



the Autonomous Management School of  
Ghent University and Katholieke Universiteit Leuven

## **Rapport: Ethische aspecten van ICT**

**Is er nood aan een gedragscode voor de ICT professional?**

**Prof Dr Dirk Deschoolmeester**

**Joachim Van den Bergh**

<b>Inhoudsopgave</b>	<b>1</b>
<b>Executive summary</b>	<b>2</b>
<b>Inleiding</b>	<b>3</b>
<b>(Relevantie, opzet, acknowledgements,...)</b>	
<b>Onderzoeksmethodologie</b>	<b>4</b>
<b>Context</b>	<b>7</b>
- <b>Ethische aspecten van ICT</b>	
- <b>Ethische codes</b>	
<b>Resultaten</b>	<b>9</b>
<b>Discussie</b>	<b>20</b>
<b>Appendices</b>	<b>22</b>

Contact:  
Prof Dr Dirk Deschoolmeester  
Joachim Van den Bergh  
Vlerick Leuven Gent Management School  
Operations & Technology Management Centre  
Vlamingenstraat 83 – 3000 Leuven – Belgium  
Tel: 09 210 98 24  
[www.vlerick.com](http://www.vlerick.com)

## INLEIDING

De impact van informatie en communicatie technologie (ICT) is in de moderne maatschappij moeilijk te overschatten. De snelle evolutie van deze technologie is een drijfveer voor de hedendaagse kenniseconomie. Grote en kleine organisaties vertrouwen op de degelijke werking van allerhande software. Daarnaast gebeurt een zeer groot deel van de communicatie over digitale kanalen zoals internet. Centraal in deze ontwikkeling van de economie staat de rol van de ICT professional die zich in een spanningsveld tussen economische en morele motieven bevindt. Een centrale vraag in dit onderzoek is waar het belang van de organisatie dat van de arbeidsethiek overtreft.

ICT verantwoordelijken beheren vaak gevoelige of waardevolle informatie. Zowel de economische als de persoonlijke waarde en de gevoeligheid van gegevens zorgen ervoor dat op de schouders van de informatiebeheerder een zware verantwoordelijkheid rust. Wie een ICT vakblad openslaat kan niet naast de talrijke ethisch geladen cases kijken. In vele gevallen gaat het om de gevolgen van een gebrekkig bewustzijn van de risico's van bepaalde beslissingen met betrekking tot het gebruik en het beheer van ICT systemen, en in sommige gevallen zelfs om slechte wil. De ruime mogelijkheden van ICT zijn uiteraard niet vreemd aan deze problematiek. Informatie van allerlei aard is vanop afstand toegankelijk en vaak moeilijk te controleren. Heel wat systemen blijken ook zeer kwetsbaar op het vlak van toegangsbeveiliging.

Naast het informatiebeheer is er nog een andere belangrijke factor die de verantwoordelijkheidszin van ICT professionals op de proef stelt. De kwaliteit van het geleverde werk vormt namelijk ook aanleiding voor bezorgdheid. Gezien het voornoemde feit dat vele ondernemingen en openbare instellingen in hoge mate afhankelijk zijn van het functioneren van hun ICT systemen ontstaan ook hier vaak situaties die vragen oproepen over de professionaliteit van het vakgebied ICT.

Het onderzoek is een gezamenlijk initiatief van de Federatie van Belgische Verenigingen voor Informatica (FBVI/FAIB) en Vlerick Leuven Gent Management School. Voor de verspreiding van de vragenlijst werd een beroep gedaan op de medewerking van ADM, Beltug, SAI, CIONet, VRI, IT Professional en CIO Forum, naast het aanspreken van de doelgroep via de kanalen van de Vlerick Leuven Gent Management School onder andere in het kader van de ICT management opleidingen.

Het onderzoek doet een beroep op de inschatting van ethisch geladen cases door de Belgische ICT professional om op deze wijze het ethisch gedrag met betrekking tot ICT gebruik en ontwikkeling onder de aandacht te brengen. Daarnaast kunnen de resultaten aangewend worden om het debat te voeden betreffende het nut van een gedragscode voor de ICT professional. Voorts stelt zich de vraag op welke schaal en in welke vorm zulke gedragscode zou kunnen voorkomen. Op deze manier kan het onderzoek bijdragen tot de bewustwording en ontwikkeling van het ICT vakgebied in België.



## ONDERZOEKSMETHODOLOGIE

Het onderzoek is opgebouwd rond negen fictieve cases die eerder door ACM<sup>1</sup> werden verzameld en uitgeschreven ter illustratie van een ethische gedragscode. Elk van deze cases draagt een potentieel ethisch geladen dilemma in zich dat op een bepaalde manier een beslissing van de ICT professional vergt. De thema's van de cases variëren van omgang met privacy tot kwaliteit van het geleverde werk. Alle respondenten werd gevraagd de ethische impact van de situatie in te schatten vanuit het standpunt van de ICT professional. Dit onder de vorm van een score op een 5-punten schaal waarbij score 5 overeenstemt met de hoogst mogelijke vorm van onethisch gedrag, die in principe een resolute correctieve actie vergt. De respondenten konden optioneel bij elke case hun antwoorden argumenteren of aanvullende bedenkingen toevoegen ter vervollediging van hun gegeven oordeel.

