Netwerkreglement Wageningen University & Research (WUR) 2022 voor werknemers en overige medewerkers

SAMENVATTING

Het gebruik van netwerkfaciliteiten, apparatuur, software en gegevens (hierna: de Faciliteiten) is voor (veel van) de werknemers binnen WUR[1] noodzakelijk om hun werk te kunnen doen. Aan het gebruik hiervan zijn echter ook risico's verbonden. WUR heeft daarom een aantal gedragsregels opgesteld, waarvan verwacht wordt dat medewerkers zich hieraan houden wanneer zij gebruik maken van de Faciliteiten. Deze gedragsregels zijn in dit reglement opgenomen.

Dit reglement is van toepassing op het gebruik van de Faciliteiten door werknemers en overige medewerkers van WUR (hierna allen te noemen: medewerkers). Hieronder vallen ook uitzendkrachten, zelfstandigen, gedetacheerden, stagiaires, gastmedewerkers en -onderzoekers, en (buiten)promovendi. Dit reglement is ook van toepassing op het gebruik door medewerkers van WUR van clouddiensten van andere instellingen, middels de federatieve toegang. Medewerkers van andere instellingen, die gebruik maken van de federatieve toegang tot clouddiensten van WUR, vallen onder het reglement van hun eigen instelling. Bij gebruikmaking door studenten van Faciliteiten van Wageningen University geldt het 'netwerkreglement Wageningen University (WU) 2021 voor studenten'. Zijn zij ook medewerker dan bepaalt de hoedanigheid waarin zij gebruik maken van de Faciliteiten, welk reglement leidend is.

WAT IS ACCEPTABEL GEBRUIK VAN DE FACILITEITEN?

Wanneer je gebruik maakt van de Faciliteiten, die door WUR aan medewerkers wordt aanboden ten behoeve van de werkzaamheden, dien je je te houden aan de WUR gedragsregels in het kader van de informatieveiligheid, beschikbaarheid, rechten van WUR en eventuele derden en een goede gang van zaken in de gebouwen en de terreinen van WUR. Deze gedragsregels zijn in dit reglement opgenomen.

De volgende beginselen gelden voor elk gebruik:

I) De Faciliteiten worden niet gebruikt voor activiteiten die in strijd zijn met geldende wetgeving of de goede zeden.

II) De Faciliteiten worden niet gebruikt voor activiteiten die schadelijk, bedreigend of aanstootgevend zijn voor anderen.

III) De beschikbaarheid, integriteit en vertrouwelijkheid van (informatie binnen) de Faciliteiten wordt door het gebruik van de Faciliteiten niet in gevaar gebracht.

De bovengenoemde beginselen worden in het reglement verder uitgewerkt in concrete gedragsregels. Deze gedragsregels geven aan wat acceptabel gebruik is van:

- apparatuur die door WUR ter beschikking wordt gesteld;
- e-mail en andere elektronische communicatiemiddelen die door WUR ter beschikking worden gesteld;
- internetverbindingen die door WUR ter beschikking worden gesteld;

[1] Voorliggend netwerkreglement is van toepassing voor medewerkers van Wageningen University en Stichting Wageningen Research. Deze twee rechtspersonen werken samen onder de naam Wageningen University & Research (verder: WUR).

- gebruik van eigen apparatuur voor werkzaamheden, die de medewerker voor WUR uitvoert;
- privégebruik van de Faciliteiten die door WUR ter beschikking worden gesteld;
- gebruik van sociale media;
- de bescherming van door intellectueel eigendom beschermd materiaal en vertrouwelijke informatie (niet zijnde persoonsgegevens).

Hoe kan WUR het gebruik en de veiligheid van de Faciliteiten controleren?

Voor de veiligheid en beschikbaarheid van de Faciliteiten en om de regels in dit reglement te handhaven, voert WUR controles uit of laat WUR deze door derden uitvoeren. WUR streeft daarbij naar een goede balans tussen verantwoord en veilig gebruik van de Faciliteiten en de privacy van de medewerker. WUR zorgt er daarom voor dat controles door of namens WUR proportioneel zijn: hoe groter de risico's en hoe specifieker de aanwijzingen op een overtreding, hoe ingrijpender en gerichter de controle kan zijn.

Algemene controle

Controle vindt in eerste instantie geautomatiseerd plaats. Dit betekent dat algemene controles worden uitgevoerd op gegevens die zo zijn samengevoegd dat er een totaalbeeld van het gebruik van (een deel van) de Faciliteiten ontstaat. Gegevens die herleidbaar zijn naar een individu worden pas geraadpleegd als een geautomatiseerde melding daar aanleiding voor geeft. Deze gegevens worden alleen gebruikt voor het uitvoeren van de controle op de naleving en handhaving van dit reglement. De gegevens worden verwijderd zodra ze niet meer nodig zijn voor dat doel.

Gericht onderzoek

Van gericht onderzoek is sprake wanneer gegevens over een specifieke medewerker worden vastgelegd naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit reglement door de medewerker. WUR kan dan bijvoorbeeld de inhoud van communicatie of bestanden controleren op daadwerkelijke overtredingen.

Wat zijn de consequenties van overtreding van dit reglement?

