Reglement verantwoord netwerkgebruik gasten

Versiebeheer

Versie	Status	Datum	Auteur	Omschrijving
0.9	Concept	01-11-2023	Niels Dutij	1e Draft op basis van Reglement verantwoord netwerkgebruik medewerkers
1.0	Definitief	09-11-2023	Niels Dutij	Final versie

Vastgesteld door het ROC Nijmegen:

Versie	Datum	Naam	Functie
1.0	09-11-2023		

Inleiding

Het gebruik van netwerkfaciliteiten en ICT-middelen (hierna: de Faciliteiten) is voor de werknemers binnen ROC Nijmegen (hierna: de Instelling), noodzakelijk om hun werk goed te kunnen doen. De Instelling werkt ook met toegang tot de Faciliteiten voor gasten, bijvoorbeeld samenwerkingspartners en andere derden die toegang nodig hebben tot de Faciliteiten van de Instelling.

Gasten dienen ook de gedragsregels van de Instelling te volgen. Er kan controle plaatsvinden op gastgebruikers op de naleving van dit reglement door de Instelling. Bij aanleiding kan de Instelling maatregelen en sancties treffen, waaronder blokkeren van de gast en het in rechte afdwingen van onrechtmatig gedrag.

Hoofdstuk 1: Algemeen

In dit Reglement voor de Faciliteiten geeft de Instelling aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van Faciliteiten en wat dit voor de werknemers in de dagelijkse praktijk betekent. Hieronder volgen het doel van dit Reglement en de toepasselijkheid.

Artikel 1. Doel

Het Reglement stelt regels ten aanzien van het gebruik van Faciliteiten door gasten. 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 privacy gevoelige informatie waaronder en persoonsgegevens van de Instelling en haar werknemers, en van studenten en ouders;
- bescherming van vertrouwelijke informatie van de Instelling en haar werknemers, en van studenten en ouders;
- bescherming van de intellectuele eigendomsrechten van de Instelling en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de Instelling;
- kosten- en capaciteitsbeheersing.

Artikel 2. Toepasselijkheid

2.1. Dit Reglement geldt voor eenieder die als gast toegang krijgt tot de Faciliteiten die door de Instelling ter beschikking gesteld worden.

2.2. Dit Reglement geldt ook indien u als gast gebruik maakt van netwerkvoorzieningen van andere instellingen, waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (Eduroam).

2.3. Dit Reglement wordt getoond bij het inloggen voor de eerste keer op de faciliteiten van de Instelling.

Artikel 3. Gebruik van faciliteiten

3.1. Om gebruik te kunnen maken van Faciliteiten van de Instelling, gebruikt de gast de persoonsgebonden inloggegevens (wachtwoord en gebruikersnaam) van de eigen instelling of bedrijf. De gast dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen. Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van de inloggegevens kan systeembeheer per direct het betrokken account ontoegankelijk maken.

3.2. De Instelling kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een Elektronische Leeromgeving, een e- mailsysteem, (mobiele) applicaties (apps), cloudvoorzieningen of multimediadiensten. De gast zal voor het delen van informatie, lesmateriaal of het uitvoeren van onderzoek alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.

3.3. Het installeren van software op de ICT-middelen/Faciliteiten is niet toegestaan zonder aparte toestemming van systeembeheer. Ook het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van systeembeheer.

3.4. Het gebruik van de Facilteiten (waaronder tevens het gebruik van webapplicaties) van de Instelling vanuit andere netwerken of vanuit huis is alleen toegestaan via beveiligde (wifi)netwerken met apparatuur van de Instelling of met eigen apparatuur mits deze apparatuur voldoet aan de gangbare beveiligingseisen.

3.5. Het gebruik van de Faciliteiten door de gast ten behoeve van nevenwerkzaamheden is niet toegestaan.

3.6. Bij de uitvoering van de taken, die aan de gast zijn toegekend, kan deze persoonsgegevens verwerken. Alle verwerkingen van persoonsgegevens, die de gast in het kader van zijn taken uitvoert, al dan niet met behulp van de Faciliteiten (waaronder voorgeschreven systemen of applicaties) van de Instelling, dienen te voldoen aan de vereisten onder de AVG en dienen te passen binnen de reguliere taken.

Artikel 4. Gebruik van internet en het netwerk

4.1 Het verwerken van persoonsgegevens van de Instelling op het internet, in het kader van de uitvoering van de taken, die aan de gast zijn toegekend, is alleen toegestaan, indien dit past binnen de reguliere taken en getoetst is aan de AVG.

4.2 Verboden bij elk gebruik (privé of niet-privé) is echter:

- sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- filesharing- of streamingdiensten (zoals Netflix) 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 van enige illegale bron of wanneer de gast daadwerkelijk weet dat dit in strijd met auteursrechten is;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

Artikel 5. Privégebruik van faciliteiten

5.1. Privégebruik van faciliteiten is door gasten nooit toegestaan.

Artikel 6. Intellectueel eigendom en vertrouwelijke informatie

6.1. De gast dient vertrouwelijke informatie en privacygevoelige informatie waaronder persoonsgegevens waar hij in het kader van de taken toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

6.2. De gast maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Instelling.

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

6.4. De gast besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van de taken de verwerking van vertrouwelijke informatie buiten de Instelling noodzakelijk is zoals via e-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen apparatuur (USB-sticks, Tablets, etc.). Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid en de bescherming van intellectueel eigendom voorschriften heeft opgesteld zal de gast deze strikt naleven.