De vragenlijst werd ingeleid met een duidelijke verwijzing naar het doel van het onderzoek en de instructies. De vragenlijst werd online beschikbaar gemaakt gedurende twee periodes in april 2007 en later december 2007 tot februari 2008. De doelgroep bestond uit ICT professionals en ICT verantwoordelijken in België. In totaal gaven 276 personen hun input over de cases. 206 personen werkten de volledige vragenlijst af. De resultaten werden vervolgens gefilterd op bruikbaarheid en betrouwbaarheid aan de hand van de tijd die over de antwoorden gedaan werd. Alle gegevens werden strikt anoniem geregistreerd en behandeld.





<b>Onvolledig:</b>	<b>70 (25,4%)</b>
<b>Volledig:</b>	<b>206 (74,6%)</b>
<b>Totaal:</b>	<b>276</b>

De populatie van de respondenten op de vragenlijst kan door enkele statistieken beschreven worden.



Geslacht	% vd antwoorden	%
1 Vrouw		12 %
2 Man		88 %
	0% 20% 40% 60% 80%	

12 percent van de bevroegde populatie ICT professionals is vrouwelijk. In de literatuur kunnen verschillende bronnen gevonden worden met tegenstrijdige conclusies over de invloed van het geslacht op ethische inschattingen en gedragingen. In deze studie echter werden geen significante verschillen opgetekend tussen man of vrouw.

<sup>1</sup> Bron: Association for Computing Machinery (ACM), Using the new ACM code of ethics in decision making, Communications of the ACM, 36(2) 1993 pp.98-107









Leeftijdscategorie	% vd antwoorden	%
21-30		19 %
31-40		30 %
41-50		38 %
51-60+		13 %
	0% 20% 40% 60% 80%	

Het merendeel van de bevroegde ICT professionals, ongeveer 68 %, bevindt zich in de leeftijdscategorieën tussen 31 en 50 jaar.

Persoonlijke ervaring	% vd antwoorden	%
Ja		76 %
Neen		24 %
	0% 20% 40% 60% 80%	

Van de respondenten geeft drie kwart aan dat zij in hun werk reeds in contact kwamen met ethisch geladen situaties wat betreft het gebruik van ICT. Dit hoge cijfer geeft aan dat ICT wel degelijk een domein is waarvan het gebruik en het beheer geregeld leiden tot ethische dilemma's in het gedrag en de beslissingen.

De vragenlijst bevatte ook een aantal vragen die peilen naar de karakteristieken van het bedrijf of de instelling waarbij de respondent in dienst is. 26 % van de respondenten is werkzaam in een bedrijf uit de ICT sector zelf. Andere grote groepen zijn de consultants (20%) en respondenten uit de productiesector (11%). Bij de restcategorie zaten veel respondenten uit de opleidingswereld.

Sector	% vd antwoorden	%
Productiebedrijven		11 %
Nutsvoorzieningen		4 %
Financieel/verzekeringen		2 %
Overheid		6 %
Consulting		20 %
ICT-services		26 %
Gezondheidszorg		6 %
Andere		24 %
	0% 20% 40% 60% 80%	

De omvang van de bedrijven van de respondenten varieert van eenpersoonsbedrijven tot bedrijven met meer dan 1000 werknemers. De grote bedrijven vormen ook de grootste groep binnen deze populatie met 45%. 30% van de respondenten is tewerkgesteld bij een grote KMO met 100 tot 500 werknemers. Door de anonieme registratie van de antwoorden kon geen kwalitatieve analyse worden uitgevoerd aan de hand van bedrijfsspecifieke gegevens. Het kan namelijk niet uitgesloten worden dat meerdere respondenten uit eenzelfde organisatie zijn en daardoor de resultaten vertekenen.

Omvang vh bedrijf	% vd antwoorden	%
0-100 werknemers.		15 %
100-500 werknemers.		29 %
500-1000 werknemers.		11 %
meer dan 1000 werknemers.		45 %

Van de respondenten geeft iets minder van de helft aan dat ICT voor hun bedrijf een strategisch middel is. Voor de andere 51% is ICT een louter ondersteunende functie in het bedrijf.

Rol van ICT in het bedrijf	% vd antwoorden	%
een ondersteunende functie.		51 %
een strategische functie.		49 %

Tot slot werd gevraagd naar de eventuele aanwezigheid van een gedragscode of richtlijn voor de ethische aspecten van ICT gebruik in de organisatie. In de helft van de gevallen beschikt de organisatie wel degelijk over een soort beleidsmechanisme om deze situaties te begeleiden en geprefereerd ethisch gedrag in goede banen te leiden. In de andere helft van de gevallen ontbreekt een richtlijn voor ethisch geladen beslissingen in de organisatie. We stellen vast dat in de organisaties waar ICT als strategisch wordt omschreven het percentage (55%) iets hoger is dan in de organisaties met ondersteunende ICT (46%). Hier geldt eveneens de opmerking dat het resultaat kan vertekend zijn door meerdere respondenten uit hetzelfde bedrijf.

Aanwezigheid van een gedragscode	% vd antwoorden	%
Ja		50 %
Neen		50 %

## CONTEXT

Alvorens de resultaten van het onderzoek te bespreken worden nog enkele concepten toegelicht die het kader van de discussie vormen. Enkele eerdere studies kunnen als referentiemateriaal en duiding dienen bij de interpretatie van de bevindingen.

