InteraktContour
verder met hersenletsel

Internetprotocol InteraktContour

Inleiding

InteraktContour biedt aan haar medewerkers de faciliteiten van het gebruik van internet, computernetwerk en e-mail. Daarbij gaat InteraktContour ervan uit dat de medewerkers de ICT-faciliteiten gebruiken ten behoeve van hun werk. Tevens gaat InteraktContour ervan uit dat bij medewerkers de intentie bestaat om de ICT-faciliteiten zodanig te gebruiken dat er geen schade aangericht wordt aan het computernetwerk en dat medewerkers de intentie hebben om de ICT-voorzieningen zodanig te gebruiken dat de organisatie niet in diskrediet zal worden gebracht. Deze uitgangspunten vormen de basis voor dit internetprotocol.

Artikel 1 Definities, doel en werking

1. Dit is een regeling voor het gebruik van het computernetwerk, internet en e-mail voor medewerkers van InteraktContour.
2. Het protocol is opgesteld conform de Wet Bescherming Persoonsgegevens.
3. Doel van het protocol: Het protocol bevat regels en afspraken over het computergebruik door medewerkers en overige gebruikers, die in het netwerk van InteraktContour zijn ingelogd. Tevens heeft het betrekking op de omgang met ICT-voorzieningen, welke InteraktContour faciliteert en de manier waarop InteraktContour omgaat met het registreren, verzamelen en monitoren van tot een persoon herleidbare data inzake het gebruik van hardware, software, e-mail en internet. Doelstelling hiervan is een goede balans te vinden tussen een verantwoord gebruik van internet en e-mail en bescherming van de privacy van gebruikers op de werkplek.
4. Het protocol geldt voor alle in artikel 1.3 genoemde gebruikers die gebruik maken van het netwerk van InteraktContour en voor medewerkers die vanaf een andere locatie gebruik maken van het netwerk van InteraktContour. In de arbeidsovereenkomst,vrijwilligersovereenkomst,stage-overeenkomst of inleenovereenkomst wordt verwezen naar dit internetprotocol. Met de ondertekening van één van de bovengenoemde overeenkomsten verklaart de gebruiker dat hij bekend is met de inhoud van dit internetprotocol.
5. Het protocol omvat e-mail-, netwerk- en internetgebruik. Hieronder wordt ieder gebruik van de door InteraktContour geboden ICT-faciliteiten verstaan.
6. Waar in dit document regiodirecteur wordt vermeld kan ook (staf)manager worden gelezen.

Artikel 2 Algemene uitgangspunten

1. Internet kent verschillende verschijningsvormen, waarvan e-mail, intranet, social media en het World Wide Web (WWW, 'surfen') de belangrijkste zijn. In de rest van dit document worden met 'internet' bedoeld alle verschijningsvormen van dit medium.
2. Gebruik van internet is voor allen binnen InteraktContour nodig om het werk goed te kunnen verrichten. Niet correct gebruik van dit middel neemt tijd en capaciteit van mensen en apparatuur in beslag en kan schade veroorzaken aan ICT-voorzieningen, bedrijfsprocessen en/of producten; voorts kunnen daardoor bedrijfsgeheimen uitlekken en kunnen de organisatie en personen in diskrediet worden gebracht.
3. Tegen de achtergrond van deze risico's wordt van gebruikers professioneel en integer handelen verwacht.
4. Ter vermijding van dergelijke risico's geeft InteraktContour diverse voorschriften voor het verrichten van arbeid, voor de controle daarop en voor het kunnen nemen van maatregelen ter bevordering van

de goede gang van zaken in de organisatie. De richtlijnen en regels van dit internetprotocol vallen onder deze voorschriften.
5. Het gebruik van internet wordt automatisch geregistreerd (gelogd) om de continuïteit van de technische infrastructuur te waarborgen, om verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan. Deze registratie kan worden gebruikt om achteraf toezicht te kunnen houden op de naleving van het internetprotocol.
6. Alle registraties van persoonsgegevens vallen onder de Wet Bescherming Persoonsgegevens (WBP), dus ook de in dit internetprotocol genoemde registraties. De WBP verstaat onder een persoonsgegeven 'elk gegeven betreffende een geïdentificeerde of identificeerbare persoon'. In het privacyreglement van InteraktContour is dit verder uitgewerkt.
7. Het voor dit toezicht beschikbaar stellen van gegevens die tot een persoon herleidbaar zijn, wordt tot het strikt noodzakelijke beperkt. Uitgangspunt is een goede balans tussen beheer van de ICT-voorzieningen en bescherming van de privacy van de gebruiker. Inhoudelijke controle van internetgebruik vindt slechts plaats indien sprake is van een sterk vermoeden van overtreding van het internetprotocol of bij ernstige verstoringen in de ICT-voorzieningen (zie bijlage 1).
8. Iedereen die kennis neemt van geregistreerde informatie en de daaruit voortvloeiende onderzoeksgegevens is verplicht tot strikt vertrouwelijke behandeling daarvan.
9. Overtredingen kunnen leiden tot disciplinaire en arbeidsrechtelijke maatregelen.

