1.2 Regeling ICT-voorzieningen en communicatiemiddelen KNAW

Kader:

In verband met de beveiligings-, juridische en ethische risico's, alsmede de mogelijkheid van uitval van systemen als gevolg van overbelasting geldt onderhavige regeling bij gebruik van door de KNAW ter beschikking gestelde ICT-voorzieningen en communicatiemiddelen, zowel binnen de KNAW-gebouwen als daarbuiten.

Algemeen

Artikel 1.

Begripsbepalingen:

Datalek:	Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging, of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
Derde:	Personen die niet werkzaam zijn ten behoeve van de KNAW
Gebruiker:	Een ieder die, middels een ICT-voorziening en/of communicatiemiddel gebruik maakt van de door de KNAW beschikbaar gestelde KNAW-infrastructuur, ICT- of internetvoorziening. Tot deze gebruikers behoren in ieder geval werknemers, door de KNAW ingehuurd personeel, externe partijen, vrijwilligers, gasten, bezoekers, anderszins personeel niet in loondienst en derden.
Functionaris gegevensbescherming:	Functionaris als bedoeld in de artikelen 37-39 Algemene Verordening Gegevensbescherming
KNAW:	Koninklijke Nederlandse Akademie van Wetenschappen
Werknemer:	De werknemer als bedoeld in artikel 1.1 sub i van de CAO Nederlandse Universiteiten.
Voorziening:	ICT-voorzieningen en communicatiemiddelen zoals: computer- en netwerkapparatuur, (cloud)diensten, systemen, kopieer-, print- en scan-apparaat, mobiele telefoon e.d.

Reikwijdte/toepassingsbereik

Artikel 2.

1 De regeling is van toepassing op een ieder die, middels een ICT-voorziening en/of communicatiemiddel – al dan niet op terrein van de KNAW – gebruik maakt van de door de KNAW beschikbaar gestelde ICT- of internetvoorziening.
2 Het voorgaande lid laat onverlet dat werknemers zich ook bij het gebruik van niet door de KNAW ter beschikking gestelde voorzieningen respectievelijk zonder gebruikmaking van KNAW-infrastructuur als een goed werknemer dienen te gedragen, als bedoeld in artikel 1.8, tweede lid, CAO Nederlandse Universiteiten, en zich niet schuldig mogen maken aan overtreding van artikel 8 van deze regeling.

Voorschriften met betrekking tot gebruik

Artikel 3.

1 De verstrekte voorziening dient te worden gebruikt ten behoeve van de functievervulling.
2 Het door de KNAW toegekende account met e-mailadres en de postbus met bijbehorende loginnaam en wachtwoord zijn strikt persoonlijk. De gebruiker mag deze toegangscodes in beginsel niet afgeven en moet ze geheimhouden in verband met de bescherming van de persoonlijke levenssfeer alsmede het voorkomen van misbruik door derden, tenzij sprake is van een situatie als bedoeld in het vierde lid.
3 De gebruiker is verantwoordelijk voor alle gebruik van zijn voorziening, tenzij aannemelijk kan worden gemaakt dat de toegangscode onrechtmatig door een ander is verkregen. Een gebruiker die weet of vermoed dat zijn toegangscode door een derde en of collega is verkregen dient dit onverwijld te melden aan de Servicedesk van de ICT afdeling, Computer Security Incident Response Team (CSIRT) en de functionaris gegevensbescherming en zijn/haar wachtwoord te wijzigen zodat het risico op een datalek en/of ander misbruik van de voorziening wordt geminimaliseerd.
4 De gebruiker kan in geval van afwezigheid een andere gebruiker - via e-mailsoftware of schriftelijk - machtigen om inzage te hebben in zijn postbus en eventueel berichten te behandelen en/of te beantwoorden namens de gebruiker. Deze machtiging dient het doel te hebben om spoedeisende kwesties af te handelen. Indien de machtiging niet langer nodig is, dient deze te eindigen.
5 De gebruiker kan bij wijze van delegeren in hiërarchische lijn in het dagelijks gebruik een andere gebruiker – via e-mailsoftware of schriftelijk – machtigen om inzage te hebben in zijn postbus en eventueel berichten te behandelen en/of te beantwoorden namens de gebruiker.
6 In geval van toepassing van lid 4 wordt, voor zover de gebruikte software hiertoe de mogelijkheid biedt, een 'out of office reply'/'afwezigheidsassistent' ingesteld met een alternatief voor het desbetreffende e-mailadres.