### **Business Ethiek en CSR**

Ethiek in de onderneming is zeker geen nieuw gegeven. Onder druk van steeds bewustere consumenten en aandeelhouders is dit domein sterk onder de aandacht gekomen in de beleidsvoering van hedendaagse bedrijven, mede door de publieke verontwaardiging die ontstond na het opduiken van frauduleuze praktijken in grote organisaties, genre Enron, Worldcom en Arthur Andersen (Svensson en Wood, 2008). De verstreckende gevolgen van deze zaken schudden wereldwijd de publieke opinie wakker. Ondernemingen worden geacht maatschappelijke verantwoordelijkheid op te nemen voor het beleid dat ze voeren en de impact die ze daarmee op de samenleving hebben. Ethische charters en gedragscodes werden in het leven geroepen waarbij bedrijven zich konden onderscheiden op het gebied van maatschappelijk verantwoorde beleidsvoering.

Business Ethiek wordt gedefinieerd als: “het geheel van morele principes en standaarden dat gedrag in de business wereld aanstuurt” (Dahlin, 2007). Ethiek is een ruimer begrip dan wetgeving, vandaar dat zelfregulering van groot belang is binnen een professie zoals ICT. Hoewel persoonlijke morele verantwoordelijkheid zeer belangrijk is, is in de context van business ethiek een belangrijk vraagstuk hoe moreel of ethisch gedrag kan geïnstitutionaliseerd worden in een organisatie (Van Gerwen, Verstraeten, 1990).

Corporate Social Responsibility (CSR) is dan “de integratie van business activiteiten en waarden waarbij de belangen van alle stakeholders in de organisatie waaronder klanten, werknemers, aandeelhouders, de maatschappij en het milieu weerspiegeld worden in het beleid en de handelingen van een bedrijf” (Dahlin, 2007).

Eén en ander kan worden teruggebracht op het natuurlijke spanningsveld tussen het geprefereerd gedrag van een manager ten opzichte van de professional, in welk domein dan ook. Aan de basis van de managementgedachte ligt het utilitarisme. Utilitarisme is in essentie de ethische stroming die de nutsmaximalisatie als hoogste doel stelt (Bentham, 1780; Mill, 1979). In termen van management komt dat neer op het maximaliseren van de waarde van de organisatie. De beslissingen en het gedrag van de manager zouden als dusdanig geïnspireerd kunnen zijn. De professional daarentegen, wordt eerder verondersteld vanuit een deontologisch principe te handelen waarbij hij of zij de opgelegde taken zo kwaliteitsvol mogelijk tracht uit te voeren binnen de vastgelegde grenzen beschreven in de professionele regels of deontologie van het vakgebied (Rawls, 1972).

### **Ethische aspecten van ICT: welke thema's?**

Een aantal van de belangrijkste aspecten van ICT gebruik en beheer die potentieel ethische vragen oproepen:

- confidentiële informatie
- controle van werknemers
- controle van gebruikers

- intellectuele eigendomsrechten
  - informatiebeheer
  - kwaliteit van software en dienstverlening
- (Healy en Iles, 2002)

### **ICT Gedragscodes**

Eén van de doelen van dit rapport is het mogelijke nut van een ethische gedragscode voor de ICT sector in deze contreien aan te kaarten. Zulke codes bestaan reeds en waren eerder al het onderwerp van verschillende studies. Organisaties kunnen onderhevig zijn aan zulke codes in allerlei vormen en op verschillende niveaus. Er zijn bijvoorbeeld internationale, nationale en sectoriële codes en daarnaast ook nog bedrijfsspecifieke gedragscodes (Van Gerwen, Verstraeten, 1990).

Definitie van een ‘Gedragscode’: “Gedragscodes zijn een middel waarmee organisaties beogen macht en controle uit te oefenen maar hun effectiviteit wordt gecompromitteerd door de aard van ICT zelf zowel als door de houding van werknemers (Healy, Iles, 2002).” Daarbij zijn gedragscodes de moreel toelaatbare grenzen die de leden van een groep zichzelf opleggen. Gedragscodes zijn doorgaans richtinggevend en bieden een houvast voor het prioriteren van conflicterende principes.

Een onderzoek naar het bestaan en de toepassing van ICT gedragscodes werd beschreven door Healy en Iles (2002). In totaal werden in deze studie 125 antwoorden verzameld. De vragenlijst bestond uit een aantal meerkeuzevragen met betrekking tot het organisatieprofiel en het gebruik van gedragscodes in de organisatie. Onderstaande tabellen geven een overzicht van de resultaten van deze studie.

Organisations with codes by sector

Sector	%
Health/medical – private	100.0
Manufacturing	100.0
Finance/banking/insurance	92.6
Government – local/national	86.7
Communications	81.8
Retail/wholesale	71.4
Education	66.7
Charity/non-profit making	54.5
Transport/utilities	50.0
Services	45.5
Health/medical – public	0.0
Other	77.8

**Bron: Healy, Iles, 2002**

Het lijkt erop dat grote organisaties meer gebruik maken van gedragscodes dan kleinere bedrijven en dus meer nood schijnen te hebben aan het expliciteren van wenselijk gedrag. Uit het onderzoek bleek eveneens dat meer organisaties, die in hoge mate van ICT afhankelijk zijn, een ICT gedragscode hebben.

