GEDRAGSLIJN COMMUNICATIEMIDDELEN

1. Doel en toepassingsgebied van de Gedragslijn.

1.1. Inleiding

Om de UZ Brussel medewerkers in staat te stellen hun taken op een professionele wijze te vervullen, stelt het bedrijf hen allerlei bedrijfsmiddelen en electronische-diensten ter beschikking, waaronder PC, portable PC, smart- of Iphone, e-mail, en internettoegang.

Het UZ Brussel respecteert het privé-leven van haar medewerkers, maar tegelijk staat het UZ Brussel erop dat de personeelsleden de ter beschikking gestelde communicatiemiddelen altijd en overal op een correcte en verantwoorde wijze gebruiken om het imago van het UZ Brussel te vrijwaren van schade.

Omdat de medewerkers steeds meer moderne communicatietechnieken ter beschikking hebben, wenst het UZ Brussel met betrekking tot die communicatiemiddelen te wijzen op een aantal basisregels en principes die, hoewel ze vanzelfsprekend zijn en gelden voor alle bedrijfsmiddelen, een waardig en gedisciplineerd gebruik ervan moeten waarborgen.

1.2. Algemeen karakter

Deze Gedragslijn regelt het gebruik van de communicatiemiddelen en diensten die het UZ Brussel ter beschikking stelt of via de UZ Brussel infrastructuur worden benaderd. Deze Gedragslijn in uitvoering van CAO Nr 81 is een aanvulling aan de Arbeidsreglement en vormt er een integraal deel van.

1.3. Persoonlijk toepassingsgebied

De Gedragslijn voor het gebruik van communicatiemiddelen geldt zonder uitzondering voor alle medewerkers (personeelsleden, consultants of externe medewerkers die binnen het UZ Brussel activiteiten uitoefenen, contractanten, stagiairs, interimarissen) die gebruik maken of toegang hebben tot de door het UZ Brussel ter beschikking gestelde communicatiemiddelen en diensten.

Voor bepaalde afdelingen of gespecialiseerde activiteiten kan deze Gedragslijn worden aangevuld met specifieke gedragsregels. Deze zullen door de directe chef schriftelijke worden gecommuniceerd aan de direct betrokken medewerkers.

1.4. Materieel toepassingsgebied

Deze Gedragslijn is van toepassing op alle communicatiemiddelen die door het UZ Brussel aan haar medewerkers ter beschikking worden gesteld, zoals telefoontoestellen, smart-, Iphones, pc's, portables, tablets, opname apparatuur, fototoestellen, e-mail, -collaboratiesystemen, interne memo-systemen, internet, LAN, WAN, partnernetwerken, fototoestellen al dan niet

digitaal, opnameapparatuur, draagbare pc's, I-mode, … Deze opsomming is niet limitatief.

De Gedragslijn geldt voor alle informatiesystemen en interne netwerken en voor alle gegevens die door die systemen worden verzonden of erin worden opgeslagen.

2. Basisregels

2.1. Uitgangspunt : professioneel gebruik

In principe mag de medewerker de ter beschikking gestelde communicatiemiddelen onbeperkt en vrij gebruiken voor zover dit kadert in en noodzakelijk is voor zijn professionele bedrijfsactiviteiten.

Privé-gebruik moet tot een strikt minimum beperkt worden.

Het gebruik van de communicatiemiddelen voor communicatie vanuit de syndicale organisaties voor algemene communicaties naar het geheel van het personeel toe is niet toegestaan. Dit geldt zowel voor mededelingen als voor verkiezingscommunicatie. De communicatiemiddelen mogen wel gebruikt door de syndicale organisaties in het kader van de communicatie rond een specifieke topic of case en voor de interne syndicale werking. Dit houdt in dat de groep bestemmelingen voor dit type communicatie sowieso beperkt blijft.