Artikel 4

1 De ICT afdeling willigt enkel een verzoek van de gebruiker tot het resetten van zijn/haar wachtwoord in, indien:
   - de gebruiker zich fysiek kan legitimeren; of
   - het verzoek via de leidinggevende en/of contactpersoon is ingediend.
2 Indien de ICT afdeling daarvoor een applicatie beschikbaar heeft gesteld, kan de gebruiker zelf zijn wachtwoord resetten.

Artikel 5

1 In geval van een zwaarwegend bedrijfsbelang kan een account, device, netwerkverbinding of anderszins een ICT-voorziening en/of communicatiemiddel, indien dit noodzakelijk en proportioneel is, direct worden geblokkeerd. De algemeen directeur dan wel instituutsdirecteur, de Functionaris gegevensbescherming en de gebruiker worden hiervan zo snel mogelijk op de hoogte gesteld.
2 Van een zwaarwegend bedrijfsbelang is in ieder geval sprake in geval van:
   a. (het vermoeden van) een datalek waarbij de inbreuk op de rechten en vrijheden van betrokkenen een hoog risico met zich meebrengt en dit risico aanzienlijk kan worden beperkt door het blokkeren van het account;
   b. (het vermoeden van) een hack waarbij het op het risico afgestemde beveiligingsniveau niet langer kan worden gewaarborgd.
3 De blokkering wordt opgeheven wanneer met voldoende mate van zekerheid kan worden vastgesteld dat de omstandigheid die noopt tot het zwaarwegende bedrijfsbelang dusdanig is beperkt dat blokkering van het account niet langer noodzakelijk is.

Artikel 6

1 Kopieën van gedeelde mailboxen worden in geval van uitdiensttreding niet aan de gewezen werknemer dan wel gebruiker verstrekt.

2 In geval een ander, bijvoorbeeld de leidinggevende of een collega, inzage of een kopie van de mailbox, anderszins digitale gegevens of toegang tot het account van de gewezen werknemer of gebruiker wenst, wordt dit enkel verstrekt na toestemming van de betreffende gewezen werknemer of gebruiker.

Artikel 7.

1 Als dit noodzakelijk is voor een goede bedrijfsvoering en het bedrijfsbelang prevaleert boven het belang van de werknemer tot bescherming van zijn persoonlijke levenssfeer, kan een wachtwoord op last van de algemeen directeur dan wel instituutsdirecteur worden gereset. Het nieuwe wachtwoord kan aan het afdelingshoofd dan wel de formeel leidinggevende worden verstrekt. De werknemer wordt hiervan zo spoedig mogelijk op de hoogte gebracht. Het is het afdelingshoofd dan wel de leidinggevende niet toegestaan het wachtwoord te delen.
2 In geval van afwezigheid van de gebruiker kan indien:
- het belang van de bedrijfsvoering dit vordert;
- als er geen andere mogelijkheid meer openstaat; en
- het bedrijfsbelang prevaleert boven het belang van de werknemer tot bescherming van zijn persoonlijke levenssfeer;

diens leidinggevende na instemming van de algemeen directeur dan wel instituutsdirecteur en na advies van de jurist arbeidsvoorwaarden en rechtspositie via de systeembeheerder de mailbox voor hem zichtbaar laten maken, teneinde kennelijk bedrijfsrelevante e-mails naar de juiste personen door te sturen. De betreffende gebruiker wordt hiervan door de leidinggevende of het afdelingshoofd zo spoedig mogelijk, indien mogelijk per e-mail en anders per brief, op de hoogte gesteld.
3 De privéberichten en persoonlijke digitale gegevens van de werknemer worden niet met derden gedeeld, tenzij dit op grond van wet- en regelgeving en/of deze Regeling ICT is bepaald dan wel de derde of de KNAW hierdoor uitzonderlijk wordt benadeeld of dit leidt tot onredelijke gevolgen.

Restricties

Artikel 8.

1 Het bekijken, bewust downloaden en/of verspreiden van discriminerend, racistisch, bedreigend, intimiderend, pornografisch of anderszins seksueel getint, aanstootgevend of beledigend materiaal is niet toegestaan; dit wordt beschouwd als een ernstige afwijking van betamelijk gedrag. Dit is slechts anders indien voorgaande uitdrukkelijk is toegestaan door de leidinggevende voor het specifieke doel: wetenschappelijk onderzoek of collectievorming.
2 Een beperkt gebruik van de ICT-voorziening en/of communicatiemiddel voor privédoeleinden is toegestaan, mits niet storend voor anderen en met inachtneming van onderhavige regeling.
3 Het via een voorziening zenden van berichten en/of ontplooien van activiteiten die de goede naam en eer van de KNAW kunnen schaden is niet toegestaan.
4 Het verrichten van frauduleuze handelingen is niet toegestaan.
5 Gebruik dat schadelijk kan zijn voor de ongestoorde werking van de aangesloten netwerken of systemen is niet toegestaan.
6 ICT-gebruik dat leidt tot schending van een licentie- en/of auteursrecht van de KNAW is niet toegestaan. Licentievoorwaarden mogen niet zonder toestemming van ICT Services worden geaccepteerd.