Organisations with codes by size

No. of employees	%
Fewer than 50	50.0
50-99	71.4
100-249	64.7
250-499	50.0
500-999	83.3
1000-4999	76.7
5000+	90.0

**Bron: Healy, Iles, 2002**

Het gebruik van gedragscodes wordt in vraag gesteld door een aantal studies die aantoonen dat de aanwezigheid van een gedragscode in een organisatie geen significante invloed hebben op ethische beslissingname. Omgekeerd is het ook niet bewezen dat het ontbreken van zulke code onethisch gedrag zou bevorderen. Een gedragscode zal pas echt een effectieve invloed op het gedrag van werknemers hebben wanneer de principes uit die code geïntegreerd zijn in de bedrijfsvoering, de organisatiecultuur, etc. Nog verregaander is de verankering van een aantal ethische principes in het performance management systeem. (Mather, 2006; Van Gerwen en Verstraeten, 1990)

Anderzijds vermelden organisaties die het gebruik van ethische codes ondersteunen verschillende voordelen voor de organisatie. Met betrekking tot de ethische code voor software ontwikkelaars die onderschreven werd door ACM en IEEE worden volgende voordelen opgesomd: (SEPEP, 2008)

- Het aantrekken van plichtsbewuste en toegewijde werknemers
- Een betrouwbaar en ethisch imago bij het publiek
- Het aanmeten van een professionele standaard biedt een kwaliteitsvolle reputatie aan het product
- Een betere interne communicatie tussen managers en professionals en tussen collega's onderling






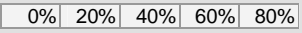
“Zelfs als een code niet echt wordt aangenomen door de doelgroep, in een organisatie of een gemeenschap, zal de code toch een klimaat van ethische bewustwording teweegbrengen” (Olsen, 1998). Volgens Van Gerwen en Verstraeten (1990) zijn de doelstellingen van het gebruik van een dergelijke code het vastleggen van een ethisch minimum dat minstens in acht moet worden genomen door werknemers. Vervolgens het scheppen van duidelijkheid over de verwachtingen van de onderneming naar de werknemers toe. Eveneens het opbouwen van vertrouwen bij de publieke opinie in het algemeen en de klanten in het bijzonder. Tot slot het anticiperen van nieuwe reguleringen door de overheid en om rechtsvervolgning te voorkomen.

## RESULTATEN

We bestuderen per case hoe de antwoorden gespreid zijn over de categorieën onethisch gedrag (score 4-5), te bespreken (score 3) en geen onethisch gedrag (score 1-2). Voor elke case worden ook de relevante commentaren besproken. Ter illustratie van de impact van een ethische gedragscode worden de cases getoetst aan de richtlijnen van de ACM ethische gedragscode, terug te vinden in de appendices.

### Case 1: Intellectuele eigendom:

In de eerste case wordt een geval van intellectuele eigendom besproken. Een software ontwikkelaar komt in tijdsnood door de complexiteit van haar opdracht en wordt door haar directe manager onder druk gezet na een langere periode van ontwikkelen om het project binnen enkele dagen af te werken. Om de deadline te halen gebruikt ze delen van de codering van een commercieel softwarepakket en van het werk van een collega. Ze maakt hiervan geen vermelding maar levert het project wel tijdig op.

Case 1: Intellectuele eigendom	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		6 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		18 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		35 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		13 %
5 Zeer onethisch gedrag met verstrekkende gevolgen voor de betrokkenen.		28 %
Gemiddelde: 3,38	Mediaan: 3	
<b>Aantal antwoorden: 276</b>		

6% van de respondenten geeft aan hier geen probleem in te zien. Iets meer dan een vierde echter vindt deze gang van zaken onaanvaardbaar en duidelijk onethisch in die mate dat er serieuze consequenties aan vast zouden moeten hangen voor de betrokkenen. In deze situatie is er een grote middengroep die twijfelt over de ernst van het vergrijp maar wel ervaart dat dit op zijn minst onrustwekkend gedrag inhoudt vanuit ethisch standpunt.






De commentaren van de respondenten wijzen erop dat de wijze van bescherming van de commerciële software code de impact van het vergrijp beïnvloedt. Indien dit een wettelijk beschermde code is stelt zich een ernstig probleem dat kan leiden tot rechtszaken. Het gebruik van de code van de collega wordt als een minder ernstig vergrijp ervaren, maar zou toch best ook vermeld worden zo luiden de commentaren. Een klein aantal respondenten maakt vermelding van een gedragscode in hun organisatie die soortgelijk gedrag intern reguleert en sanctioneert. Enkel argumenteren hun keuze voor de laagste score, dus geen onethisch gedrag, met de opmerking dat er geen sprake van eigendom kan zijn wanneer het om slechts om delen van code gaat en niet om een volledig pakket. Daarnaast valt ook de opmerking

dat dit gedrag vrij gangbaar is en dat het op tijd opleveren van de gevraagde software toch belangrijker mag geacht worden.

De case bevat een aantal inbreuken op de ACM code. Ten eerste honoreert ze het werk van een collega niet en ten tweede maakt ze gebruik van een commercieel softwarepakket dat vermoedelijk auteursrechtelijke bescherming geniet. De code stelt dat de ICT professional te allen tijde formeel vermelding moet maken van het gebruik van andermans werk (imperatief 1.6). Het naleven van wetgeving, hier met betrekking tot intellectuele eigendom en copyrights, valt onder imperatief 2.3. De software ontwikkelaar had dus zeker moeten nagaan of de commerciële software al dan niet auteursrechtelijk beschermd is en of er van gebruik mocht gemaakt worden (Anderson et al., 1993).

### Case 2: Data beveiliging

Een consulting bedrijf adviseert een middelgrote onderneming bij het ontwerpen van een databank management systeem. De cliënt wordt nauw betrokken bij het proces en moet nu de beslissing nemen welke soort beveiliging in het systeem zal worden opgenomen. De CEO van het bedrijf beslist om de goedkoopste versie met de laagste graad van beveiliging te nemen om de hoger dan verwachte kosten van het project enigszins te drukken. De consultant voelt aan dat deze beveiliging grote risico's inhoudt waarbij werknemers en zelfs hackers toegang zouden kunnen krijgen tot gevoelige data zoals salarissen, evaluaties, medische dossiers, etc. De zorgen worden aan de CEO voorgelegd maar die houdt voet bij stuk ondanks het expliciete advies over de ontoereikende beveiliging.

