Policy

Deontologische code informatiebeveiliging voor Digipolis-medewerkers.

Versie 1.5 19/07/2010

Versiebeheer			
Datum	Omschrijving	Wijziging gemaakt door	Versie
03/02/2010	Initieel document	Spanoghe Bob	1.0
04/03/2010	Aangepaste versie	Spanoghe Bob	1.1
18/03/2010	Aanpassing toelichting	Spanoghe Bob	1.2
12/04/2010	Juridische controle	DLI, Spanoghe Bob	1.3
20/05/2010	Document ter goedkeuring	BCC, Spanoghe Bob	1.4
19/07/2010	Definitief document na controle vakorganisaties	Bob Spanoghe	1.5

Inhoudsopgave

1 Doel van het document

Waarom dit document?

In bepaalde situaties is het voor een Digipolis-medewerker (informatiebeheerder of telematicagebruiker) niet altijd duidelijk hoe juist te handelen. Als er sprake is van een deontologisch dilemma, kan je dit document gebruiken als leidraad bij het maken van de juiste keuzes.

Het basisuitgangspunt blijft de verantwoordelijkheidszin en arbeidsethiek van de medewerkers. De deontologische code geeft als normenkader de grenzen weer waarbinnen je moet handelen. Het opzet is om de belangen van Digipolis als werkgever te behartigen in haar professionele activiteiten. Anderzijds vrijwaart de code de privacyrechten van de medewerkers.

Wat is de doelstelling van dit document?

De deontologische code heeft 3 belangrijke functies:

1. Het is een normenkader waarin we de rechten, plichten en verantwoordelijkheden van de gebruikers voor de domeinen “informatiegebruik” en “telematicagebruik” beschrijven.

2. Het is een praktische en eenduidige leidraad voor het omgaan met informatiebeveiliging en meer in het bijzonder het gebruik van telematicamiddelen.

3. Als medewerker geef je – op basis van de richtlijnen in deze code – aan Digipolis de toestemming om de ingebouwde controlemechanismen te gebruiken. Concreet: na het ondertekenen van de code geef je er expliciet de toestemming voor dat Digipolis het telematicagebruik mag controleren. Uiteraard gebeurt dit conform de wet op de privacy.

Waarom deze gedragscode voor informatiebeveiliging?

Met deze gedragscode wil Digipolis:

- haar medewerkers bewust maken van hun specifieke rol als informatiebeheerder;
- voorkomen dat ongeoorloofde (strafbare) of lasterlijke feiten worden gepleegd met de ter beschikking gestelde telematicamiddelen;
- voorkomen dat door het gebruik van telematica schade wordt berokkend, van welke aard dan ook, aan de organisatie of aan derden;
- de dienstverlening aan de klant garanderen;
- de belangen van de organisatie beschermen;
- de veiligheid en de goede technische werking van het netwerk garanderen;
- kostenbewustzijn stimuleren bij het gebruik van de telematicamiddelen.

Wat is het toepassingsdomein en wie zijn de doelgroepen?

Volgens de code hebben Digipolis-medewerkers twee rollen, nl. telematicagebruiker en informatiebeheerder. Je bent een telematicagebruiker binnen Digipolis. Tegenover Digipolis en haar klanten ben je een informatiebeheerder. Voor beide rollen zijn er specifieke richtlijnen.

Gebruik je informatie of systemen van Digipolis-klanten, dan moet je de specifiek geldende regels of afwijkingen naleven.

Wie is informatiebeheerder?
Een informatiebeheerder heeft verhoogde toegangsrechten. Hiermee kan hij het functioneel gebruik van gegevens overschrijden. Het gaat om systeembeheerders, databeheerders, applicatiebeheerders, netwerkbeheerders, consultants, veiligheidsbeheerders, enz.

Wie is telematicagebruiker?
Een telematicagebruiker heeft toegang tot het telematicanetwerk van Digipolis en/of dat van al haar klanten. De code is bijgevolg ook van toepassing op elke derde die beroepshalve toegang heeft tot één of meerdere telematicamiddelen van Digipolis.

Wat verstaan we onder telematica?
Als Digipolis-medewerker krijg je alle noodzakelijke telematicamiddelen ter beschikking om je taken op een efficiënte manier uit te voeren. Telematicamiddelen die tot de werkomgeving behoren zijn: computer/laptop, printer, kopieerapparaat, telefoon, gsm, toegang tot intra- en internet, de noodzakelijke software, informatiedragers, … Deze middelen blijven altijd eigendom van de organisatie en kunnen nooit als verworven beschouwd worden.

Hoe is dit document opgebouwd?

Inhoudelijk zijn er 2 grote thema's:

1. De algemene richtlijnen over de specifieke rol van informatiebeheerder: de zogenaamde "Code voor informatiebeheerders"[1]

2. De specifieke richtlijnen over het gebruik van telematica-instrumenten: de zogenaamde "Acceptable Use Policy"

Het document beschrijft 24 richtlijnen. Elke richtlijn illustreren we met een voorbeeld.

[1] De "ADM gedragscode voor informatiebeheerders" werd geïntegreerd, er wordt per richtlijn verwezen naar de originele nummering van dit document. ADM code v1.1, 2005

2 Deel 1: Code voor informatiebeheerders

2.1 Basisbegrippen

De gedragscode wil alle informatiebeheerders bewust maken van het belang om hun bevoegdheden op een ethisch verantwoorde manier uit te oefenen. Ze is een ethische leidraad bij professionele handelingen.