SURFnet

Artikel 9.

1 Gebruik van de digitale infrastructuur van SURF door derden is enkel toegestaan als aan de voorwaarden van de Regeling derdenverkeer SURFnet is voldaan.
2 Lid 1 is niet van toepassing op toegestaan gebruik van voorzieningen door bezoekers van bibliotheken, studiezalen e.d. van KNAW-instituten.

Nadere voorschriften

Artikel 10.

1 De algemeen directeur dan wel instituutsdirecteur is bevoegd - met inachtneming van onderhavige regelingen relevante wet- en regelgeving - met instemming van de Onderdeelcommissie ter nadere concretisering van onderdelen van deze regeling voorschriften te geven voor uitsluitend:
   - de collectieve afsluiting van toegang tot bepaalde websites en/of telefoonnummers;
   - het gebruik van online radio en/of TV en video e.d. indien dit interfereert de uitvoering van de werkzaamheden.
2 Het is de algemeen directeur dan wel instituutsdirecteur toegestaan om zonder instemming van de Onderdeelcommissie over te gaan tot het (laten) afsluiten van toegang tot bepaalde websites en/of telefoonnummers indien dit noodzakelijk is vanwege informatie-, technische-, of anderszins beveiligingsredenen.

Registratie en controle

Artikel 11.

1 Alle handelingen van gebruikers met betrekking tot gebruikmaking van een voorziening binnen de KNAW kunnen worden gelogd.
2 Ter voorkoming van beheer- en capaciteitsproblemen en ter voorkoming van misbruik vindt met inachtneming van de Algemene Verordening Gegevensbescherming automatische registratie van technische onregelmatigheden en het persoonsgerichte gebruik van de voorzieningen en het netwerkverkeer plaats. Bij deze automatische registratie dienen de beginselen van proportionaliteit en subsidiariteit in acht te worden genomen. Wanneer op grond van het gerechtvaardigd belang persoonsgegevens worden verwerkt, dient de belangenafweging te worden gedocumenteerd.
3 Automatische registratie gericht op het persoonsgerichte gebruik van voorzieningen en netwerkverkeer als bedoeld in het eerste lid vindt onder andere plaats door het monitoren van (vaste) telefoniegegevens voor het netwerkverkeer en budgetoverschrijdingen.
4 Met inachtneming van de Algemene Verordening Gegevensbescherming en voor zover nodig na inwinning van advies van de Functionaris Gegevensbescherming van de KNAW kunnen door netwerkbeheer na instemming van de algemeen directeur dan wel instituutsdirecteur via geautomatiseerde processen gegevens over het persoonsgerichte gebruik van voorzieningen verzameld en verwerkt worden ten behoeve van anonieme trendanalyses over het gebruik.
5 Verdergaande controle van persoonsgerichte verkeersgegevens door netwerkbeheer kan met instemming van de algemeen directeur dan wel instituutsdirecteur en na inwinning van advies van de Functionaris Gegevensbescherming plaatsvinden in verband met een verdenking van gebruik dat schadelijk kan zijn voor de aangesloten netwerken of systemen, indien noodzakelijk in verband met het schaderisico tot op het niveau van de fysieke machine en inlognaam. In geval van een crisissituatie waarbij de instemming van de algemeen directeur dan wel instituutsdirecteur en het advies van de Functionaris gegevensbescherming niet kan worden afgewacht, kan verdergaande controle plaatsvinden.
6 De persoonsgegevens die als gevolg van dit artikel worden verwerkt, worden conform artikel 5, eerste lid, sub e Algemene Verordening Gegevensbescherming niet langer bewaard dan noodzakelijk.

Artikel 12.

1 Uitsluitend met toestemming van de algemeen directeur dan wel instituutsdirecteur, zo nodig de Functionaris gegevensbescherming geconsulteerd hebbend, kan in verband met een concrete verdenking van:
   - overtreding van een norm zoals genoemd in deze regeling of
   - gebruik dat schadelijk kan zijn voor de aangesloten netwerken of systemen

met inachtneming van lid 3 van dit artikel controle en vervolgonderzoek naar de inhoud plaatsvinden van het gebruik van voorzieningen door individuele gebruikers indien er geen minder vergaand middel voorhanden is en het middel in verhouding staat tot de ernst van de vermoedelijke overtreding/schadelijke gebruik.