Case 2: Data beveiliging	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		17 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		15 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		37 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		12 %
5 Zeer onethisch gedrag met verstrekking gevolgen voor de betrokkenen.		19 %
Gemiddelde: 3	Mediaan: 3	
<b>Aantal antwoorden: 250</b>		<input type="checkbox"/> 0% <input type="checkbox"/> 20% <input type="checkbox"/> 40% <input type="checkbox"/> 60% <input type="checkbox"/> 80%

De antwoorden op deze case liggen zeer verspreid. In dit geval werden ook de meeste commentaren toegevoegd door de respondenten. Een grote groep van 37% ziet wel degelijk een probleem maar is niet zeker over de gevolgen die hieraan moeten gegeven worden. De consultant gaf immers het juiste advies. De vraag stelt zich of de consultant moet doorgaan met het project waarbij een onveilig systeem wordt afgeleverd voor de opdrachtgever. 19% ziet duidelijk onethisch gedrag in deze case.






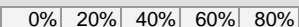
De commentaren leren dat deze groep van respondenten de CEO in hoofdzaak verantwoordelijk acht en dat hij hier zwaar over de schreef gaat en met name de

economische belangen niet boven de persoonlijke en professionele belangen van de werknemer mag stellen. De consultant handelt niet onethisch volgens de commentaren wanneer het advies in de wind wordt geslagen en de consultant bewijs kan leveren van de veronachtzaming van zijn advies. De klant is op de hoogte en draagt de verantwoordelijkheid. Bovendien wordt verschillende malen geargumenteed dat de consultant zich best goed documenteert en op papier laat zetten dat de CEO de verantwoordelijkheid opneemt ingeval de beveiliging faalt. Sommige respondenten oordelen dat de consultant best formeel zou overgaan tot de stopzetting van het project.

De ACM code adresseert zowel privacy als confidentialiteit. ICT professionals hebben de plicht de integriteit van persoonlijke data te vrijwaren van ongeoorloofde toegang of accidentele onthulling ten aanzien van onbevoegde individuen (1.7). De verantwoordelijkheid van de leiders in een organisatie is volgens de code het nagaan dat alle systemen zo ontworpen en geïmplementeerd worden dat persoonlijke privacy en waardigheid van ieder die bij het systeem betrokken is, in bescherming worden genomen (3.4 en 3.5). De software ontwikkelaar moet volgens de code alles in het werk stellen om de beslissingnemers in het bedrijf op hun verantwoordelijkheden te wijzen. Wanneer dit niet helpt moet ze afwegen of haar morele verantwoordelijkheid haar contractuele verplichtingen teniet doet (Anderson et al., 1993).

### Case 3: Vertrouwelijke gegevens

Een persoon werkt op een overheidsdienst ter bestrijding van alcohol en drugsmisbruik. Hij wordt gevraagd een rapport en analyse samen te stellen dat voor alle cliënten van het departement beschrijft welke behandelingen werden gevolgd, of er criminele feiten zijn vastgesteld of de cliënt hervallen is, enzovoort. Hij krijgt voor dit project toegang tot alle bestanden op de mainframe van de overheidsdienst. Om het rapport samen te stellen download hij de data op zijn persoonlijk werkstation in zijn kantoor. Om de deadline te halen besluit hij de gegevens op een aantal disks te kopiëren en thuis verder te werken aan het rapport. Thuis werkt hij het rapport af en vergeet daarna de disks te vernietigen of terug naar het kantoor te brengen.

Case 3: Vertrouwelijke gegevens	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		3 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		10 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		26 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		27 %
5 Zeer onethisch gedrag met verstrekkende gevolgen voor de betrokkenen.		33 %
Gemiddelde: 3,77	Mediaan: 4	
<b>Aantal antwoorden: 239</b>		






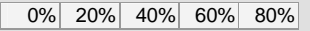
De antwoorden in deze case neigen eerder naar de 'onethische' kant. Ruim 33% ziet het kopiëren en thuis laten slingeren van data als een toonbeeld van zeer onethisch gedrag waaraan duidelijke gevolgen moeten verbonden worden. Slechts 13% van de respondenten vindt het gedrag van de werknemer hier aanvaardbaar of slechts licht verontrustend.

In de aanvullende commentaren wordt een grote afkeuring voor zulke acties duidelijk. De respondenten vinden echter dat een gedragscode hier op zijn plaats is en zulk onaanvaardbaar gedrag kan helpen voorkomen. Iemand maakt melding dat deze praktijk van slordige omgang met gegevens zeer vaak voorkomt hoewel het duidelijk niet acceptabel is. Een opmerkelijke vaststelling is dat velen het wel vinden kunnen mits er toelating is en er geen regels zijn die het meenemen van de informatie verbieden. De werknemer moet daarvan dan wel melding maken en de data achteraf vernietigen. In de actuele tijd met toenemend telewerk zou dit ook voor soortgelijke conflicten kunnen zorgen door misbruik van bedrijfsgegevens die van thuis uit beschikbaar zijn.