De code gaat uit van vier basisbegrippen: de professionele integriteit, de beschikbaarheid en integriteit van het netwerk en de computersystemen, informatiebescherming en informatieplicht.

- De professionele integriteit handelt over de ethische gedragsvoorschriften voor een informatiebeheerder.
- De integriteit van de computersystemen en netwerken handelt over de bewaking van gegevens en geautomatiseerde processen.
- Informatiebescherming handelt over privacybescherming en het omgaan met vertrouwelijke informatie.
- Informatieplicht gaat over het informeren van gebruikers en het documenteren van het computersysteem en/of -netwerk.

De verantwoordelijkheid van het informatiebeheer ligt zowel bij Digipolis als bij haar klanten. Binnen de werking van Digipolis is:

- de **verwerker** van de persoonsgegevens **Digipolis**;
- de **verantwoordelijke** voor het verwerken van de persoonsgegevens de **klant** van Digipolis.

De gedragscode voorziet passende technische en organisatorische maatregelen voor de beveiliging en de bescherming van persoonsgegevens, zoals vereist door artikel 16 van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, ook wel de Privacywetgeving genoemd.

2.2 Richtlijnen

2.2.1 Ethische integriteit van de informatiebeheerder

Richtlijn 1 *(ADM code 1.1)*

De informatiebeheerder stelt zich objectief en onpartijdig op in de uitvoering van zijn functie.

Als informatiebeheerder vervul je je functie op een kritische en verantwoorde manier. Je werkt onafhankelijk en onpartijdig tegenover de diensten binnen Digipolis en haar klanten. Je beslissing is gebaseerd op een rationele beoordeling van de relevante informatie.

Laat je niet meeslepen door je eigen standpunt. Zo mag bijvoorbeeld je eigen politieke voorkeur geen impact hebben op de dienstverlening aan de klanten.

In je relatie tot leveranciers en klanten spring je voorzichtig om met uitnodigingen of geschenken. Om enige schijn van persoonlijke beïnvloeding te vermijden worden geschenken en uitnodigingen overgemaakt aan HRM. Op het intranet vind je hierover 2 standpunten.

- *Standpunt_Algemene geschenken en uitnodigingen van leveranciers en klanten*
- *Standpunt_Individuele geschenken en uitnodigingen van leveranciers en klanten*

Richtlijn 2 *(ADM code 1.2)*

De informatiebeheerder streeft ernaar persoonlijke belangenconflicten te vermijden. Wanneer deze zich toch voordoen, zal hij zijn oversten daarover inlichten.

Hier kan het gaan om persoonlijke belangen die onverenigbaar zijn met het belang van de organisatie of die van de klanten.
Er zijn bijvoorbeeld duidelijke regels over nevenactiviteiten of bijberoepen in relatie tot Digipolis en haar klanten. Je vindt ze terug op het intranet.

- *Deontologie_Bijklussen in IT: wat kan, wat kan niet?*

Stel jezelf ook in vraag als je bijvoorbeeld in een gunningtraject van een bestek mee beoordelingen maakt en één van de partijen een familielid of vriend is.

Twijfel je? Doe dan even de brillentest. Bekijk je eigen gedrag door de bril van een collega of chef. Voel je je ongemakkelijk? Dan heb je waarschijnlijk een belangenconflict.

Richtlijn 3 *(ADM code 1.3)*

De informatiebeheerder zal zijn vaardigheden steeds op gepaste wijze ten dienste stellen van de onderneming en de gebruikers van de ICT-systemen.

Als informatiebeheerder beschik je over zeer waardevolle kennis, maar moet je erover waken deze op gepaste wijze te gebruiken.

Je gebruikt bestaande rechten bijvoorbeeld niet om jezelf of een collega (toegangs)rechten te geven tot applicaties of informatie die je niet voor je eigen werk nodig hebt. Hiervoor bestaan aanvraagprocedures waarin een verantwoordelijke de aanvraag zal evalueren. Je maakt bijvoorbeeld ook geen gebruik van service accounts omdat die meer rechten hebben dan jij. Zelfs al is dit om snel even een probleem op te lossen of op vraag van een leidinggevende.
Denk eraan dat ongeoorloofde toegang tot applicaties en informatie eigenlijk "hacken" is, hoe goed je bedoelingen ook zijn.

Richtlijn 4 *(ADM code 1.4)*

De informatiebeheerder streeft ernaar in de best mogelijke verstandhouding samen te werken met iedereen binnen de onderneming.

Als informatiebeheerder handel je steeds in het belang van Digipolis en haar klanten door te ijveren voor een vlotte samenwerking, ook met externe medewerkers binnen de organisatie. Klantgerichtheid, kostenbewustzijn en kwaliteit zijn hierbij steeds de uitgangspunten.

Denk bij al je handelingen verder dan je eigen verantwoordelijkheid. Het testen van een applicatie kan invloed hebben op de performantie van operationele toepassingen. Als je niet zeker bent van de mogelijke gevolgen van bepaalde acties, ga er dan vanuit dat communicatie met de betrokken partijen de eerste stap moet zijn.
In een professionele omgeving kunnen meningsverschillen over gebruikte technologie of architecturale opzet niet leiden tot conflicten die de algemene werking in het gedrang kunnen brengen.