2.2. Basisregels

In het kader van het professioneel gebruik van de ter beschikking gestelde communicatiemiddelen gelden de hierna volgende basisregels :

- Houd steeds voor ogen dat u optreedt in naam van het UZ Brussel.
- Gebruik de u toegekende communicatiemiddelen nooit als amusement.
- Plaats op weblocaties geen referenties naar het UZ Brussel-weblocaties, e-mail adressen of -mailboxen, tenzij u daar uitdrukkelijk de toestemming toe kreeg.
- Respecteer het auteursrecht op informatie.
- Deel geen niet publieke bedrijfsinformatie en redactionele informatie mee aan niet-bevoegden. Telefoonlijsten of lijsten met de namen van de medewerkers, abonnees, zakenrelaties, … technische gegevens, worden als vertrouwelijke informatie beschouwd. Deze opsomming is niet limitatief.
- Het bezoeken van internetlocaties (sites) of andere vindplaatsen die pornografisch, racistisch of enig ander materiaal bevatten dat strijdig is met de openbare orde of goede zeden, is ten strengste verboden.
- Verbindingen met telefoonnummers waarop erotische of andere gesprekken die strijdig zijn met de openbare orde of goede zeden, worden gevoerd zijn ten strengste verboden.
- U mag de ter beschikking gestelde communicatiemiddelen niet gebruiken voor de verzending, opslag of opvraging van bestanden of berichten : met een onwettige inhoud of doelstelling (zoals software zonder licentie, schending van de openbare orde of de goede zeden, ongewenst gedrag,

laster, enz.) of die indruisen tegen het beleid of de belangen van de onderneming (zoals bv. De ongeoorloofde onthulling van informatie, het verspreiden van malware, e.d.).

- Als medewerker moet u op eerste verzoek de communicatiemiddelen die het bedrijf u ter beschikking stelt in goede staat en inclusief toebehoren terugbezorgen.
- Op een aantal communicatiemiddelen werden beveiligingsmechanismen aangebracht zoals anti-malware software, toegangsbeveiliging, beperkingen mbt de grootte of de aard van bestanden, enz. Deze beveiligingsmechanisme mag u onder geen enkel beding uitschakelen of omzeilen. Indien om welke reden ook deze beveiligingsmechanismen niet meer of slechts gedeeltelijk actief zouden zijn, verwittigt u onmiddellijk de IT-helpdesk en staakt u het gebruik van het bewuste communicatiemiddel.
- Indien u e-mails of teams-uitnodigingen ontvangt al dan niet met bijlage met voor u onbekende namen of waarvan de afzender u onbekend is of met vreemde hoofding, of vreem vraag qua timing of inhoud, verwittigt u de helpdesk zonder de bewuste bijvoegsels te openen of op eventueel aanwezige links binnen de e-mail te klikken of in te gaan op de uitnodiging.
- Het gebruik van algemene mailgroepen is strikt voorbehouden aan specifieke gebruikersgroepen. Zonder expliciete toestemming mag u deze mailgroepen niet gebruiken.
- Het verspreiden van kettingbrieven, zelfs voor liefdadige doeleinden, is niet toegestaan.
- De introductie en de verspreiding van computervirussen, Trojaanse paarden of andere malware die de vertrouwelijkheid, de beschikbaarheid of de integriteit van de gegevens in gevaar kan brengen, is verboden.
- Het gebruik van de ter beschikking gestelde communicatiemiddelen voor deelname aan spelletjes of aan gokspelen is niet toegestaan.
- Alle binnenkomende berichten zonder een professioneel karakter (bv. moppen, foto's, afbeeldingen, e.d.) moet u onmiddellijk verwijderen. Als u regelmatig zulke berichten krijgt van bekende bronnen, is het uw verantwoordelijkheid om de nodige maatregelen te nemen, zodanig dat een dergelijke communicatie zich niet meer herhaalt.
- Om de beschikbaarheid van het netwerk niet in gevaar te brengen wordt het verzenden en ontvangen van omvangrijke bestanden door de mailserver automatisch beperkt. Wanneer u regelmatig bestanden groter dan de gestelde limiet dient te verzenden of te ontvangen, neemt u contact op met de IT helpdesk.
- Alle junk mail moet u onmiddellijk verwijderen
- Op deze regels kan in functie van specifieke opdrachten afgeweken worden na uitdrukkelijke toestemming van de IT-directeur.
- In geval u binnen de context van uw opdracht voor het UZ gebruik maakt van electronische diensten van het UZ, zoals wifi connectie, e-mail, teams… via uw eigen toestel, smartphone, computer… zogenaamd Bring Your Own Device (BYOD), blijven bovenstaande topics onverminderd van toepassing
- Als u gebruik maakt van persoonlijke toestellen (BYOD) om door het UZ aangeboden diensten zoals E-mail … te gebruiken dient u er voor te zorgen dat uw toestel veilig is, geen malafide software bevat en naar veiligheid – updates "up-to-date" is.
- Binnen het ziekenhuis en zijn satelieten is het verboden zelf op eigen initiatief en zonder overleg met de ICT dienst informtieverwerkende toestellen op te stellen :pc's, netwerkmateriaal… onegacht deze via het UZ vaste netwerk ,wifi of niet zijn gekoppeld.