In deze case is er een gelijkaardige problematiek met betrekking tot privacy als in case 2. Opnieuw geldt de opmerking dat de ICT professional in zijn gedrag de privacy en confidentialiteit in acht moet nemen en geen mogelijkheden tot onbevoegde toegang mag creëren. De organisatie draagt ook verantwoordelijkheid want zij had door duidelijke beleidsregels kunnen voorkomen dat de gegevens het kantoor verlieten of dat ze niet persoonlijk identificeerbaar waren door een codering van de identiteitsgegevens. (1.7, 1.8, 2.8, 3.3 en 3.5) (Anderson et al., 1993)

#### Case 4: Kwaliteit van geleverd werk

Een ICT bedrijf werkt aan een efficiënt accounting systeem voor de overheid. Het systeem zal de belastingbetaler jaarlijks een substantieel bedrag besparen. De ICT professional, verantwoordelijk voor het ontwerp, verdeelt de taken onder zijn personeel en legt het resultaat voor aan de manager die akkoord gaat dat het systeem aan de vereisten voldoet. Uiteindelijk wordt het systeem geïnstalleerd maar de werknemers vinden de interface moeilijk werkbaar. Hun klachten worden door het hoger management gehoord en men schakelt terug over op het oudere duurdere systeem.

Case 4: Kwaliteit van geleverd werk	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		33 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		17 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		30 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		9 %
5 Zeer onethisch gedrag met verstrekende gevolgen voor de betrokkenen.		12 %
Gemiddelde: 2,50	Mediaan: 3	
<b>Aantal antwoorden: 224</b>		

Van alle cases in de vragenlijst werd deze het minst onethisch bevonden. Ongeveer de helft van de respondenten ziet geen ethische problematiek in dit geval. Een grote groep van 30% twijfelt over de consequenties van het beschreven probleem. Toch is er nog 12% die vinden dat er wel degelijk sprake is van zeer onethisch gedrag in dit verhaal.

Waarom de antwoorden wijzen op weinig of geen onethisch gedrag blijkt uit de commentaren. Er is sprake van onprofessioneel gedrag en foute beslissingen maar voor heel wat respondenten is dit geen ethische kwestie. Gebrekkige kwaliteit is wel degelijk een probleem maar heeft dus geen ethische aspecten in dit geval. Er wordt verwezen naar slecht management en incompetentie. Men adviseert eerder de fouten weg te werken dan heel het nieuwe systeem over boord te gooien. De eindgebruikers zouden vroeger bij het project moeten betrokken worden aldus de commentaren. De vraag rijst of kwaliteit, en vooral het gebrek daaraan, in sommige gevallen toch een ethische kwestie kan zijn.

Volgens de ACM code in elk geval wel. Die stelt expliciet dat de ICT professional moet streven naar de hoogst mogelijke kwaliteit in proces en product (2.1). Een andere regel die hier van toepassing is, is dat gebruikers en betrokkenen hun noden en eisen duidelijk tot uitdrukking kunnen brengen. Het probleem in deze case is de vermoedelijk gebrekkige kwaliteit van het gevolgde proces. Een betere controle procedure tijdens de ontwikkelingsfase, bijvoorbeeld met de eindgebruikers, had deze

afloop kunnen voorkomen. Wanneer het resultaat zoals hier schade toebrengt aan de belastingbetaler is er een duidelijke inbreuk op de ethische code. (2.1, 2.4 en 3.4) (Anderson et al., 1993)

### Case 5: Discriminatie

Een tewerkstellingskantoor stelt de vereisten op voor een informatiesysteem. Ze leggen uit aan de leverancier dat het systeem de kandidaten met geschikte kwalificaties moet kunnen tonen. Voor bepaalde banen echter dienen mannelijke en blanke kandidaten echter voorrang te krijgen in het systeem ten opzichte van vrouwen of kandidaten van een ander ras. Men vraagt de leverancier om dit in het systeem mogelijk te maken.

Case 5: Discriminatie	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		4 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		1 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		11 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		9 %
5 Zeer onethisch gedrag met verstrekkende gevolgen voor de betrokkenen.		76 %
Gemiddelde: 4,52	Mediaan: 5	
<b>Aantal antwoorden: 221</b>		






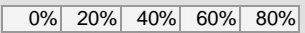
Drie kwart van de respondenten is van oordeel dat deze case duidelijk onethisch gedrag in zich draagt. Een kleine minderheid vindt dat onder bepaalde omstandigheden deze beslissing moet mogelijk zijn.

Een enkeling argumenteert dat deze zaken toch gebeuren dus dat de leverancier de opdracht niet hoeft te weigeren. Een andere commentaar nuanceert de case: in sommige gevallen kan misschien wel degelijk de voorkeur gegeven worden aan blanke of mannelijke kandidaten. Dit zou echter niet systematisch moeten/mogen gebeuren. Anderen raden de leverancier af zulk systeem te leveren. Er is sprake van onethisch en zelfs onwettelijk gedrag. Voor vele respondenten is elke opdracht die discriminatie jegens ras of geslacht inhoudt onaanvaardbaar.

De ACM code is sluitend wat betreft discriminatie. Elk lid dat onder de code valt mag in geen geval deelnemen aan discriminatie. De leverancier van het systeem heeft de plicht de klant aan te spreken over het doel van de discriminerende specificaties. Ingeval er sprake is van discriminatie moet de leverancier weigeren het systeem te bouwen. Volgende regels van professioneel gedrag zijn hier van toepassing: 1.1, 1.2, 1.4, 2.3, 2.5 en 4.1 (Anderson et al., 1993).