Richtlijn 5 *(ADM code 1.5)*

De informatiebeheerder vermijdt het om foutieve voorstellingen van de eigen capaciteiten te geven en zal, wanneer dit nodig blijkt, professionele hulp inroepen voor technische bijstand.

Te fier zijn om hulp in te roepen en daarom verder blijven knoeien, kan niet de bedoeling zijn. Het einddoel van heel de organisatie moet het opleveren van kwaliteit zijn. Dit betekent ook dat indien je problemen vaststelt buiten je eigen verantwoordelijkheid, je deze bespreekbaar probeert te maken.

Als informatiebeheerder is het je taak om ervoor de zorgen dat alle hard- en software op een correcte manier blijven werken. Kan je een probleem niet onmiddellijk oplossen, vraag dan raad aan je collega's. Kennisoverdracht is vaak de efficiëntste manier om op zeer korte tijd een probleem op te lossen.

Laat je eigen mening over gekozen technische standaarden bij Digipolis niet doorwegen in je opdrachten. Toets je eigen mening over technologieën of infrastructuur altijd af aan de voorliggende functionele wensen, het beschikbare budget of het tijdskader. De volgens jou beste oplossing op technisch vlak is niet altijd de beste oplossing voor de klant of voor de organisatie.

Richtlijn 6 *(ADM code 1.6)*

De informatiebeheerder zal een voortdurende inspanning leveren om op de hoogte te blijven van de stand van de techniek en van maatschappelijke aangelegenheden die een impact hebben op de manier waarop hij zijn functie uitoefent.

Als informatiebeheerder ben je leergierig en tracht je steeds bij te blijven.
Als medewerker neem je zelf actief initiatief om je kennis en vaardigheden uit te breiden of te vervolmaken.

2.2.2 Integriteit van het computersysteem en/of –netwerk

Richtlijn 7 *(ADM code 2.1)*

De informatiebeheerder staat in voor het behoorlijk functioneren van het systeem. De informatiebeheerder mag enkel die handelingen stellen die nodig zijn om de integriteit van het computersysteem of -netwerk te verzekeren.

Als informatiebeheerder handel je steeds in het belang van Digipolis en haar klanten, waarbij het verzekeren van de goede werking van het computersysteem één van je belangrijkste taken blijft. Sta er steeds bij stil dat kleine aanpassingen grote gevolgen kunnen hebben. Denk altijd aan de mogelijk gevolgen voor de volledige keten van processen. Een server herstarten omdat er een probleem optrad, kan gevolgen hebben voor de ganse organisatie.
Stem daarom voldoende af met alle betrokken partijen voordat je handelt. Gebruik hiervoor de geijkte kanalen. Het laten lopen van een query op een database kan tot gevolg hebben dat de performantie van infrastructuurcomponenten zoals het mainframe ernstig beïnvloed wordt.

Richtlijn 8 *(ADM code 2.2)*

De informatiebeheerder waakt erover dat zijn handelingen niet het verlies of de beschadiging van gegevens tot gevolg hebben. Als het nodig blijkt bepaalde gegevens of bestanden te wijzigen, kiest de informatiebeheerder steeds voor de oplossing die het minste invloed heeft op de informatie en die de gebruikservaring het minst verstoort.

De informatiebeheerder zal, indien mogelijk, bestanden hernoemen of verplaatsen in plaats van ze te bewerken of te verwijderen.
Zo worden gegevens op operationele databases enkel aangepast na afstemming met alle betrokken partijen. Leef altijd het gecontroleerde wijzigingsbeheer en het gestructureerde versiebeheer na.

Hou steeds voor ogen dat de continuïteit van de dienstverlening en het bewaken van de integriteit van gegevens prioriteit nummer 1 zijn. Zorg dat er altijd een back-up reflex is of werk met tussenstappen die het mogelijk maken gegevens te recupereren bij het oplossen van incidenten.

Richtlijn 9 *(ADM code 2.3)*

Aangezien bepaalde handelingen van gebruikers de integriteit van het computersysteem of -netwerk kunnen schaden, mag de informatiebeheerder ingrijpen. Het is zijn taak toe te zien op de naleving door de gebruikers van de bedrijfspolitiek inzake aanvaardbaar gebruik van het computersysteem ("Acceptable Use Policy").

Voor de specifieke richtlijnen, zie deel 2 " Gebruikerscode".
Hierin vind je onder meer richtlijnen voor het gebruik van user account & paswoord, het gebruik van e-mail & internet en informatiebronnen. Het is normaal dat de naleving van de "Acceptable Use Policy" gecontroleerd wordt. Dit moet echter gebeuren met respect voor de wet op de privacy.
Over deze controlemogelijkheden geven we in hoofdstuk 3.3 meer uitleg.

Richtlijn 10 *(ADM code 2.4)*

Informatiebeheerders waken erover dat toegang tot het systeem voorbehouden blijft aan diegenen voor wie dergelijke toegang vereist is uit hoofde van hun functie.

Als informatiebeheerder geef je enkel gebruikersrechten aan eindgebruikers nadat de nodige goedkeuringsprocedures zijn doorlopen. De informatiebeheerder vervult hierbij een voorbeeldfunctie en vraagt zelf alle nodige rechten aan via het goedkeuringscircuit.
Speciale accounts voor informatiebeheerders worden met extra zorg voor confidentialiteit en integriteit behandeld. De heersende IT-security policies worden altijd nageleefd.
Je mag deze speciale bevoegdheden gebruiken om taken uit te voeren, maar niet om informatie voor persoonlijke doeleinden te raadplegen.