Indien het nodig is om schade te voorkomen, kan (een deel van) het gebruik van de Faciliteiten onmiddellijk worden geblokkeerd. Wanneer WUR een overtreding van dit reglement constateert, zal de betrokken medewerker de kans krijgen om een zienswijze te geven, voordat wordt overgegaan tot eventuele disciplinaire maatregelen. Naast disciplinaire maatregelen kan WUR aangifte doen in het geval van strafbare feiten en/of de geleden schade op de overtreder verhalen.

Hoe wordt de privacy van de medewerker beschermd?

WUR leeft bij de uitvoering van dit reglement de geldende wet- en regelgeving, waaronder de Algemene verordening gegevensbescherming (AVG), na. De persoonsgegevens die WUR bewaart naar aanleiding van algemene controle en gericht onderzoek worden passend beveiligd. Alleen medewerkers voor wie dat noodzakelijk is, een zeer beperkte groep, heeft toegang tot de persoonsgegevens. Er wordt altijd naar gestreefd om zo min mogelijk persoonsgegevens te verzamelen om de doelen van dit reglement te bereiken. In de gevallen dat WUR persoonsgegevens verwerkt, hebben zo min mogelijk personen daar toegang toe en worden deze passend beveiligd. Op de verwerking van persoonsgegevens is het Reglement bescherming persoonsgegevens van WUR van toepassing. Zie ook de overzichten verwerkte persoonsgegevens werknemers in loondienst, en medewerkers niet in loondienst aan het einde van dit Reglement.

Contents

1. Doel en toepasselijkheid

In dit reglement zijn de gedragsregels vastgelegd met betrekking tot het gebruik, door medewerkers van WUR (hierna ook: de instelling), van de netwerkfaciliteiten, apparatuur, software en gegevens die WUR ter beschikking stelt voor de werkzaamheden (hierna: de Faciliteiten). Ook wordt beschreven wat de gevolgen van de toepassing van dit reglement voor de medewerkers kunnen zijn. Door in dit reglement aan te geven welke gedragsregels er gelden voor medewerkers die gebruik maken van de Faciliteiten, maakt WUR duidelijk wat acceptabel gebruik is ten aanzien van:

- de beveiliging van systemen en netwerken, bijvoorbeeld tegen schade en misbruik;
- het tegengaan van (online vormen van) seksuele intimidatie, discriminatie en andere strafbare feiten;
- de bescherming van privacygevoelige informatie (waaronder persoonsgegevens);
- de bescherming van bedrijfsvertrouwelijke informatie;
- de bescherming van door intellectuele eigendomsrechten beschermd materiaal, waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen WUR;
- het voorkomen van negatieve publiciteit door onrechtmatig gebruik van de Faciliteiten;
- het voorkomen van spionage;
- de kosten- en capaciteitsbeheersing.

Dit reglement geldt voor iedereen die voor WUR werkzaam is, wanneer deze gebruik maakt van de Faciliteiten die door WUR ter beschikking gesteld worden. Dit reglement geldt dus ook voor uitzendkrachten en zelfstandigen, gedetacheerden, stagiaires, gastmedewerkers en -onderzoekers, en (buiten)promovendi, die zijn ingezet om werkzaamheden voor WUR uit te voeren. Dit reglement geldt ook wanneer u als gast gebruik maakt van de federatieve toegang tot voorzieningen van andere instellingen, waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen instelling. Dit reglement geldt niet voor studenten. Hiervoor is een afzonderlijk Netwerkreglement voor studenten opgesteld. Voor medewerkers die ook student van WUR zijn, gelden beide reglementen. De hoedanigheid waarin de Faciliteiten worden gebruikt bepaalt in dat geval welk reglement leidend is.

Bij indiensttreding, of bij een volgende door het college van bestuur vastgestelde update van dit reglement, wordt iedereen tijdens de eerste inlog met het (nieuwe) account eenmalig aan de hand van een pop up in de gelegenheid gesteld kennis te nemen van de verkorte inhoud van dit reglement. De medewerker dient zich vervolgens akkoord te verklaren alvorens kan worden ingelogd. Medewerkers worden daarnaast gewezen op de vindplek van de geldende versie van dit netwerkreglement.

2. Gebruik van de faciliteiten

WUR verwacht dat medewerkers in beginsel hun eigen verantwoordelijkheid nemen voor een wijze van gebruik van de ter beschikking gestelde Faciliteiten die niet in strijd is met wet- en regelgeving en maatschappelijke fatsoensnormen. In dit hoofdstuk geeft WUR concrete gedragsregels waaraan medewerkers worden geacht zich te houden bij het gebruik van de Faciliteiten.

2.1. ALGEMEEN

Om gebruik te kunnen maken van de Faciliteiten, ontvangt de medewerker persoonsgebonden inloggegevens (wachtwoord, gebruikersnaam en WUR passcode) en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). WUR verwacht van de medewerker dat deze te allen tijde zorgvuldig omgaat met aan hem persoonlijk toegekende of zelf ingestelde inloggegevens en aanvullende authenticatiemiddelen. Persoonsgebonden inloggegevens en aanvullende authenticatiemiddelen mogen niet met anderen worden gedeeld of worden hergebruikt buiten de WUR-omgeving. Bij een vermoeden van misbruik van inloggegevens kan WUR per direct maatregelen nemen of zelfs het betrokken account ontoegankelijk maken.