3. Opleiding en sensibilisering

Van het ogenblik men verwerking van informatie binnen de context van het ziekenhuis verricht wordt geacht dat men voldoende bekwaamheid verwerft om dit op een veilige manier te kunnen uitvoeren. Om deze bekwaamheid te bevorderen wordt verwacht minimaal één maal per jaar het basis sensibiliserings traject te doorlopen.

4. Toezicht en controle

4.1. Controle

Het UZ Brussel stelt de communicatiemiddelen enkel ter beschikking onder de uitdrukkelijke voorwaarde van strikte naleving van deze Gedragslijn. Een controle op het gebruik van die middelen is dus noodzakelijk. Die controle gebeurt in overeenstemming met alle geldende wettelijke en reglementaire bepalingen terzake, inzonderheid de procedure voorzien in CAO Nr 81. Zo worden bv. een aantal acties geregistreerd in logboeken of logbestanden. Dergelijke logs kunnen gebruikt worden voor het systeemmanagement, beveiligingscontroles, algemene gebruiksanalyses, trendbepaling en gebruiksvergelijkingen op individueel niveau.

Alle netwerkverkeer kan worden nagetrokken, bijvoorbeeld op schadelijke elementen zoals programmas, virussen of andere dubieuze codes, pogingen tot inbraak, inhoud van documenten of mails in strijd met deze Gedragsregels.

Alle software welke op de verschillende apparatuur staat wordt regelmatig nagetrokken en gecontroleerd op conformiteit met de gebruikte policies. Indien ongeautoriseerde software wordt aangetroffen of configuraties welke niet in overeenstemming zijn met de bedrijfsstandaards, wordt de software automatisch verwijderd en wordt de oorspronkelijk bedrijfsconfiguratie in ere hersteld.

Slechts ingeval van aanwijzingen van misbruik, kan gebruik gemaakt worden van concrete informatie over het gebruik van de diverse communicatiemiddelen.

Het UZ Brussel kan ten allen tijde de toegang tot bepaalde gegevensbronnen blokkeren door middel van filters of andere geautomatiseerde controlemiddelen. De (technische) mogelijkheid om toch een verboden locatie te bezoeken impliceert niet dat een dergelijk bezoek is toegelaten.

Als er aanwijzingen van misbruik zijn wordt een gericht onderzoek ingesteld. Enkel de Personeelsdirecteur, de Gedelegeerd Bestuurder of de directeur Informatica kunnen een dergelijk gericht onderzoek uitvoeren.

4.2 Niet-naleving : gevolgen

Het imago, het succes, veiligheid en de resultaten van het UZ Brussel worden mee bepaald door de wijze waarop wij ons gedragen. Het UZ Brussel rekent dan ook op een gedisciplineerd gebruik van de communicatiemiddelen en een strikte naleving van deze Gedragslijn.