Een collega een account geven, zelfs tijdelijk, zonder de nodige goedkeuring is niet toegelaten. Zelfs in "dringende gevallen" raadpleeg je altijd eerst je leidinggevende.

Het gebruik van algemene administrator- of service accounts is niet toegelaten. Als je dit soort rechten nodig hebt, volg je eerst de hiervoor geldende aanvraagprocedure.

Digipolis volgt het gebruik van deze speciale bevoegdheden op en zal overtredingen als een ernstig veiligheidsincident behandelen.

De verschillende IT-security policies voor deze speciale bevoegdheden vind je terug in het informatieveiligheidsbeleid op het intranet.

2.2.3 Informatiebescherming

2.2.3.1 Respect voor de privacywetgeving

Richtlijn 11 *(ADM code 3.1.1 en 3.1.2)*

Informatiebeheerders hebben toegang tot grote hoeveelheden persoonsgegevens, waarop de privacywetgeving van toepassing is.

De informatiebeheerder is zich bewust van het dwingend karakter van de regels uit de privacywetgeving. Hij ziet er dus nauwgezet op toe deze regels na te leven, met bijzondere aandacht voor de regels inzake verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijkt, en de verwerking van gegevens over gezondheid of seksuele oriëntatie.

Als informatiebeheerder hou je steeds rekening met de privacywetgeving. Je maakt geen gebruik van persoonsgegevens voor jezelf of derden. Een uitgebreide beschrijving van de privacywetgeving vind je in de handleiding op het intranet.

- *Handleiding inzake telematicaonderzoek*

Het is niet toegestaan om bijvoorbeeld na te gaan of je buurman een rijbewijs heeft of niet. Die gegevens zijn beschermd door de privacywetgeving.

Richtlijn 12 *(ADM code 3.1.3)*

De informatiebeheerder neemt passende technische en organisatorische maatregelen voor de beveiliging en bescherming van persoonsgegevens tegen
- **toevallige of ongeoorloofde vernietiging,**
- **toevallig verlies,**
- **de wijziging van of de toegang tot en iedere andere niet toegelaten verwerking van persoonsgegevens.**

Als informatiebeheerder hou je bij het nemen van beveiligingsmaatregelen rekening met de technische mogelijkheden, de aard van de te beveiligen gegevens en de mogelijke risico's.
Alle mogelijke conflicten moet je onmiddellijk melden aan je leidinggevende of de betrokken partijen binnen de organisatie.
Ga er steeds van uit dat Digipolis naar hogere overheden toe een belangrijke verantwoordelijkheid heeft inzake gegevensbeheer. Spring dus extra voorzichtig om met deze gegevens. Soms zijn ze immers onvervangbaar als ze verloren gaan.

Informatiebeheerders worden wel eens geconfronteerd met aanvragen voor toegang tot applicaties die persoonsgebonden gegevens bevatten. Bekijk de motivatie van deze aanvragen steeds kritisch. Ga na of de juiste aanvraagprocedures zijn doorlopen. Besteed als informatiebeheerder voldoende aandacht aan het principe van de "openstaande achterdeur". Een goed bedoelde webservice in een applicatie die rechtstreeks een persoonsgegevensbestand benadert om bijvoorbeeld een adres op te halen, opent mogelijk ook onbewaakte deuren naar andere persoonsgegevens.

Richtlijn 13 *(ADM code 3.1.4)*

De informatiebeheerder stelt derden en externe medewerkers die toegang krijgen tot de gegevens op de hoogte van hun verplichting om de privacywetgeving te respecteren.

Als informatiebeheerder licht je derde partijen in (waaronder externe medewerkers) over het respecteren van de privacywetgeving als die partijen voor Digipolis en/of haar klanten werken.

Bij aanvang van je loopbaan teken je een contract waarin staat dat je op een correcte manier zal omgaan met gevoelige informatie. Externen tekenen een gelijkaardig document als ze bij Digipolis starten. Ondanks deze contractuele verbintenis moet je als informatiebeheerder steeds alert zijn en ervoor zorgen dat alle partijen zich in al hun handelingen bewust zijn van de gevoeligheid van de gegevens. Dat operationele informatie beschermd moet worden, lijkt voor iedereen vanzelfsprekend, maar gegevens die gebruikt worden in de ontwikkelings- of acceptatiefase moeten met dezelfde voorzichtigheid behandeld worden.
Stel jezelf de vraag of jij het leuk zou vinden mochten jouw persoonlijke gegevens ongemerkt op het internet verschijnen.

Stel je vast dat collega's of externe partijen de regels niet naleven, dan maak je hen er opmerkzaam op of meld je dit aan je leidinggevende.

2.2.3.2 Controle van elektronische online communicatiegegevens en inzage in de bestanden

Richtlijn 14 *(ADM code 3.2.1)*

De informatiebeheerder kan enkel overgaan tot controle van elektronische online communicatiegegevens wanneer aan de wettelijke voorwaarden voldaan is.

Controle op elektronische online communicatiegegevens is aan strikte regels onderworpen en moet dan ook tot een minimum beperkt worden (voor meer uitleg zie onderdeel controlemogelijkheden 3.3).