WUR kan voor onderwijs, onderzoek en bedrijfsvoering bepaalde systemen of applicaties, zoals een elektronische leeromgeving, een e-mailsysteem, (mobiele) applicaties, Cloudvoorzieningen of multimediadiensten zoal berichtendiensten, voorschrijven of verbieden. De whitelist vindt u hier. Daarnaast stimuleert WUR het gebruik van applicaties op de whitelist waarop is te zien voor welke dataclassificatie een systeem geschikt is. WUR verwacht van de medewerker dat zij voor het geven van onderwijs, uitvoeren van onderzoek en ondersteunende processen alleen deze systemen gebruikt en de daarbij gestelde beperkingen en eisen strikt naleeft.

Het installeren van software op door WUR ter beschikking gestelde apparatuur is toegestaan wanneer dat noodzakelijk is voor de uitvoering van de werkzaamheden, mits de medewerker redelijkerwijs mag aannemen dat de software legaal is en niet schadelijk voor de Faciliteiten is. Daarnaast dient het gebruik van zelf geïnstalleerde third-party software – dus buiten de door WUR ter beschikking gestelde Software centre te allen tijde in overeenstemming te zijn met de daarvoor geldende gebruiks- of licentievoorwaarden. De gevolgen van niet-naleving van die voorwaarden komen uitdrukkelijk voor rekening en risico van de betreffende medewerker of diens directie. Voor software die niet noodzakelijk is voor de uitvoering van de werkzaamheden is toestemming van de WUR dienstenleverancier vereist. Deze kan algemene toestemming geven, bijvoorbeeld middels het aanbieden van het kernassortiment: Apparatuur & software - Intranet WUR.

Het aansluiten van actieve netwerkcomponenten (zoals access points, firewalls, routers en wifi-printers) is niet toegestaan zonder toestemming van de dienstenleverancier van het netwerk.

De toegang tot informatie van WUR vanuit andere netwerken dan onze eigen netwerkfaciliteiten (bijvoorbeeld vanuit huis) is alleen toegestaan via beveiligde (wifi)netwerken of de daarvoor door WUR beschikbaar gestelde beveiligde VPN. Toegang tot de informatie is verder alleen toegestaan met door WUR beheerde apparatuur (WURclient danwel MyWorkspace) of met eigen apparatuur mits deze actief wordt beheerd en voorzien is van een deugdelijke door WUR voorgeschreven beveiliging.

2.2. GEBRUIK E-MAIL EN ANDERE COMMUNICATIEMIDDELEN

De medewerker ontvangt bij indiensttreding een e-mailadres, een telefoonnummer en inloggegevens waarmee ingelogd kan worden op het door WUR ter beschikking gestelde e-mailsysteem. Daarnaast kunnen ook andere door WUR ondersteunde systemen ter beschikking worden gesteld om informatie uit te wisselen. Deze elektronische communicatiemiddelen worden aan de medewerker beschikbaar gesteld, zodat deze zijn functie kan uitoefenen. Privégebruik is daarnaast toegestaan, maar onder voorwaarde van het gestelde in dit reglement.

Het is bij gebruik (privé of niet) van door WUR beschikbaar gestelde elektronische communicatiemiddelen verboden om:

- berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud (uitgezonderd wanneer strikt noodzakelijk voor de uitvoering van de werkzaamheden) te verzenden;
- berichten met een (seksueel) intimiderende inhoud of berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld te verzenden;
- ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven of kwaadaardige software (zoals virussen, ransomware of spyware) te verzenden.

- Specifiek ten aanzien van berichtenapps geldt, tenzij expliciet door WUR goedgekeurde enterprise versie (business accountant) en derhalve op de whitelist van WUR voorkomende applicaties[2], dat het niet toegestaan is om in het zakelijk WUR-verkeer andere gratis elektronische beschikbare communicatiemiddelen[3] te gebruiken voor:
- Berichten die persoonsgegevens van medewerkers/studenten bevatten;
- Berichten over beleidsvorming waarvoor een archiveringsverplichting en bovendien een wettelijke verplichting tot openbaarmaking geldt;
- Berichten die onder de WUR dataclassificatie: beschikbaar, integer of vertrouwelijk vallen en kunnen worden geclassificeerd als 'enig', ernstig of ontwrichtend. Zie link data classificatie.

Indien medewerkers behoefte hebben aan een berichtenapp, bijvoorbeeld in communicatie met externen, dan wordt dringend verzocht om de enterprise versie (business account) van MS Teams chat of de Signal app (beiden op de whitelist) te gebruiken voor uitwisseling van niet-vertrouwelijke gegevens.

In geval van ziekte, onverwachte of langdurige afwezigheid of grove nalatigheid van de medewerker, mag WUR een vervanger of leidinggevende toegang tot de mailbox en werk gerelateerde bestanden van de medewerker verschaffen. Er dient een zwaarwegende reden van bedrijfsbelang te zijn voor het verschaffen van de toegang, en de betreffende medewerker zal hierover zo mogelijk worden ingelicht. Geen toegang mag worden verschaft tot: als privé gemarkeerde mappen, als privé herkenbare e-mails, of e-mails die klaarblijkelijk zijn verzonden naar, dan wel afkomstig zijn van een vertrouwenspersoon, (bedrijfs)arts, HR-consulent of in de hoedanigheid van advocaat.