Artikel 3. E-mailgebruik (in plaats van oude tekst)

1. E-mailberichten worden behandeld als persoonlijke post. Inhoudelijke controle van e-mails vindt alleen plaats als er een sterk vermoeden is dat de inhoud in strijd is met dit internetprotocol (zie bijlage 1).
2. Werknemers zijn gerechtigd het e-mailsysteem voor niet-zakelijk verkeer kortstondig te gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten zowel intern als extern, mits dit niet storend is voor hun dagelijkse werkzaamheden of voor anderen en het de goede werking van het netwerk niet verstoort.
3. Het recht van de werknemer om persoonlijke e-mailberichten te ontvangen en versturen is gebonden aan de volgende voorwaarden:

- Het bericht bevat een herleidbare afzender.
- Het bericht bevat een disclaimer.
- Het bericht bevat geen dreigend, seksueel intimiderend, racistisch, discriminerend, beledigend of aanstootgevend materiaal.
- Het bericht is niet in strijd met de fatsoensnormen en schaadt het aanzien van de organisatie niet.

4. De werkgever zal niet de inhoud van zowel persoonlijke als zakelijke e-mailberichten lezen. Gegevens omtrent het aantal e-mails, e-mailadressen en andere data hieromtrent worden wel geregistreerd, voor zover dit vereist is i.v.m. wettelijke of contractuele verplichtingen (Telecommunicatiewet). Op incidentele basis kunnen vanwege een zwaarwichtige reden controles plaats vinden.
5. e-mails van leden van de ondernemingsraad onderling, van bedrijfsartsen en andere vertrouwenspersonen zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het berichtenverkeer.
6. Registraties en rapportages worden bewaard zolang dit noodzakelijk wordt geacht voor de uitoefening van de taken door de ICT-afdeling. Controlegegevens die tot een persoon herleidbaar zijn, worden niet langer dan noodzakelijk bewaard, met een maximum van 6 maanden, behoudens het bepaalde in punt 15 van de bijlage.

7. Medewerkers worden geacht om niet in te gaan op phishing[1] mails. Mocht de medewerker het vermoeden hebben, toch op een phishing mail te zijn in gegaan moet hier direct melding van gemaakt bij de leidinggevend en de servicedesk. Dit gezien de potentieel zeer grote gevolgen hiervan.

Artikel 4 Internetgebruik

1. InteraktContour biedt gebruikers via het eigen netwerk toegang tot het internet door middel van een gebruikersidentificatie (inlognaam) en een wachtwoord, die persoonsgebonden zijn en dus niet aan anderen mogen worden verstrekt. Aan de gebruikersidentificatie zijn autorisaties verbonden, die bepalen over welke functionaliteit de gebruiker beschikt. Het is de gebruiker niet toegestaan om zich op andere wijze toegang te verschaffen tot internet.
2. Iedere gebruiker is persoonlijk verantwoordelijk voor de naleving van de in dit internetprotocol gestelde richtlijnen en regels en dient op een verantwoorde wijze om te gaan met informatie die hem via internet bereikt.
3. Internet wordt aan de gebruiker voor zakelijke doeleinden beschikbaar gesteld. Het gebruik is derhalve verbonden met taken die voortvloeien uit de functie.
4. Incidenteel en kortstondig gebruik van internet voor privé-doeleinden is toegestaan voor zover de werkzaamheden en/of de gebruikte ICT-voorzieningen daardoor niet worden gehinderd en de in dit internetprotocol gedefinieerde regels worden gerespecteerd.
5. Het gebruik van internet is niet toegestaan:
   - voor commerciële doeleinden anders dan voor InteraktContour;
   - om berichten te versturen met een pornografische, racistische, discriminerende, beledigende of anderszins aanstootgevende inhoud;
   - internetsites te bezoeken die soortgelijk materiaal bevatten;
   - om deel te nemen aan kansspelen en te gokken;
   - om mee te doen aan kettingbrieven, chatsessies;
   - om zich ongeoorloofde toegang te verschaffen tot computersystemen (‘hacken’);
   - om (muziek- en film)bestanden te downloaden voor privégebruik;
   - om auteursrechtelijk beschermd materiaal ongeoorloofd te downloaden;
   - voor enig ander onfatsoenlijk, onverantwoord of onwettig doel.
6. InteraktContour behoudt zich het recht voor met technische maatregelen de toegang tot bepaalde sites te blokkeren, de inhoud van berichten te filteren en bepaalde typen bestanden tegen te houden.
7. Het downloaden, installeren en aanbrengen van welke wijzigingen ook aan hardware, software en applicaties is voorbehouden aan de ICT-afdeling. Derhalve is dit de gebruiker niet toegestaan, tenzij per keer opnieuw vooraf toestemming door de manager FI&H is verleend.
8. Vertrouwelijke bedrijfsgegevens mogen niet zonder toestemming van de regiodirecteur door de gebruiker aan derden worden verstrekt en dan nog alleen indien zulks voortvloeit uit de uitoefening van de functie van de gebruiker. Digitale verstrekking is alleen toegestaan wanneer de verstrekking op papier ook geoorloofd zou zijn. De kans op fouten bij digitaal verspreiden, met name bij het gebruik van e-mail, is aanzienlijk en van de gebruiker wordt derhalve uiterste oplettendheid vereist.
9. InteraktContour behoudt zich het recht voor om aan verstuurde e-mails een disclaimer toe te voegen. In deze mededeling worden alle ontvangers en in het bijzonder ontvangers van verkeerd geadresseerde berichten gewezen op hun plicht zorgvuldig met de ontvangen informatie om te gaan.
10. Voor richtlijnen omtrent het gebruik van social media verwijzen we naar de integriteitscode van InteraktContour.