Moet/Mag ik op aanvraag van één van mijn collega's of leidinggevende opzoekingen doen? Hiervoor bestaan strikte procedures die enkel kunnen geïnitieerd worden door de directie, de hoogste verantwoordelijke bij de klanten of het gerecht. In alle gevallen moet aan een aantal voorwaarden voldaan zijn en wordt het proces gecoördineerd door de security officer van Digipolis. Zonder deze voorwaarden mag dergelijk onderzoek niet uitgevoerd worden. De gebruikte procedures voor de verschillende hoofdklanten Antwerpen en Gent zijn terug te vinden op het intranet.

Richtlijn 15 *(ADM code 3.2.2)*

De informatiebeheerder mag zich enkel toegang verschaffen tot bestanden van gebruikers en deze raadplegen als hij de voorafgaande toestemming van de betrokken gebruiker heeft verkregen.

Dit is wat de privacywetgeving theoretisch weergeeft. In de praktijk is dit echter genuanceerd. Eerst en vooral wordt er een onderscheid gemaakt tussen het zich toegang verschaffen tot een batch van gegevens en individuele gegevens. Het eerste is toegestaan in het kader van beheertaken. In het tweede geval, waarbij op persoonsniveau naar gegevens wordt gekeken, ligt dit anders. Dit soort gegevens raadplegen mag enkel onder bepaalde omstandigheden, bijvoorbeeld bij een vermoeden van misbruik en mits toestemming van de betrokken gebruiker. Deze toestemming kan op verschillende manieren gegeven worden: rechtstreeks of onrechtstreeks via het goedkeuren van een deontologische code. Om alle vergissingen te vermijden heeft Digipolis hiervoor een procedure opgesteld (zie richtlijn 14). Bij enige twijfel contacteer je best de security officer.

2.2.3.3 Vertrouwelijke gegevens

Richtlijn 16 *(ADM code 3.3.1)*

De informatiebeheerder is er zich van bewust dat alle informatie en communicatie van de onderneming als vertrouwelijk beschouwd en behandeld moet worden.

Als informatiebeheerder mag je geen misbruik maken van je kennis of commercieel gevoelige informatie en handel je steeds in het belang van Digipolis en haar klanten.

In het contract dat je getekend hebt bij Digipolis staat hierover een duidelijke clausule. Bij twijfel kan je deze clausule raadplegen.

Uit het arbeidscontract - Artikel 10

Zowel tijdens de duur van de verbintenis als daarna verbindt de werknemer zich ertoe geen enkel zakelijk geheim of feiten van de werkgever, haar klanten enz., kortom alles aangaande de bedrijfswerking bekend te maken aan derde personen, concurrenten of niet en dit ongeacht de belangrijkheid.
Iedere overtreding van deze verbintenis, hoe gering ook, is een dringende reden die de onmiddellijke beëindiging van deze overeenkomst rechtvaardigt, ongeacht strafvervolging overeenkomstig artikel 309 van het Strafwetboek en ongeacht het vorderen van alle verdere schadevergoedingen.

De informatie en documentatie die aan de werknemer tijdens de duur van deze overeenkomst worden toevertrouwd, zijn strikt persoonlijk, blijven steeds eigendom van de werkgever en dienen op het einde van de verbintenis te worden teruggegeven.

De werknemer verklaart zich in het bijzonder akkoord met de strikte naleving van artikel 458 van het strafwetboek inzake beroepsgeheim.

Zo mag je bijvoorbeeld geen informatie geven aan leveranciers over de stand van zaken van bestekken of aankoopprocedures. Persoonlijke e-mail adressen of telefoonnummers van klanten doorgeven voor het versturen van nieuwsbrieven of commerciële doeleinden doe je ook liever niet.

2.2.4 Informatieplicht

Richtlijn 17 *(ADM code 4.1.1)*

De informatiebeheerder zorgt ervoor dat de gebruikers terdege geïnformeerd zijn over de bedrijfspolitiek inzake aanvaardbaar gebruik van het computersysteem ("Acceptable Use Policy"). Deze bedrijfspolitiek wordt gecommuniceerd in bewoordingen die voor niet-IT-professionals verstaanbaar zijn.

Deel 2 van deze code beschrijft de voor Digipolis geldende "Acceptable Use Policy". Vanuit jouw voorbeeldfunctie draag je de richtlijnen van deze deontologische code uit.

Richtlijn 18 *(ADM code 4.1.2)*

Naar aanleiding van een operationele interventie licht de informatiebeheerder zijn handelingen toe, zodat de gebruiker behoorlijk geïnformeerd is over de gevolgen hiervan voor het gebruik van het systeem. Deze informatie wordt tijdig verstrekt en is geformuleerd in verstaanbare bewoordingen. De informatiebeheerder zorgt ervoor dat er steeds geactualiseerde documentatie voorhanden is die de infrastructuur van het netwerk en/of het systeem (hard- en software) op zodanige wijze beschrijft dat elke professionele informatiebeheerder zich op basis van deze documentatie een precies en volledig beeld zou kunnen vormen van de betrokken infrastructuur en in staat zou zijn het ononderbroken beheer ervan te verzekeren.

Als informatiebeheerder zorg je ervoor dat alle betrokken partijen steeds tijdig en voor hen verstaanbaar geïnformeerd worden, zowel bij pannes als bij onderhoudswerken.
Je maakt hiervoor gebruik van de bestaande kanalen voor crisiscommunicatie en wijzigingsbeheer.