Het is van belang dat de medewerker, indien van toepassing, dergelijke markeringen in de mailbox en bestanden aanbrengt. Heeft de medewerker dit niet gedaan, dan kan WUR een vertrouwenspersoon inschakelen om de betreffende informatie van de medewerker te controleren om zo privé-informatie te herkennen en apart te plaatsen, voordat de vervanger of leidinggevende toegang krijgt.

Na het uit diensttreden of overlijden van een medewerker wordt zo mogelijk na 2 weken het account opgeheven en indien aanwezig, privé e-mailcommunicatie of privé-informatie op gegevensdragers van WUR vernietigd.

2.3. Gebruik internetverbinding

In gebouwen van de WUR heeft de medewerker in het kader van de werkzaamheden toegang tot een door WUR ter beschikking gestelde internetverbinding. Het gebruik

[2] Als voorbeeld MS Teams met chatfunctie
[3] SMS en 'apps' zoals: Whatsapp, Signal, Teams, Telegram, etc.

van een internetverbinding is daarom in beginsel verbonden aan werkzaamheden die voortvloeien uit deze functie.

Het is in ieder geval bij elk gebruik van een door WUR ter beschikking gestelde internetverbinding verboden om:

- sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten (uitgezonderd wanneer noodzakelijk voor de uitvoering van de werkzaamheden);
- filesharing- of streamingdiensten te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de Faciliteiten in gevaar kan brengen;
- films, muziek, software en overig (auteursrechtelijk) beschermd materiaal te downloaden of te verspreiden (versturen of uploaden) naar derden, wanneer de medewerker weet of redelijkerwijs kan vermoeden dat dit in strijd is met op dat materiaal berustende (intellectuele) eigendomsrechten of een verplichting de vertrouwelijkheid van dat materiaal te beschermen;

2.4. Gebruik van de Faciliteiten met privéapparatuur

De medewerker mag eigen apparatuur zoals smartphone, tablet en laptop gebruiken om de werkzaamheden uit te voeren mits er voldoende beveiligingsmaatregelen getroffen zijn. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- gebruik alleen legale software die nog actief onderhouden wordt door de leverancier;
- beveilig het apparaat met een wachtwoord of pincode. Indien mogelijk kan het apparaat ook middels gezichtsherkenning of vingerafdruk beveiligd worden;
- versleutel de opslag van het apparaat;
- stel in dat het apparaat automatisch binnen 5 minuten vergrendelt bij het onbewaakt achterlaten of vergrendel actief zelf het apparaat;
- sla originele (bestanden met) informatie die onder de verantwoordelijkheid van WUR valt op in de ter beschikking gestelde gedeelde omgeving op de servers van WUR;
- Verzend bestanden met persoonsgegevens uitsluitend veilig via Teams of OneDrive;
- bewaar kopieën van (bestanden met) informatie met betrekking tot WUR op de centrale omgeving van WUR;
- houd software up-to-date door het (minimaal maandelijks) controleren en uitvoeren van updates;
- neem voldoende maatregelen tegen virussen of malware door het installeren van antivirussoftware, het up-to-date houden daarvan en het regelmatig scannen van de apparatuur.

WUR behoudt zich het recht voor om beveiligingsmaatregelen, waaronder de bovengenoemde, te controleren bijvoorbeeld door Mobile Device Management (zie paragraaf 3.2.2). Bij het einde van het dienstverband wordt de medewerker geacht alle nog eventueel op de (privé)apparatuur aanwezige informatie die onder verantwoordelijkheid van de WUR valt, te hebben verwijderd.

2.5. Privégebruik van Faciliteiten

Faciliteiten worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Het gebruik hiervan is daarom verbonden aan werkzaamheden die voortvloeien uit deze functie. Het is uitsluitend toegestaan om de Faciliteiten voor

nevenwerkzaamheden te gebruiken indien en voor zover WUR hiervoor schriftelijk toestemming heeft verleend.

Beperkt privégebruik van de Faciliteiten is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of de beschikbaarheid of capaciteit van de Faciliteiten van WUR. Het opslaan van privébestanden of privé-informatie op beperkte schaal, mits niet in strijd met de wet of de maatschappelijke fatsoensnormen, op door WUR ter beschikking gestelde apparatuur, is toegestaan. WUR is niet verplicht om van dergelijke bestanden of informatie reservekopieën te maken, of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.

Het verstrekken van privé e-mailcommunicatie of privé-informatie op gegevensdragers van WUR of het anderszins toegankelijk maken van de e-mailcommunicatie en informatie van een overledene aan nabestaanden staat op gespannen voet met het integriteitsbelang van een overledene en het privacybelang van betrokken communicatiepartners[4]. Uitsluitend overdracht van de gevraagde informatie onder bepaalde waarborgen aan een betrouwbaar en in overleg met WUR geselecteerd onafhankelijk bureau dat de informatie beoordeelt en vervolgens toestemming vraagt aan de communicatiepartners voor vrijgave, behoort tot de mogelijkheden. De aanvragende partij dient dit bureau zelf in te huren en de kosten hiervoor te dragen.