### Case 6: Risico op onbetrouwbaarheid

Een software ontwikkelingsfirma heeft een nieuw softwarepakket geproduceerd dat de nieuwe belastingwetgeving bevat en belastingen voor individuele personen en kleine bedrijven afbeeldt. De zaakvoerder van het bedrijf is op de hoogte dat de software een aantal ‘bugs’ bevat. Daarnaast is hij ervan overtuigd dat degene die eerst deze markt betreedt waarschijnlijk het grootste marktaandeel zal veroveren. Het programma wordt op grote schaal geadverteerd. Bij het versturen van de software wordt een disclaimer toegevoegd die elke verantwoordelijkheid afwijst voor problemen of fouten tengevolge het gebruik van de software. Het bedrijf verwacht een aantal klachten en suggesties ter verbetering te zullen ontvangen van klanten die zich gedupeerd voelen. Op grond van deze in te winnen informatie wil de onderneming naderhand een verbeterde versie zonder ‘bugs’ ontwikkelen. De bedrijfsleider argumenteert dat iedereen die een 1.0 versie aanschaft van een programma, deze problemen verwacht en zich erop voorbereidt. Tengevolge van de ‘bugs’ worden verschillende gebruikers gepenaliseerd door de belastingdienst wegens foute gegevensinvoer en -verwerking.

Case 6: Risico op onbetrouwbaarheid	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		1 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		6 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		22 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		24 %
5 Zeer onethisch gedrag met verstrekkinge gevolgen voor de betrokkenen.		46 %
Gemiddelde: 4,08	Mediaan: 4	
<b>Aantal antwoorden: 217</b>		






Meer dan de helft antwoordde dat in dit geval redelijk onethisch tot zeer onethisch gedrag aanwezig is. 22% twijfelt aan de impact van de case maar ziet wel reden tot discussie. Slechts een zeer kleine minderheid vindt het beschreven gedrag niet of nauwelijks onethisch.

Hoewel velen in hun commentaren aanduiden dat deze praktijk vermoedelijk vrij gangbaar is in de software industrie, keuren de meesten dit af. Echter, de uitvlucht “alle software heeft bugs” gaat niet op volgens de respondenten. Bugs die gekend zijn mogen niet ontkend worden door simpelweg een disclaimer toe te voegen. Het bedrijf loopt zelfs het risico op rechtszaken doordat het commerciële belangen voorop stelt boven die van de klanten en hun relatie met de overheid. Iedereen kan fouten maken maar deze bewust exploiteren is onethisch. Toch stelt iemand dat dit gedrag misschien wel laakbaar is maar dat de klanten die zich een 1.0 versie aanschaffen zouden moeten weten dat er ernstige fouten kunnen optreden en zich daarop instellen.

De case bevat een aantal inbreuken op de ACM code. Het publiceren van software met fouten waarvan men op de hoogte is strookt niet met het principe van hoogst mogelijke kwaliteit in de code (2.1). Het niet informeren van de klant betreffende de 'bugs' is een tweede inbreuk (2.5). Vooral omdat het risico in dit geval hoog is voor de gebruiker door de kans op strafmaatregelen tengevolge van de foute belastingaangifte. Er is ook een probleem met het gebruik van de disclaimer. Het management in de organisatie is eveneens in fout door het niet aanmoedigen van het personeel om maatschappelijke verantwoordelijkheid op te nemen (3.1). (Anderson et al., 1993)

### Case 7: Software risico's

Een klein softwarebedrijf werkt aan een geïntegreerd voorraadbeheersysteem voor een groot internationaal bedrijf werkzaam in de schoenendistributie. Het systeem zal worden gebruikt door alle accounting, shipping en ordering departementen wereldwijd. De voorraadfunctie is cruciaal voor de werking van het totale systeem. Hoewel alle contractueel vastgelegde tests werden uitgevoerd, vermoedt de kwaliteitscontroleur van het softwarebedrijf dat de voorraadfunctie onvoldoende getest is. Wettelijk hoeven enkel de contractuele tests uitgevoerd te worden. Toch zegt haar ervaring dat het systeem risico's loopt. Haar werkgevers zeggen haar dat het bedrijf op de helling staat als de software niet tijdig geleverd kan worden. Indien het systeem faalt, schat ze in dat de klant en diens werknemers aanzienlijke schade zullen lijden. Er wacht haar een lastige morele beslissing.

Case 7: Software risico's	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		5 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		19 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		44 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		21 %
5 Zeer onethisch gedrag met verstrekkende gevolgen voor de betrokkenen.		12 %
Gemiddelde: 3,16	Mediaan: 3	
<b>Aantal antwoorden: 209</b>		<input type="checkbox"/> 0%   <input type="checkbox"/> 20%   <input type="checkbox"/> 40%   <input type="checkbox"/> 60%   <input type="checkbox"/> 80%

Uit de spreiding van de antwoorden wordt onmiddellijk duidelijk dat deze case een zeer moeilijk in te schatten situatie bevat. De druk op de beslissing van de kwaliteitscontroleur is zeer hoog. Wat die ook beslist, het is waarschijnlijk dat één van beide partijen schade zal ondervinden. De grote middengroep, 44%, wijst erop dat ook vele respondenten twijfelen welke beslissing de juiste is hier en of er sprake is van onethisch gedrag.






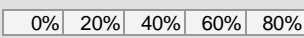
Een aantal commentaren geeft aan dat de verantwoordelijkheid niet bij de kwaliteitscontroleur ligt maar bij de klant. Tenminste wanneer ze aan de klant rapporteert dat additionele tests nodig zijn om potentiële fouten op te sporen. De klant

neemt dan met kennis van zaken een beslissing. Anderzijds wordt het management verweten druk te zetten voor het leveren van risicohoudende software. De kwaliteitscontroleur wordt geadviseerd om haar visie formeel te rapporteren aan zowel de klant als het eigen management en de beslissing aan hen te laten.