3 Deel 2 Gebruikerscode telematicamiddelen “Acceptable Use Policy”

3.1 Toepassingsgebied

In de gebruikerscode telematicamiddelen worden een aantal richtlijnen opgenomen die specifiek handelen over het gebruik van telematica.

Naast een aantal algemene richtlijnen wordt ook dieper ingegaan op:

- Gebruik pc, randapparatuur, gebruikersaccounts en wachtwoorden;
- Gebruik e-mail en internet;
- Controle en privacybewaking.

3.2 Richtlijnen

3.2.1 Algemeen gebruik telematicamiddelen

Richtlijn 19

- **Digipolis-medewerkers vervullen een voorbeeldfunctie in het gebruik van informatieveiligheidsregels en geldende IT-security procedures.**
- **Zij stellen zelf geen handelingen die de veiligheid of de werking van de verschillende netwerken kunnen bedreigen.**
- **Zij geven derden niet de mogelijkheid om handelingen te stellen die de veiligheid of de werking van de verschillende netwerken kunnen bedreigen.**
- **Zij stellen geen handelingen die als ongeoorloofd of als lasterlijk beschouwd kunnen worden of de dienstverlening in het gedrang kunnen brengen.**
- **Zij springen zuinig om met de ter beschikking gestelde telematicamiddelen.**
- **Zij plegen geen ongeoorloofde feiten of feiten die strijdig zijn met de openbare orde, de goede zeden of die de waardigheid van Digipolis, van een rechtspersoon of een natuurlijke persoon kunnen schaden.**
- **Zij plegen geen inbreuken tegen de wet op het auteursrecht en schenden geen copyright en/of andere intellectuele rechten.**

Je mag geen informatie verspreiden of opslaan die

- *het imago van Digipolis of dat van haar klanten schendt;*
- *Digipolis in het algemeen zowel moreel als economisch kan schaden;*
- *beledigend en aanstootgevend is;*
- *lasterlijk en discriminerend is;*
- *schade kan toebrengen aan derden;*
- *strijdig is met de openbare orde of goede zeden;*
- *een pornografisch of uitgesproken erotisch karakter heeft;*
- *aanstootgevend is voor anderen omdat ze tegen de algemeen geldende fatsoensregels indruist.*

3.2.2 Gebruik pc, randapparatuur, gebruikersaccounts en wachtwoorden

Richtlijn 20

- **Digipolis-medewerkers zorgen als een goede huisvader voor de ter beschikking gestelde middelen: ze springen zorgvuldig om met telematica alsof het persoonlijke middelen zouden zijn.**
- **Als een computer buiten de werkuren voor privédoeleinden wordt gebruikt, moeten de nodige beveiligingsmaatregelen in acht genomen worden om de werking van IT-middelen te vrijwaren.**
- **Privégebruik van een pc of een laptop die door de werkgever ter beschikking wordt gesteld, wordt door de belastingsdiensten als een voordeel in natura beschouwd. Dit wordt verrekend via het loon. Medewerkers die de thuis-pc enkel voor beroepsdoeleinden gebruiken, moeten een verklaring ondertekenen.**

Gebruik je je pc thuis, dan mag je op je pc of laptop bv. spelletjes of muziek zetten mits het toestel optimaal blijft functioneren voor gebruik op het werk. Privégebruik van pc of laptop doe je uiteraard niet tijdens de werktijd.
De medewerker volgt bij deze richtlijn de bestaande standpunten op het intranet:

- *Standpunt_gebruik Digipolis-materiaal voor privédoeleinden;*
- *Standpunt_ pc-configuratie medewerker voor thuis;*
- *Standpunt_gebruik bedrijfs-gsm.*

Mag ik via mijn computer muziek beluisteren op het werk?
In principe mag je op het werk muziek beluisteren zolang het de collega's niet stoort en het jouw eigen productiviteit niet negatief beïnvloedt. Wanneer je dit via de pc doet, moet je ervoor zorgen dat je hierdoor het netwerk niet belast en dat de performantie van je pc niet vermindert. Opladen van muziek via het netwerk of luisteren naar webradio's belasten het netwerk wel en kan dus niet.

Mag ik mijn computer aanpassen aan mijn persoonlijke voorkeur?
Je mag je computer aanpassen zodat je optimaler kan werken. Zo is het instellen van het bureaublad, de lettergrootte, enz. toegelaten. Heb wel respect voor iedereen waarmee je in contact komt. Een seksueel getint bureaublad kan bijvoorbeeld niet omdat dit mogelijk aanstootgevend is voor een collega. De configuratie zo aanpassen dat die schadelijk is voor de goede werking van het toestel en van het netwerk mag uiteraard niet. Hardware toevoegen doe je via de lokale netwerkbeheerder.

Mag ik fotokopieën nemen voor privédoeleinden?
Ja, dat mag mits het betalen van een vergoeding per kopie. Het verschuldigde bedrag wordt in de voorziene brievenbussen gestort. Meer informatie over o.a. de tarieven vind je op de brievenbussen en in het standpunt op het intranet.

Mag ik mijn bedrijfs-gsm gebruiken voor privégebruik?
Ja, dat mag, maar in de eerste plaats dient de gsm voor de verbetering van de dienstverlening. Zorg er dan ook voor dat je bereikbaar bent op die momenten dat het in het kader van je opdracht vereist is. Meer informatie over o.a. de kostendeling vind je terug in het standpunt op het intranet.