2.6. Gebruik van sociale media

Het gebruik van sociale media voor zaken die raken aan de werkzaamheden of de positie als medewerker voor WUR is toegestaan. Wel dient de medewerker rekening te houden met onze goede naam en iedereen die hierbij betrokken is. Ga dus verantwoordelijk om met het gebruik van sociale media en volg hierbij de social media-richtlijnen van WUR (link: https://intranet.wur.nl/umbraco/media/13562/richtlijnen-social-media-gebruik-door-medewerkers-op-eigen-accounts.pdf en https://intranet.wur.nl/umbraco/media/13558/richtlijnen-social-media-gebruik-offici%C3%ABle-accounts-wageningen-university-research.pdf.

2.7. Omgang met vertrouwelijke en privacygevoelige informatie

De medewerker dient vertrouwelijke en privacygevoelige informatie, waaronder persoonsgegevens waar hij in het kader van het werk toegang toe heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen. De medewerker dient informatie alleen te verwerken in systemen die voldoen aan de eisen die de WUR stelt aan de categorie waarin deze informatie geclassificeerd is. De verwerking van persoonsgegevens in het kader van de werkzaamheden bij WUR vindt plaats in overeenstemming met het Reglement bescherming persoonsgegevens van WUR en het op die basis vigerende beleid.

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

[4] Er is immers het belang te respecteren dat over de e-mailcommunicatie niet meer bekend wordt dan wat overledene en communicatiepartners zelf aan derden (hebben) willen prijsgeven.

Tenzij dat nodig is voor de werkzaamheden, mag de medewerker geen grote hoeveelheden artikelen uit, of substantiële delen van, de bestanden of databases in de digitale bibliotheek downloaden of kopiëren.

Wanneer WUR met betrekking tot het waarborgen van de vertrouwelijkheid en de bescherming van materiaal dat beschermd is door (intellectueel) eigendom nadere voorschriften heeft opgesteld, zal de medewerker deze strikt naleven.

Deze bepalingen gelden in het bijzonder voor systeembeheerders, voor wie schending van deze bepalingen gezien hun bijzondere positie als een zeer ernstig plichtsverzuim wordt aangemerkt. Alle medewerkers die in het kader van toezicht en controle op dit reglement kennis moeten nemen van persoonsgebonden informatie zijn bovendien contractueel gebonden aan een aanvullende geheimhoudingsverplichting, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

3. Controle en monitoring

In dit hoofdstuk wordt beschreven op welke manier de controle op de naleving van dit reglement en de monitoring van de Faciliteiten door WUR plaatsvindt en welke maatregelen er kunnen volgen, wanneer het reglement niet nageleefd wordt.

WUR handelt bij de controle en monitoring van de Faciliteiten binnen de geldende wet- en regelgeving en de beginselen van noodzakelijkheid en proportionaliteit. WUR streeft, in het kader van de controle en monitoring, naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. WUR zal daarbij uitgaan van de juiste balans tussen verantwoord gebruik van de Faciliteiten en de bescherming van de privacy van de medewerkers bij WUR. WUR zal, waar mogelijk, geautomatiseerd controleren of filteren, zonder daarbij inzage te verkrijgen in het gedrag van individuele personen.

3.1. Voorwaarden voor controle

De controle op en de monitoring van het gebruik van de Faciliteiten vindt slechts plaats in het kader van de handhaving van de regels uit dit reglement en uitsluitend voor de doelen zoals genoemd in hoofdstuk 1.

3.1.1 Controle op incidenten

Monitoring en logging
Om de controle uit te kunnen voeren op bedreigingen voor de integriteit, beschikbaarheid en vertrouwelijkheid van WUR-systemen worden doorlopend alle activiteiten en gegevens van alle gebruikers van de Faciliteiten geautomatiseerd verwerkt (monitoring en logging). Deze logging-gegevens worden door automatische processen verwerkt die volgens voorgedefinieerde regels kunnen leiden tot een melding.

Analyse van incidenten
Enkel als uit de voorgedefinieerde regels volgt dat een melding uit het systeem aanleiding geeft tot nader onderzoek (bijvoorbeeld een virusdetectie of afwijkende aanlogpogingen), zal er een verdere analyse uit worden gevoerd van de meldingen door de beheerders van de dienst en/of de (externe) analisten. Onderdeel van de analyse kan zijn het herleiden van de meldingen naar een systeem of persoon. Dit betekent dat de systeembeheerders van WUR en externe analisten op dat moment

toegang kunnen krijgen tot de inhoud van de gegevens en activiteiten van de betreffende medewerker van WUR, voor zover de melding daarop betrekking heeft (bijv. de inhoud van het phishingbericht).

In spoedeisende gevallen en waar noodzakelijk ter voorkoming van (verdere) verwezenlijking van risico's of schade, kunnen deze medewerkers besluiten tot het nemen van technische maatregelen, zoals een blokkering van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken. Het gaat daarbij altijd om tijdelijke maatregelen voor ten hoogste de duur van het incident. Indien de situatie het toestaat wordt vooraf getoetst door de information security officer (ISO) of de maatregel passend is. In spoedgevallen wordt de ISO zo snel mogelijk na het toepassen van de maatregel geïnformeerd.

3.1.2 Controle individu

Wanneer WUR vermoedt dat een medewerker de regels overtreedt, kan gedurende een vastgestelde (korte) periode, gerichte controle worden uitgevoerd in de reeds beschikbare logging zoals genoemd in 3.1.1. Alleen als blijkt dat hiervoor zwaarwegende redenen aanwezig zijn, vindt gerichte controle op de inhoud plaats. De procedure voor gericht onderzoek wordt in paragraaf 3.3. beschreven.