[1] Phishing is het vissen (hengelen) naar inloggegevens en persoonsgegevens van gebruikers. Bij Phishing proberen fraudeurs persoonlijke, vertrouwelijke gegevens te ontfutselen. Hiervoor wordt onder meer spam en malware gebruikt. Een nietsvermoedende gebruiker denkt met een bonafide instelling (bijvoorbeeld de bank) te maken te hebben. De vertrouwelijke informatie komt echter in handen van criminelen die zich met een valse identiteit op het internet manifesteren. Het gaat bij phishing vooral om het verzamelen van identiteits-, bank- en creditcardgegevens.

11. Mocht bij het bezoeken van een website, direct een melding komen van de antivirus software, wordt de medewerker gevraagd het adres van de website door te geven aan de servicedesk, zodat deze kan controleren of volledige blokkade van de website nodig is.

Artikel 5 Registratie en controle

1. Binnenkomend en uitgaand internetverkeer wordt gecontroleerd op virussen. Het merendeel van de virussen wordt automatisch tegengehouden en verwijderd. Indien toch een virusmelding op het beeldscherm verschijnt, dient de ontvanger dit direct te melden bij de servicedesk en het werken op de computer pas te hervatten na toestemming van de servicedesk.
2. Rapportage over internetverkeer vindt plaats op het niveau van getotaliseerde verkeersgegevens die niet zonder meer tot individuele personen zijn te herleiden.
3. Analyse en controle beperken zich in beginsel tot deze verkeersgegevens.
4. Bij een sterk vermoeden van overtreding van regels door een gebruiker of een groep van gebruikers kan gericht worden gecontroleerd.
5. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

Artikel 6 Rechten van de gebruiker

1. De gebruiker heeft het recht kennis te nemen van het soort gegevens dat over het internetgebruik wordt vastgelegd.
2. De gebruiker heeft het recht op inzage in de over hem in het kader van het onderzoek naar een vermoedelijke overtreding verzamelde informatie.
3. Indien de gebruiker van oordeel is dat hij in het kader van dit internetprotocol benadeeld is, kan hij een beroep doen op het klachtenreglement van InteraktContour.

Artikel 7 Sancties

1. Bij overtreding van dit internetprotocol kunnen, afhankelijk van de aard en de ernst daarvan, maatregelen worden getroffen. Hierbij gaat het om disciplinaire en arbeidsrechtelijke maatregelen, zoals intrekken van internetrechten, waarschuwing, overplaatsing, schorsing, beëindiging van de arbeidsovereenkomst en aangifte bij de politie.
2. Schenden van de vertrouwelijkheid met betrekking tot de geregistreerde informatie, de onderzoeken en/of de conclusies daarvan is een zware overtreding van dit internetprotocol en wordt als zodanig behandeld.

Artikel 8 Slot

1. In gevallen waarin dit internetprotocol niet voorziet beslist de Raad van Bestuur van InteraktContour.
2. Dit internetprotocol heeft de instemming van de ondernemingsraad van InteraktContour.