De niet-naleving van de Gedragslijn kan niet worden aanvaard. Bij ernstige inbreuken zal streng worden opgetreden. Afhankelijk van de aard van de inbreuk, de gevolgen ervan voor het UZ Brussel en de repetitiviteit van de inbreuk kunnen volgende sancties of combinaties ervan volgen:

- Onmiddellijke stopzetting van de samenwerking
- Vergoeding van de kosten welke het UZ Brussel heeft als gevolg van het oneigenlijke gebruik van de ter beschikking gestelde communicatiemiddelen.
- Vergoeding van de vervanging van beschadigde of verloren communicatiemiddelen.
- Herroepen van de machtiging tot het gebruik van de communicatiemiddelen.
- Administratieve sanctie als schriftelijke verwittiging
- Mondelinge verwittiging

Wij zijn ervan overtuigd dat wij kunnen rekenen op de loyauteit en de medewerking zodat correctief optreden kan vermeden worden.
Tegen de genomen sanctie kan beroep worden aangetekend, dit dient schriftelijk te gebeuren ter attentie van de HR Directeur.

Deze gedragslijn en de voorziene controle zal regelmatig geëvalueerd worden door de ondernemingsraad met het oog op een goed functioneren en de aanpassing aan de technologische ontwikkelingen.

4.3 Toegang tot informatie in persoonlijke folders

Externen kunnen bedrijfsinformatie opslagen in persoonlijke folders op de ter beschikking gestelde communicatiemiddelen.

Indien tijdens een periode van ziekte, een bij einde van de samenwerking of een periode van afwezigheid van de externe een vraag reist naar bepaalde bedrijfsinformatie en er een sterk vermoeden bestaat dat deze bedrijfsinformatie opgeslagen is in de persoonlijke folders op de ter beschikking gestelde communicatiemiddelen dan kan de directe chef, de personeelsdirecteur of een door de informatica directeur daartoe aangeduide IT-medewerker deze folders doorkijken teneinde de betrokken informatie op te sporen en deze ter beschikking te stellen van het bedrijf.

5. Hard- en software

5.1. Wijzigingen aan hardware

U mag geen wijzigingen aanbrengen aan de u ter beschikking gestelde communicatiemiddelen. De medewerkers van de helpdesk mogen zulke wijzigingen doorvoeren.

5.2. Gebruik van eigen hardware

U mag geen bedrijfsvreemde computerhardware of communicatieapparatuur koppelen aan het bedrijfsnetwerk, tenzij na uitdrukkelijke toestemming.

5.3. Modems en elektronische koppelingen

U mag via een modem of een ander electronisch toestel geen rechtstreeks verbinding maken met het internet of met een ander bedrijfsvreemd netwerk als het toestel vanaf dewelke u die verbinding maakt een daaraan gekoppeld toestel eveneens via een ander kanaal gekoppeld is met het bedrijfsnetwerk.

Het doel van deze richtlijn is het bypassen van beveiligingsmechanisme voorkomen en het bedrijfsnetwerk afschermen en beschermen tegen ongecontroleerde toegang.

5.4. Alleen geautoriseerde software gebruiken

U mag binnen het bedrijf alleen software gebruiken welke door de Helpdesk op het communicatiemiddel werd geïnstalleerd. U mag nooit software installeren op apparatuur van het bedrijf, zelfs indien u over een persoonlijke licentie beschikt. Gebruik dus nooit illegale software: het is strafbaar en zowel het bedrijf als u zelf kan aansprakelijk gesteld worden.

5.5. Eigendom van ontwikkelde software

Software die door externen binnen het kader van de beroepsactiviteiten werd ontwikkeld, maakt integraal deel uit van het patrimonium van het bedrijf. U mag deze software dan ook niet gebruiken of commercialiseren voor eigen rekening en u mag geen handelingen stellen die het verder gebruik van de software of de exploitatie van de software kunnen hinderen.