3.2. Uitvoering van algemene controle

Om controle op de naleving van dit reglement en monitoring van de Faciliteiten uit te kunnen voeren, kan WUR enkele specifieke maatregelen treffen, te weten:

- controle ter voorkoming van negatieve publiciteit en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van een geautomatiseerde scan op inhoud, zoals e-mail filtering en virusscanners;
- controle in het kader van kosten- en capaciteitsbeheersing. Als deze bronnen tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;
- controle ter bevordering van de beveiliging van de Faciliteiten en de voorkoming van cybersecurity-incidenten. Deze controle kan bijvoorbeeld plaatsvinden door middel van aanvalssimulaties (zoals red team-acties[5] en pentesten) en social engineering, zoals phishing-campagnes (zie paragraaf 3.2.1);
- installatie van Mobile Device Management (MDM) software, waarmee bepaalde gedragingen kunnen worden gevolgd en waar nodig onmogelijk gemaakt. Een medewerker kan kiezen om MDM te gebruiken om privé apparatuur geschikt te maken voor het uitvoeren van WUR werkzaamheden (zie paragraaf 3.2.2 en 3.3);

3.2.1. Aanvalssimulaties en social engineering

Om kwetsbaarheden in kaart te brengen is het nodig om aanvalssimulaties en social engineering acties uit te voeren op de Faciliteiten en op eigen apparatuur die gebruikt wordt voor het uitvoeren van werkzaamheden voor WUR. Dergelijke aanvalssimulaties en social engineering acties worden alleen uitgevoerd in overleg met en na formele goedkeuring van de ISO. Voor social engineering acties worden aanvullend vooraf de privacyrisico's vastgesteld en zo veel mogelijk beperkt in

[5] Red teaming heeft tot doel het reduceren van risico's en het vergroten van mogelijkheden voor WUR om de juiste en meest efficiënte maatregelen te nemen.

samenspraak met de Functionaris voor gegevensbescherming (F-G) middels een gegevensbeschermingseffectbeoordeling (GBEB, ook wel DPIA genoemd).

Voorbeelden van dergelijke acties zijn red teaming en pentesten. Acties in het kader van aanvalssimulaties en social engineering worden uitgevoerd in lijn met de geldende privacywetgeving. Bij aanvalssimulaties en social engineering kunnen bijvoorbeeld op de volgende manieren persoonsgegevens worden verzameld:

- Social engineering: Een gebruiker kan verleid worden om handelingen uit te voeren of gegevens zoals zijn wachtwoord af te geven;
- Aanvalssimulatie: Er kan worden geprobeerd in te loggen in apparaten of systemen onder een account met hoge privileges waardoor mappen en bestanden (met daarin mogelijk persoonsgegevens en andere gegevens van vertrouwelijke aard) kunnen worden ingezien;

Met de uitvoerende partij worden afspraken gemaakt om te zorgen dat aangetroffen persoonsgegevens vertrouwelijk worden behandeld. Aangetroffen (persoons)gegevens worden niet langer bewaard dan noodzakelijk voor de test. (Persoons)gegevens worden passend beveiligd. Mappen en bestanden die expliciet als 'privé' zijn aangemerkt, worden niet doorzocht, tenzij het redelijkerwijs niet te voorkomen is.

3.2.2. Mobile Device Management

De door WUR beschikbaar gestelde apparatuur en eigen apparatuur die gebruikt wordt voor het uitvoeren van werkzaamheden voor WUR, zal uitgerust worden met een Mobile Device Management (MDM)-agent. MDM biedt WUR de mogelijkheid centraal beheer uit te voeren en zo de beveiliging van apparatuur en gegevens te verbeteren en risico's op bijvoorbeeld ernstige datalekken te elimineren. Middels MDM kan WUR controle uitvoeren of invloed uitoefenen op (het gebruik van) de apparatuur via de onderstaande manieren. Bij elke mogelijkheid geldt dat deze alleen wordt ingezet wanneer dat noodzakelijk en proportioneel is.

De medewerker dient ervoor te zorgen dat privégegevens opgeslagen worden in een map die gemarkeerd is als privé, persoonlijk, persoonsvertrouwelijk of een soortgelijke aanduiding. WUR voert middels de MDM geen controle uit op deze als privé gemarkeerde map. WUR heeft enkel controle over de gegevens die niet als privé gemarkeerd zijn. In het geval van remote wipe zullen echter ook alle privégegevens worden gewist.

De middels het gebruik van MDM verkregen gegevens zullen in geen geval gebruikt worden voor andere doeleinden (zoals het beoordelen en functioneren van de werknemer) dan de beschikbaarheid, integriteit en vertrouwelijkheid van interne gegevens.

3.3. Uitvoering van gericht onderzoek

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere gegevens betreffende een specifieke medewerker, naar aanleiding van concrete aanwijzingen bij WUR van het overtreden van dit reglement, worden vastgelegd en geanalyseerd op daadwerkelijke overtredingen.