2 Indien geen sprake is van schade als bedoeld in lid 1 van dit artikel start het onderzoek met het steekproefsgewijs controleren van e-mail en/of internetgebruik van de gebruiker. Indien de steekproeven daartoe aanleiding geven vindt vervolgonderzoek plaats met inachtneming van lid 3 van dit artikel.
3 Controle en vervolgonderzoek vinden plaats op zo min mogelijk op de persoonlijke levenssfeer van gebruiker inbreuk makende wijze onder gebruikmaking van de verschillende niveaus van controle, zoals: filtering op hoeveelheid capaciteit, filtering op woordgebruik, filtering op subject line, filtering op bepaalde woorden in e-mailverkeer enz.
4 Controle en vervolgonderzoek vinden plaats dooreen gekwalificeerde ICT beheerder, onder leiding van het afdelingshoofd van de ICT afdeling.
5 Voorafgaand aan controle wordt de desbetreffende gebruiker namens de algemeen directeur dan wel instituutsdirecteur van het voornemen op de hoogte gesteld, tenzij noodzakelijk onderzoek hierdoor zou worden geschaad.
6 De algemeen directeur dan wel instituutsdirecteur stelt de gebruiker schriftelijk op de hoogte van de bevindingen van de controle/het vervolg onderzoek.
7 E-mailberichten dan wel anderszins digitale gegevens van, bedrijfsmaatschappelijk werker en andere werknemers in een vertrouwensfunctie zijn uitgesloten van gericht onderzoek als bedoeld in dit artikel. Uitsluitend bij een uitvoerig onderbouwde verdenking dat deze regeling wordt overtreden kan de algemeen directeur dan wel instituutsdirecteur anders besluiten.
8 E-mailberichten dan wel anderszins digitale gegevens van OR- en OC-leden in functie, waaronder tevens de ambtelijk secretaris van de Ondernemingsraad, mogen niet worden onderworpen aan gericht onderzoek. Uitsluitend bij een uitvoerig onderbouwde verdenking dat deze regeling wordt overtreden kan de algemeen directeur dan wel de desbetreffende instituutsdirecteur anders besluiten indien de aanleiding van dit onderzoek niet is gelegen in de uitvoering van hun OR- en/of OC-functie.
9 Verzoeken van politie en/of justitie om inzage of nader onderzoek van ICT-gebruik van een specifieke gebruiker kan uitsluitend worden gehonoreerd na toestemming van de algemeen directeur dan wel instituutsdirecteur en in uitzonderlijke situaties door het bestuur van de KNAW.

Artikel 13.

1 Indien er sprake is van een (vermoeden van een) datalek dient dit direct te worden gemeld bij de Functionaris gegevensbescherming, dan wel een ander contactpersoon conform de interne procedure ‘melden datalek KNAW’ en, indien het datalek ICT-gerelateerd is., eveneens bij het Computer Security Incident Response Team (CSIRT).
2 De Functionaris gegevensbescherming dan wel de Afdeling Juridische Zaken beoordeelt of de KNAW verplicht is het datalek te melden bij de Autoriteit Persoonsgegevens. De melding dient bij de Autoriteit Persoonsgegevens door de Functionaris gegevensbescherming, indien mogelijk, binnen 72 uur te geschieden.

Maatregelen en sancties

Artikel 14.

1 Werknemers van wie is geconstateerd dat zij zich niet aan de voorschriften houden, worden door de leidinggevende op hun gedrag aangesproken.
2 Overtreding van de voorschriften in deze regeling kan voor de werkgever aanleiding vormen tot het nemen van rechtspositionele maatregelen.
3 Gebruikers van wie is geconstateerd dat zij zich niet aan de voorschriften houden, worden door hun functioneel of formeel leidinggevende of opdrachtgever aangesproken op hun gedrag. Desgewenst stelt deze tevens de formele werkgever op de hoogte van de overtreding van de regeling.

4 Afhankelijk van de aard van de overtreding kan de algemeen directeur dan wel instituutsdirecteur besluiten (de formele werkgever te verzoeken) deze gebruiker, anders bedoeld dan in het eerste en tweede lid, niet meer werkzaam te laten zijn ten behoeve van de KNAW en in geval van gastvrijheidsverlening deze gemotiveerd te beëindigen.

Artikel 15.

De algemeen directeur dan wel instituutsdirecteur beslist in situaties waarin deze regeling niet voorziet.

Slotbepalingen

Artikel 16.

Eventuele door instituten uitgevaardigde interne richtlijnen zijn per ingangsdatum vervallen.

Artikel 17.

Deze regeling treedt op 1 januari 2020 in werking, onder intrekking van de Gedragscode ICT-voorzieningen en communicatiemiddelen d.d. 21 januari 2010.