Zorg ervoor dat je niet moreel verantwoordelijk kan gesteld worden voor diefstal van je pc, gsm en randapparatuur. Je laptop is verzekerd, dus als je aan de voorwaarden van de verzekering voldoet, ben je niet financieel aansprakelijk. Een laptop achterlaten op een bank in het park is bijvoorbeeld geen daad van goed beheer. Ook in de kantoorgebouwen moet je laptops, wanneer je naar huis gaat, achter slot en grendel plaatsen.

Richtlijn 21

De pc of de laptop die ter beschikking wordt gesteld, mag nooit illegale software of illegaal verkregen muziek of films bevatten. Voor alle aanwezige software moet er een geldige licentie zijn.

Standaardpc's worden met een basissoftwarepakket uitgerust door de medewerkers van LAN-beheer. Zij zorgen ervoor dat er enkel met officiële licenties gewerkt wordt. Voor alle bijkomende software volgt de medewerker de bestaande aanvraagprocedures die je op het intranet vindt.

Richtlijn 22

Gebruikersaccounts en wachtwoorden zijn persoonlijk en mogen niet vrijgegeven worden. Iedere medewerker is verantwoordelijk voor de handelingen die met zijn gebruikersaccount gebeuren op het netwerk.

Vergelijk je gebruikersaccount en paswoord met de sleutels van je huis. Die geef je ook niet aan iedereen in bruikleen.

3.2.3 Gebruik e-mail en internet

Richtlijn 23

Het door Digipolis ter beschikking gestelde e-mailadres en de toegang tot het internet moeten door de medewerkers van Digipolis op een verantwoorde manier worden gebruikt, dit zowel op het vlak van beroepsethiek als op het vlak van algemeen aanvaarde maatschappelijke en ethische regels.

Mag ik mijn privémails lezen en versturen van op het werk?
Privémails behandelen op het werk is toegestaan, maar hiervoor word je natuurlijk niet betaald. Doe dat tijdens een pauze of na de werkuren. Zorg ervoor dat de dienstverlening niet wordt verstoord en dat het netwerk niet extra wordt belast. De infrastructuur gebruiken om kettingmails, commerciële berichten, racistische boodschappen of persoonlijke advertenties te versturen mag niet. Wees zorgzaam bij het gebruik van verzendlijsten en gebruik ze enkel voor de juiste professionele doeleinden.

De medewerker volgt bij deze richtlijn het bestaande standpunt op het intranet:

- *Standpunt_e-mailgebruik voor privédoeleinden*

Mag ik surfen op het internet?
Indien dit te maken heeft met je werk is het uiteraard toegelaten. Surfen voor privédoeleinden mag je in geen geval tijdens de werktijd doen – daarvoor word je immers niet betaald – maar wel tijdens een pauze of buiten de werkuren. Een randvoorwaarde hierbij is dat je surfgedrag de dienstverlening niet in gevaar brengt. Het binnenhalen van virussen of het opladen van bestanden of programma's kunnen het netwerk destabiliseren. Gokken, porno en spelletjes op het werk doe je niet, ook niet buiten de werkuren.
Surfgedrag kan gelogd worden, waardoor men precies weet welke websites werden bezocht, wanneer en hoe lang. Dat gebeurt niet systematisch, maar kan worden opgezet als misbruik vermoed wordt. Regelmatig wordt een top 20 van meest bezochte sites gemaakt. Op basis daarvan kan het surfgedrag onder meer worden onderzocht.
Ben je niet zeker of je surfgedrag door de beugel kan? Doe dan even de voorpaginatest. Stel dat 'Jef Janssens zit dagelijks 1 uur op Facebook tijdens de werkuren' een krantenkop zou zijn, zou je dan blozen? Ja? Dan ben je vermoedelijk niet goed bezig.

3.3 Controlemogelijkheid

De IT-middelen die Digipolis ter beschikking stelt aan haar personeelsleden, zijn eigendom van Digipolis. De controle op het correct gebruik ervan behoort dus tot de rechten van Digipolis.
De controle op het gebruik van de communicatiemiddelen gebeurt alleen voor gerechtvaardigde doeleinden. Daarom worden controles enkel uitgevoerd voor volgende doelstellingen en gaan de controles niet verder dan in verhouding nodig is voor het verwezenlijken ervan:

- de naleving van de bepalingen van de deontologische code;
- de bescherming van de vertrouwelijkheid van de gegevens van Digipolis en haar klanten;
- het vrijwaren van de veiligheid en/of de goede technische werking van de IT-middelen en de fysieke bescherming van de installaties;
- het voorkomen van criminele acties of fraude;
- het onderzoek en de opsporing van misbruik;
- het zich ervan vergewissen dat alle IT-middelen goed gebruikt worden.

Hierbij respecteert Digipolis de toepasselijke wetgeving, waaronder de privacywetgeving.