WUR kan gericht onderzoek uitvoeren naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit reglement door de medewerker. WUR zal uitsluitend gericht onderzoek uitvoeren na schriftelijke opdracht vanuit de directeur Facilitair bedrijf, na advies te hebben ingewonnen bij de CISO en de Functionaris voor gegevensbescherming (F-G), welke de redenen zal noemen waarom deze

opdracht wordt gegeven. Het college van bestuur ontvangt een afschrift van de opdracht en een geaggregeerde samenvatting van de uitkomst van het onderzoek. Indien het advies van de CISO en/of de F-G afwijkt van de opdracht vanuit de directeur Facilitair Bedrijf, dient het college van bestuur vooraf in te stemmen met de opdracht tot het uitvoeren van het onderzoek. Wanneer het onderzoek geen aanleiding geeft tot verdere maatregelen, wordt de vastlegging geanonimiseerd of vernietigd.

Ook kan WUR, op basis van concrete aanwijzingen zoals genoemd in 3.1.1, gericht onderzoek uitvoeren naar de beveiliging of integriteit van geautomatiseerde systemen of randapparatuur (zoals routers of printers). In afwijking van het hiervoor genoemde, is in dit geval een schriftelijke opdracht van de directeur Facilitair bedrijf niet nodig.

Gericht onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit regelement beperkt zich in eerste instantie tot de data uit reeds beschikbare logging zoals genoemd in 3.1.1 van een individuele gebruiker of systeem. Als gericht onderzoek nader bewijs oplevert, kan WUR overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist opnieuw schriftelijke toestemming van de directeur Facilitair bedrijf, conform het proces zoals hierboven omschreven, welke de redenen zal noemen waarom toestemming wordt verleend.

Enkele specifieke persoonsgebonden maatregelen ter controle die WUR kan uitvoeren zijn:

- de controle op het uitlekken van vertrouwelijke informatie. Dit vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het CvB;
- de controle op verboden gebruik van e-mail en andere elektronische communicatiemiddelen. Dit vindt door twee personen plaats door, op basis van een overtuigend onderbouwde klacht, elektronische berichten te openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud.

De medewerker die verdacht wordt van overtreding van dit regelement wordt binnen drie weken schriftelijk geïnformeerd door de directeur Facilitair bedrijf over de aanleiding, de uitvoering en het resultaat van het onderzoek. De medewerker wordt in de gelegenheid gesteld een zienswijze te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou kunnen schaden en uitsluitend voor de periode die noodzakelijk is om onmiddellijke disciplinaire maatregelen te treffen. Advies wordt vooraf ingewonnen bij de F-G.

Werknemers van WUR, die de directe verantwoordelijkheid voor toezicht en controle op de naleving van dit reglement hebben, verschaffen zich, behoudens in dringende gevallen of bij een duidelijk vermoeden van schending van dit reglement, slechts toegang tot de inhoud van documenten, e-mail of andere bestanden als je daarvoor schriftelijk toestemming hebt gegeven. Je zal in dat geval achteraf worden geïnformeerd over de uitkomst van het onderzoek.

3.4. Waarborging privacy bij controle

Bij het toezicht en de controle op de naleving van dit reglement en het monitoren van de Faciliteiten verwerkt WUR persoonsgegevens van de gebruikers van de Faciliteiten. Dit kan alle persoonsgegevens betreffen die verwerkt worden via de

Faciliteiten, waaronder de inhoud van werkgerelateerde communicatie of opgeslagen bestanden. WUR houdt zich bij het controleren en monitoren op het niveau van persoonsgegevens onverkort aan de AVG en andere relevante wet- en regelgeving, zoals omschreven in dit hoofdstuk.

3.4.1. Maatregelen ten behoeve van privacy

Doelbinding
WUR verwerkt de persoonsgegevens van de medewerker uitsluitend voor de doeleinden zoals omschreven in hoofdstuk 1.

Juistheid
WUR treft, in het kader van de controle op dit reglement, de nodige maatregelen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij verwerkt worden, juist en nauwkeurig zijn.

Dataminimalisatie
WUR heeft het controleproces zo ingericht dat de verwerking van persoonsgegevens beperkt blijft tot wat noodzakelijk is voor de doeleinden zoals genoemd in hoofdstuk 1. Onder meer doordat monitoring van het gebruik van Faciliteiten uitsluitend plaatsvindt via geautomatiseerde verwerking, zonder dat sprake is van geautomatiseerde besluitvorming. Uitsluitend indien sprake is van een concrete melding of bij een gericht onderzoek kunnen beheerders en (externe) analisten toegang krijgen tot de inhoud van internet-, data- en e-mailverkeer van medewerkers.

Opslagbeperking
Persoonsgegevens, die zijn vastgelegd in het kader van toezicht en controle op de naleving van dit reglement, worden zo kort mogelijk bewaard. Alleen wanneer er een redelijk vermoeden bestaat van onrechtmatig gebruik kan deze periode worden verlengd, zolang als nodig is om het onderzoek wat daaruit voortvloeit af te ronden. Zodra een onderzoek is afgerond en dit niet leidt tot disciplinaire maatregelen tegenover een betrokkene, worden de gegevens geanonimiseerd of verwijderd. Wanneer een onderzoek wel leidt tot een disciplinaire maatregel, worden de gegevens bewaard zolang dat noodzakelijk is voor de bewijslast of voor de uitvoering van de disciplinaire maatregel.

