet zijnde de werknemer, werkzaamheden bij Wageningen UR verricht en in strijd met deze Regeling handelt, kan het college van bestuur naast de maatregelen a t/m c tevens de tewerkstelling bij Wageningen UR beëindigen.
- 8.3 Bij het handelen van een student in strijd met de Regeling kan het college van bestuur passende maatregelen nemen gebaseerd op de regels ten aanzien van het gebruik van de Wageningen UR gebouwen en andere voorzieningen. Deze regels zijn, voor zover het studenten betreft, vastgesteld op basis van artikel 7.57h Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). Studenten kunnen tegen besluiten op grond hiervan in beroep komen bij het College van Beroep voor het hoger onderwijs.
- 8.4 Indien wordt geconstateerd dat een WUR-net gebruiker handelt in strijd met strafrechtelijke wettelijke bepalingen in dezen, dan wordt hiervan aangifte gedaan bij de bevoegde autoriteiten. De gebruiker, leidinggevende of onderwijseenheid worden hiervan op de hoogte gesteld.
- 8.5 Wageningen UR kan bij schending van de artikelen 3 en 4 tevens eventuele schade op de betrokken gebruiker verhalen via het instellen van een privaatrechtelijke (schadevergoeding-)actie.

9 Slotbepalingen

- 9.1 Dit Reglement treedt in werking op 1 januari 2011.
- 9.2 Dit Reglement kan met instemming van de medezeggenschap worden gewijzigd. Deze wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de in artikel 2.1 genoemde gebruikers bekend gemaakt.
- 9.3 Dit Reglement wordt éénmaal in de 3 jaar met de medezeggenschap geëvalueerd.

- 9.4 Dit Reglement is met instemming van de medezeggenschap tot stand gekomen bij besluit van het college van bestuur van respectievelijk WU, DLO en VHL d.d. 13 december 2010.