Hoofdstuk 2: Controle en disciplinaire maatregelen

Dit hoofdstuk beschrijft op welke manier de controle op de naleving van dit Reglement door de Instelling plaatsvindt en welke maatregelen er kunnen volgen, indien het Reglement niet nageleefd wordt.

De Instelling handelt bij de controle op het gebruik van de Faciliteiten, die door de Instelling ter beschikking worden gesteld voor de uitvoering van de taken van de gast, binnen de geldende wet- en regelgeving.

De Instelling streeft in het kader van de controle en handhaving van dit Reglement naar maatregelen, die inzage in privacygevoelige informatie of persoonsgegevens van individuele gasten zo veel mogelijk beperken. De Instelling zal daarbij uitgaan van de juiste balans tussen verantwoord gebruik van Faciliteiten en de bescherming van de privacy van eenieder, die aan de Instelling verbonden is. Zij zal, waar mogelijk, slechts geautomatiseerd controleren of filteren, zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

Artikel 7. Voorwaarden controle

7.1. Controle van gebruik van de Faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement voor de doelen zoals genoemd in artikel 1. Verboden gebruik van de Faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

7.2. Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens, die niet herleidbaar zijn tot identificeerbare personen. De gegevens, die uit een dergelijke controle voortkomen, zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten.

7.3. Bij vermoedens van overtreding van de regels kan gedurende een vastgestelde (korte) periode, gerichte controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats. De procedure voor gericht onderzoek verloopt, zoals beschreven in artikel 12.

7.4. De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de Algemene verordening gegevensbescherming (AVG) en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

7.5. Persoonsgegevens die zijn vastgelegd in het kader van toezicht en controle worden bewaard voor een zo kort mogelijke periode. Enkel indien er een redelijk vermoeden bestaat van onrechtmatig gebruik kan deze periode worden verlengd. Zodra een onderzoek is afgerond en niet leidt tot maatregelen tegenover een betrokkene, worden de gegevens verwijderd.

Artikel 8. Uitvoering controle

8.1. Enkele specifieke maatregelen ter controle die de Instelling kan voeren, zijn:

- de controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van filtering van de inhoud op trefwoorden, ook wel content-filtering genoemd. Verdachte berichten worden automatisch teruggestuurd naar de afzender;
- de 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;
- de controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is;
- de controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.

8.2. De afdeling ICT en de systeembeheerder(s) zijn aan geheimhouding gebonden als men in het kader van de controle op dit Reglement om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

8.3. Door de Instelling worden in het kader van de controle op dit Reglement de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij verwerkt worden, juist en nauwkeurig zijn.

8.4. Door de Instelling worden in het kader van de controle op dit Regelement passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

Artikel 9. Procedure bij gericht onderzoek

9.1. Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende een specifieke gast worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door de gast.

9.2. Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur Operations. Het College van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

9.3. In afwijking van het vorige lid vindt gericht onderzoek naar de beveiliging of integriteit van randapparatuur plaats door het systeembeheer op basis van concrete aanwijzingen. Aparte toestemming van de in lid 2 bedoelde instantie is niet nodig. De resultaten van dit onderzoek worden alleen gedeeld met de gast met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit lid 2 worden gevolgd.

9.4. Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de Faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de Instelling overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Dit vereist schriftelijke toestemming van het College van Bestuur, welke in de toestemming de redenen zal noemen waarom deze wordt verleend.

9.5. Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van gasten als de gast daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit artikel. De gast zal in dat geval achteraf worden geïnformeerd.

Artikel 10. Consequenties van overtreding

10.1. Bij het handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het bestuur afhankelijk van de aard en de ernst van de overtreding maatregelen treffen. Hieronder vallen een waarschuwing, berisping, schadevergoeding, aangifte bij de politie, overplaatsing en het eventueel informeren van de werkgever van de gast.

Daarnaast kan het bestuur besluiten tot een al dan niet tijdelijke beperking in de toegang tot bepaalde Faciliteiten.

10.2. Aanvullend op voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende Faciliteit invoert. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

10.3. De Instelling is te allen tijde gerechtigd om aangifte te doen van geconstateerde strafbare feiten.

Artikel 11. Rechten van de gasten met betrekking tot persoonsgegevens

11.1. Gasten hebben, evenals alle andere betrokkenen, recht op inzage, verwijdering, correctie, rectificatie en bezwaar conform de rechten van de AVG. Alle AVG-rechten van de betrokkenen zullen conform wet- en regelgeving worden afgehandeld. Betrokkenen kunnen hun rechten uitvoeren door een e-mail te sturen aan ibploket@roc-nijmegen.nl

Artikel 12. Slotbepaling

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