Integriteit en vertrouwelijkheid
Daarnaast treft WUR passende technische en organisatorische maatregelen om de bij toezicht en controle op de naleving van dit reglement vastgelegde persoonsgegevens tegen verlies en/of tegen enige vorm van onrechtmatige verwerking te beveiligen. Dit omvat onder andere de volgende maatregelen:

- Via technische, organisatorische en juridische maatregelen waarborgt WUR dat medewerkers en externen geen toegang kunnen krijgen tot de inhoud van (persoons)gegevens, behoudens voor zover bepaald in dit reglement.
- Alleen die medewerkers hebben toegang tot de persoonsgegevens, voor wie toegang noodzakelijk is in het kader van de uitvoering van hun werkzaamheden.
- Alle medewerkers die in het kader van toezicht en controle op dit reglement kennis moeten nemen van persoonsgebonden informatie zijn bovendien contractueel gebonden aan een aanvullende geheimhoudingsverplichting, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
- WUR zal periodiek toetsen of de beheerders van de dienst zich bij de uitvoering van hun werkzaamheden houden aan de voor hen geldende afspraken ten aanzien van autorisatie, doelbinding en geheimhouding.

- WUR zal periodiek toetsen of de partijen met wie de gegevens worden gedeeld zich houden aan de gemaakte afspraken.

3.4.2. Derde partijen

WUR deelt de uit een controle verkregen informatie enkel met derde partijen wanneer dit noodzakelijk is voor de uitvoering van het onderzoek en de uitvoering van de eventuele disciplinaire maatregel. Zo kan WUR de persoonsgegevens doorgeven aan de politie bij een vermoedelijk of geconstateerd strafbaar feit. WUR waarborgt dat waar zij persoonsgegevens deelt met externe organisaties, bindende afspraken worden gemaakt rond de verwerking van die gegevens door die externen die ten minste voldoen aan de uitgangspunten van artikel 28 AVG.

3.4.3. Vertrouwelijke communicatie

Communicatie, zoals e-mailberichten, die herkenbaar is als afkomstig van of verstuurd aan leden van een medezeggenschapsorgaan onderling, (bedrijfs)artsen, de Functionaris voor gegevensbescherming, HR-consulenten, advocaten (in die hoedanigheid) en iedereen die zich op grond van de wet op vertrouwelijkheid mag beroepen, worden niet gecontroleerd bij een gericht onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit regelement. Dit geldt niet voor algemene geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk, met dien verstande dat de inhoud van de communicatie niet ingezien wordt in het kader van de algemene geautomatiseerde controle.

3.4.4. Rechten van betrokkenen, contactgegevens en algemene bepalingen

Het Reglement bescherming persoonsgegevens van WUR is van toepassing op de verwerking van persoonsgegevens in het kader van dit reglement. Klik hier voor meer informatie over de omgang met persoonsgegevens door WUR. De mogelijkheden voor het uitoefenen van de rechten op grond van de AVG vindt u hier.

4. Consequenties van overtreding van dit reglement

Bij handelen in strijd met dit reglement bij het gebruik van de Faciliteiten, kan het college van bestuur, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen, Faciliteiten blokkeren of juridische stappen nemen.

4.1 Disciplinaire maatregelen

Bij het handelen in strijd met dit reglement of de algemeen geldende wettelijke regels, kan het college van bestuur afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, overplaatsing, schorsing en/of beëindiging van de arbeidsovereenkomst. Daarnaast kan het college van bestuur besluiten tot een al dan niet tijdelijke beperking in de toegang tot bepaalde Faciliteiten.

Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens, zoals een constatering door een automatisch filter of automatische blokkade (zie ook 4.2). Voorts worden geen disciplinaire maatregelen getroffen zonder dat de werknemer de gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

4.2 Blokkeren Faciliteiten

Bij een constatering van een overtreding of verdacht gedrag kan WUR, geautomatiseerd of handmatig een tijdelijke blokkade van de betreffende faciliteit invoeren. Indien de situatie het toestaat wordt vooraf getoetst door de ISO of de maatregel passend is. In spoedgevallen wordt de ISO zo snel mogelijk na het toepassen van de maatregel geïnformeerd. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

4.3 Aangifte en schadevergoeding

WUR is te allen tijde gerechtigd om, na gedocumenteerd overleg met de hiervoor meest aangewezen disciplines binnen WUR, aangifte te doen in geval van vermoede of geconstateerde strafbare feiten. Wanneer bij een strafrechtelijk onderzoek om de medewerking van WUR wordt verzocht, zal WUR deze medewerking in lijn met de wet verlenen.

Schade voortvloeiend uit een overtreding van dit reglement kan in opdracht van het college van bestuur door WUR op de overtreder worden verhaald.

5. Slotbepalingen

WUR is als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer, zo volgt uit de wet.

Omdat het reglement voorziet in de verwerking van persoonsgegevens en controle op gedrag of prestaties van medewerkers, is het medezeggenschapsorgaan namens werknemers instemmingsplichtig. Dit orgaan heeft op 28 februari 2022 ingestemd met de inhoud van dit reglement.

Dit reglement wordt in ieder geval elke drie jaar geëvalueerd door het college van bestuur. WUR kan dit reglement bovendien met instemming van het medezeggenschapsorgaan wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de medewerkers bekend gemaakt. Het college van bestuur zal feedback van medewerkers in overweging nemen alvorens de wijzigingen in te voeren.

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