ZADKINE

AUTEURS
Richard de Koning (Informatieveiligheid en Privacy)
Cebeli Gonul (Juridische Zaken)

STATUS
Finaal Concept – ter vaststelling CvB

VERSIENUMMER
1.9

DATUM
22-6-2020

Reglement Verantwoord Netwerkgebruik

Acceptable use policy

Reglement voor het veilig gebruik
van ICT-voorzieningen voor studenten

Model IBPDOC26 – Verantwoord Netwerkgebruik

INHOUD

1 Reglement Verantwoord Netwerkgebruik studenten

Stichting Zadkine, hierna te noemen de Instelling, biedt aan de eigen studenten, die van haar onderdelen en/of samenwerkingsscholen en aan bezoekende deelnemers de mogelijkheid internet te gebruiken ten behoeve van de studie. Tevens worden aan studenten voor persoonlijk gebruik een instellingsgebonden mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar gesteld ten behoeve van de studie. Aan het gebruik van deze faciliteiten zijn regels verbonden.

1.1 Gebruik van faciliteiten

Computer- en netwerkfaciliteiten (zoals openbare computers, draadloze en bedrade netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen) worden aan de student beschikbaar gesteld, onder meer voor het kunnen maken van opdrachten, verslagen en werkstukken, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten.

Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van de Instelling is toegestaan zolang dit gebruik voldoet aan de regels van dit Reglement. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door de Instelling is alleen toegestaan met aparte toestemming van de ict-beheerder. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op de bedrade of draadloze netwerkaansluitingen, is te allen tijde verboden.

Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en wachtwoord. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. De instelling kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten. Bij een vermoeden van misbruik van een wachtwoord kan de instelling per direct het betreffende account ontoegankelijk maken.

1.2 Intellectueel eigendom en vertrouwelijke informatie

De student maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert de licentieafspraken zoals die van toepassing zijn binnen de Instelling. De zeggenschap over de informatie van de Instelling berust bij Instelling. De student heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling.

Indien de student in het kader van zijn studie of het uitvoeren van taken voor de Instelling toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen.

Zie **“Privacy reglement voor studenten”**

De student besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van deze 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 client-apparatuur (USB-apparaten, Tablets, etc.).

Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld, dient de student deze stipt op te volgen.

1.3 Beveiliging door de Instelling én de student

De Instelling neemt informatiebeveiliging serieus. Zij hanteert dan ook een streng beveiligingsbeleid en neemt adequate technische en organisatorische maatregelen om de infrastructuur te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van vertrouwelijkheid, schending van privacy-rechten en schending van intellectuele eigendomsrechten.

Natuurlijk is een perfecte beveiliging onmogelijk. Daarom verwacht de Instelling ook van studenten een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. Zo is de student te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.
In het bijzonder dient de student, indien met zijn apparatuur gebruikt wordt gemaakt van de instellingsfaciliteiten, in het kader van beveiliging:

- deze apparatuur te voorzien van een adequate virusscanner en firewall;
- data veilig op te slaan in de aangewezen systemen van de Instelling
- geen persoonsgegevens op te slaan op een locatie die niet wordt beheerd door de Instelling
- Een voldoende lang en moeilijk te raden en te kraken wachtwoord of wachtzin te gebruiken (zie: **wachtwoordbeleid / voorschrift gebruikerswachtwoorden**)
- deze apparatuur up-to-date te houden wat betreft software-instellingen.

1.4 Privégebruik en overlast

Beperkt privégebruik van de faciliteiten is toegestaan. Gebruik, privé of voor studie, mag niet storend zijn voor de goede orde bij de Instelling en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de Instelling of derden of de integriteit en de veiligheid van het netwerk aantasten.

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

- het raadplegen 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 of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;
- filesharing-, media- of streamingdiensten (zoals Spotify of 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 student weet/moet weten 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.

Het gebruik van computer- en netwerkfaciliteiten voor commerciële activiteiten is uitsluitend toegestaan wanneer de Instelling hiervoor schriftelijk toestemming heeft verleend.

1.5 Monitoring door de Instelling

Controle van gebruik van de faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement ten behoeve van de goede orde op de Instelling en de bewaking van de integriteit en de veiligheid van het netwerk en de computerfaciliteiten van de Instelling. Verboden gebruik van de faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Voor deze controle worden geautomatiseerd gegevens verzameld (gelogd). Deze gegevens 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, zoals een blokkade van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken.

In het bijzonder kan bij overlast, veroorzaakt door apparatuur van studenten, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de student vooraf gewaarschuwd, zodat hij de gelegenheid heeft de overlast te staken. Wanneer dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, doet de directeur (MBO) zo snel mogelijk melding van de maatregel.

Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het gebruik van de faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de Wet bescherming persoonsgegevens en andere relevante regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en worden personen met toegang daartoe contractueel verplicht tot geheimhouding.

1.6 Procedure bij gericht onderzoek

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

Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de school, waarbij de reden vermeld zal worden waarom tot dit gerichte onderzoek zal worden overgegaan. Het College van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek.

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. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

Nader onderzoek naar de beveiliging of integriteit van randapparatuur mag in afwijking hiervan door de ict-beheerder worden uitgevoerd op basis van concrete aanwijzingen, zonder aparte toestemming. De resultaten van dit onderzoek worden alleen gedeeld met de student met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure zoals hiervoor beschreven voor het gericht onderzoek worden gevolgd.

De student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De student wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

Ict-beheerders verschaffen zich slechts toegang tot accounts of computers van de student als de student daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan na toestemming van de Functionaris Gegevensbescherming, in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit reglement. De student zal in dat geval achteraf worden geïnformeerd.

1.7 Rechten van de student met betrekking tot persoonsgegevens

Zie **“Privacy reglement voor studenten”**

1.8 Consequenties van overtreding

Bij handelen in strijd met dit Reglement of algemeen geldende (wettelijke) regels, kan de Instelling afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student.

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

In afwijking van het voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal maximaal een week worden gehandhaafd of korter als de oorzaak naar tevredenheid van de ict-beheerder is weggenomen. Indien na een week geen verbetering is geconstateerd door de ict-beheerder, kan deze besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen alsnog disciplinaire maatregelen worden genomen.

1.9 Slotbepalingen

Dit Reglement kan door de Instelling worden herzien. Wijzigingen worden bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer de Instelling door omstandigheden van buitenaf gedwongen is tot een snellere invoering.
De Instelling zal voorafgaand advies en feedback van Ondernemingsraad en Studentenraad in overweging nemen alvorens de wijzigingen in te voeren. In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.