Dit impliceert dat telematicaonderzoeken enkel kunnen verricht worden onder volgende omstandigheden:

1. ondersteuning bij geheime onderzoeken door politionele en gerechtelijke autoriteiten;
2. technisch onderhoud van het communicatienetwerk;
3. ondersteuning bij de handelingen van hulp- en nooddiensten;
4. **mits er uitdrukkelijke toestemming is van de betrokkene.**

Door de ondertekening van de deontologische code door de medewerker

1. bevestigt hij het bestaan ervan;
2. verklaart hij zich bewust te zijn van de opgenomen regels;
3. engageert hij zich tot het naleven ervan;
4. **verleent hij de toestemming aan Digipolis om een telematicaonderzoek te verrichten voor de doeleinden zoals beschreven in de deontologische code en conform de privacywetgeving.**

Bij het uitvoeren van deze controles kan Digipolis onder meer volgende niet-limitatieve lijst van gegevens inzake telecommunicatieverkeer bekijken:

- e-mailadressen van uitgaand en inkomend e-mailverkeer;
- telefoonnummers van uitgaand en inkomend telefoonverkeer (vast en mobiel);
- faxnummers van uitgaand en inkomend faxverkeer;
- ip-adressen, historiek, cookies en cache van internetbezoek;
- handelingen via het verleende gebruikersaccount of speciale accounts op het netwerk en manipulatie van datacomponenten.

Bij ernstig vermoeden van misbruik of fraude kan de controle bestaan uit real time monitoring van telematicagebruik of retroactieve controle en kan de controle zowel betrekking hebben op verkeersgegevens als op de inhoud van de communicatie. Digipolis zal bij het beslissen over de te nemen maatregelen steeds rekening houden met het principe van proportionaliteit en zal geen controles uitvoeren die verregaander zijn dan strikt noodzakelijk voor de beoogde doeleinden.

Onder vermoeden van misbruik of fraude wordt bijvoorbeeld het downloaden van illegale films of muziek verstaan, werkverzuim door langdurig privé surfen op het internet, het misbruik van speciale toegangsrechten om (persoonlijke) administratieve dossiers in te kijken of te vervalsen, het lekken van confidentiële informatie over o.a. bestekken aan potentiële leveranciers, het raadplegen van vertrouwelijke persoonsgegevens van burgers en deze aan de buitenwereld bekend maken, misbruik van de telefoonlijnen door het voeren van dure persoonlijke (buitenlandse) telefoongesprekken of het illegaal kopiëren, verspreiden of verkopen van bedrijfssoftware die onder de licentiewetgeving valt.

Het management is hierbij altijd het opdrachtgevend orgaan, de security officer is het uitvoerend orgaan en elk onderzoek wordt in een formeel verslag gedocumenteerd. De gehanteerde procedures voor de verschillende klanten zijn terug te vinden op het intranet van Digipolis (zie richtlijn 14).

Richtlijn 24

De Digipolis-medewerker is op de hoogte van de inhoud van de deontologische code en verleent door ondertekening van de code toestemming aan Digipolis om het telematicagebruik te controleren in het kader van een onderzoek naar het correct gebruik van de telematicamiddelen die ter beschikking zijn gesteld. De controle kan enkel bij ernstig vermoeden van misbruik of fraude en zal altijd in verhouding zijn met de beoogde doelstelling en met respect voor de persoonlijke levenssfeer van de medewerker conform de wet op de privacy.

Kan men controleren naar waar ik gesurft heb?
Ja, dat kan. Surfgedrag kan gelogd worden waardoor men precies weet welke websites je bezocht hebt, wanneer en hoe lang. Logging van websites gebeurt niet systematisch, maar kan worden opgezet wanneer men misbruik vermoedt. Regelmatig wordt een top 20 gemaakt van de meest bezochte websites en op basis daarvan kan onder meer het surfgedrag worden onderzocht.

Kan men mijn e-mails lezen?
Neen, dat kan niet, tenzij er een ernstig vermoeden is van misbruik of fraude. In dat geval kunnen e-mails wel gelezen worden maar dit is verbonden aan een aantal voorwaarden. De controle moet altijd in verhouding zijn met het vermoede misbruik en gebeurt niet systematisch. In een eerste fase wordt enkel het e-mailverkeer gecontroleerd. Er kan zo nagegaan worden wie jou e-mails gestuurd heeft en naar wie jij e-mails hebt gestuurd. Vervolgens kunnen e-mails die betrekking hebben op het vermoede misbruik dan op inhoud worden gecontroleerd.

Kan men nakijken hoeveel en met wie ik getelefoneerd heb?
Ja, dat kan. Internationale gesprekken komen op een aparte top 50-lijst. Deze telefoons zijn meestal te verantwoorden vanuit de functie, maar soms ook niet.

Mag mijn leidinggevende mijn e-mail-, telefoon- of surfgedrag controleren?
Nee, dat mag hij niet alleen beslissen. Heeft je leidinggevende een vermoeden van misbruik, dan moet hij de directie van Digipolis informeren. De directie beslist, in overleg met de leidinggevende, welke stappen er ondernomen moeten worden. Zij kan de opdracht geven de loggings na te kijken of een logging op te starten, maar zij kan ook klacht neerleggen bij het gerecht.

Meer informatie over de privacywetgeving vind je op het intranet:

- *Digipolis dienstencatalogus onderzoek telematicagebruik.*

3.3.1 Sanctionering

De gehanteerde regels voor sanctionering in geval van overtredingen, zijn opgenomen in het arbeidsreglement van Digipolis.

4 Bevestiging inhoud en akkoordverklaring

Ik _____ verklaar het document

'Deontologische code informatiebeveiliging voor Digipolis-medewerkers *(versie 1.5 van 19/07*) gelezen te hebben en geef mijn goedkeuring over de inhoud van het document en verbind mij tot het naleven ervan conform de opgenomen richtlijnen.

De medewerker

Handtekening _____

Datum _____