Bijlage 1

Procedure voor het onderzoek naar vermoedelijke overtredingen van het internetprotocol

1. In het belang van zowel het onderzoek als de betrokken gebruiker worden zo min mogelijk functionarissen betrokken bij dit proces. Het is de opdracht aan iedere bij het onderzoek betrokken functionaris dit zorgvuldig te bewaken.
2. Onderzoek naar een vermoedelijke overtreding van het internetprotocol door individuele gebruikers kan alleen worden geïnitieerd door de betreffende regiodirecteur, na overleg met de manager P&O en in de vorm van een schriftelijke opdracht.
3. De manager P&O beoordeelt of de opdracht van de regiodirecteur voldoet aan de volgende eisen:
   - het verzoek tot onderzoek is deugdelijk gemotiveerd;
   - het onderwerp van onderzoek is duidelijk omschreven;
   - het onderzoek gaat niet verder dan strikt noodzakelijk en fiatteert deze daarvoor.
4. De manager P&O stuurt het verzoek naar de manager FI&H.
5. De manager FI&H beoordeelt het verzoek en start – indien akkoord – het onderzoek. Bij niet akkoord beslist de Raad van Bestuur.
6. De regiodirecteur informeert de betrokken gebruiker zo spoedig mogelijk over het voorgenomen onderzoek naar zijn internetgebruik, de reden daarvan en zo mogelijk de verwachte duur.
7. De manager FI&H is en blijft voor de gehele duur van het onderzoek verantwoordelijk voor een correct verloop van het onderzoek en is het aanspreekpunt voor de manager P&O. Hij dient zorg te dragen voor een spoedige en zorgvuldige afhandeling van het onderzoek.
8. Bij aanvang van het onderzoek zullen alle mogelijk relevante data veilig worden gesteld zodat deze, indien nodig, als bewijsmateriaal gebruikt kunnen worden. Zodra dit is gebeurd, wordt de regiodirecteur hiervan op de hoogte gesteld.
9. De door de manager FI&H met het onderzoek belaste personen mogen alle noodzakelijke informatie gebruiken die deel uitmaakt van de door hen te controleren objecten. Deze medewerkers zijn eveneens gebonden aan strikte geheimhouding over het onderzoek zelf, de betreffende persoon/personen en de mogelijke conclusies. In dit verband zal schriftelijke communicatie over het onderzoek niet via e-mail plaatsvinden en zal alle informatie betreffende het onderzoek – tijdens en na het onderzoek – altijd veilig en slechts toegankelijk voor diegenen die daartoe gerechtigd zijn, worden opgeborgen. De onderzoekers dienen een logboek bij te houden van de wijze waarop het onderzoek is uitgevoerd en welke data daarbij zijn gebruikt.
10. Onderzoek op de inhoud van e-mails dient tot het strikt noodzakelijke te worden beperkt. De inhoudelijke beoordeling van dergelijke e-mails vindt plaats door de manager P&O.
11. De manager FI&H rapporteert de uitkomst van het onderzoek schriftelijk, voorzien van een onderbouwing, aan de manager P&O. Deze stelt de betreffende gebruiker en de regiodirecteur op de hoogte van de resultaten en de daaruit getrokken voorlopige conclusies.
12. De gebruiker wordt in de gelegenheid gesteld hierop te reageren. Daarbij heeft hij het recht op inzage in de gegevens die in het kader van het onderzoek over hem c.q. zijn internetgebruik zijn verzameld.
13. De regiodirecteur wint advies in bij de manager P&O en besluit vervolgens welke vervolgstappen genomen worden en stelt de gebruiker daarvan op de hoogte.
14. Wanneer het onderzoek resulteert in de vaststelling dat er geen sprake is van een overtreding zullen alle onderzoeksgegevens terstond door de ICT-afdeling worden vernietigd. Aan de gebruiker zal schriftelijk worden meegedeeld dat hem binnen het kader van dit internetprotocol niets te verwijten valt, dan wel dat de geconstateerde handelingen anderszins niet verwijtbaar zijn.
15. Wanneer het onderzoek resulteert in de vaststelling dat er wel sprake is van een overtreding, worden de onderzoeksgegevens voor verdere behandeling en archivering aangeboden

aan het manager P&O. De regiodirecteur stelt de Raad van Bestuur hiervan op de hoogte. Alle stukken worden door P&O gedurende drie jaren bewaard en daarna vernietigd. De oorspronkelijke schriftelijke opdracht en de conclusie van het onderzoek, voorzien van de genomen vervolgstappen, worden gearchiveerd in het digitaal personeelsdossier van betrokkene.

16. Mocht de uitslag van het onderzoek leiden tot de conclusie dat beëindiging van het dienstverband aan de orde zou moeten zijn, zal de regiodirecteur na advies te hebben ingewonnen bij de manager P&O hiertoe besluiten.

17. De betreffende gebruiker kan tegen dit besluit bezwaar aantekenen bij de Raad van Bestuur, die daarover in dat geval definitief beslist.