Volgens de code is de ICT professional verantwoordelijk om te vermijden dat anderen schade oplopen (1.2). Deze case roept ook vraagtekens op betreffende items 1.1, 1.3 en 2.8 die respectievelijk menselijk welzijn, professionele integriteit en kwaliteit behandelen. Deze case is extra delicaat aangezien er ook een werkgever-werknemer relatie in betrokken is. Op de letter beschouwd zegt de code dat de kwaliteitscontroleur geen systeem mag goedkeuren waarvan ze gelooft dat het van inferieure kwaliteit is, noch mag ze de eindklant in het ongewisse laten over de lage kwaliteit (1.3). Eigenlijk zou ze verder moeten gaan met het testen. Men heeft haar erop gewezen dat dit het falen van de onderneming tot gevolg kan hebben. Zelfs onder die omstandigheden moet ze volgens de ACM code tenminste de klant inlichten over haar bedenkingen (Anderson et al., 1993).

### Case 8: Belangenconflict

Een consultant negotieert een contract met een lokale overheid om hun verkeerscontrolesysteem te ontwerpen. Hij raadt hen daarbij aan het TCS systeem te selecteren uit de beschikbare tools op de markt. De consultant vermeldt niet dat hij één van de hoofdaandeelhouders van het bedrijf is dat TCS produceert.






Case 8: Belangenconflict	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		2 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		4 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		11 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		17 %
5 Zeer onethisch gedrag met verstrekkende gevolgen voor de betrokkenen.		65 %
Gemiddelde: 4,38	Mediaan: 5	
<b>Aantal antwoorden: 209</b>		

Een grote meerderheid vindt deze situatie getuigen van zeer onethisch gedrag. Nochtans legt een klein aantal van de respondenten de verantwoordelijkheid minstens voor een deel bij de klant die zich beter zou moeten informeren. De meerderheid echter vindt dat de consultant zich onder alle omstandigheden bekend moet maken als aandeelhouder van het software bedrijf. In dat geval kan hij alsnog de TCS software aanbevelen bij zijn klant als dat waarlijk de beste oplossing is naar zijn inschatting. Sommigen vinden zelfs dat de consultant onder geen beding objectief kan oordelen in deze situatie.

De regels in de ACM code schrijven voor dat ICT professionals moeten streven naar goede, duidelijke en vooral objectieve evaluaties en aanbevelingen (2.5). Bovendien moet een ICT professional elke mogelijkheid tot belangenvermenging op een eerlijke manier duiden (1.3). (Anderson et al., 1993)

### Case 9: Ongeoorloofde toegang

Joe werkt aan een project voor zijn cursus computerwetenschappen. Zijn leraar heeft hem een beperkte tijd op de computer toegekend voor dit project. Joe raakt in tijdsnood en slaagt er niet in het project binnen de tijd af te werken. De leraar is niet bereikbaar. Joe werkte vorig jaar als student als programmeur aan de ICT afdeling van de campus en kent de procedures om tijd toe te kennen aan de verschillende accounts. Met deze kennis slaagt hij erin in zijn account binnen te dringen en geeft hij zichzelf genoeg tijd om het project af te werken.

Case 9: Ongeoorloofde toegang	% vd antwoorden	%
1 Geen onethisch gedrag in deze case.		1 %
2 Er is reden tot bezorgdheid. Er is geen correctieve actie nodig.		8 %
3 De ethische impact van deze case is discutabel, eventueel kunnen acties volgen.		18 %
4 Er is sprake van onethisch gedrag, een reactie op gebied van sancties en beleid is op zijn plaats.		26 %
5 Zeer onethisch gedrag met verstrekende gevolgen voor de betrokkenen.		46 %
Gemiddelde: 4,08	Mediaan: 4	
<b>Aantal antwoorden: 209</b>		<input type="checkbox"/> 0% <input type="checkbox"/> 20% <input type="checkbox"/> 40% <input type="checkbox"/> 60% <input type="checkbox"/> 80%

Ook in dit geval is er een vrij grote consensus dat het beschreven gedrag onethisch is. Slechts een kleine minderheid vindt dat Joe niet onethisch handelt door zich zonder toestemming toegang tot de systemen te verschaffen en zo zijn werktijd aan te passen.

Wel argumenteren enkelen dat de ICT afdeling betere beveiliging zou moeten hebben om dergelijke misbruiken te vermijden. De student mag zich wel geen onrechtmatige toegang verschaffen tot een systeem ongeacht zijn kennis. Voor de meeste respondenten is hier sprake van fraude.

De case beschrijft een duidelijke inbreuk op imperatieven 1.5 en 2.8 van de ACM code. Die stellen dat de ICT professional zich enkel toegang verschafft tot gegevens wanneer hij daartoe bevoegd is of toestemming heeft gekregen (Anderson et al., 1993).

## DISCUSSIE

Elk van de voorgaande situatiebeschrijvingen stelt de betrokken ICT professional voor een moeilijke beslissing of inschatting. De spreiding van de antwoorden biedt inzichten in hoe Belgische ICT professionals tegenover de situatie staan en meerbepaald welk gedrag zij als ethisch en onethisch beschouwen. We observeren dat er een brede waaier van uiteenlopende meningen bestaat binnen de doelgroep ten aanzien van de voorgelegde cases. Een niet onbelangrijk deelprobleem is de tweeledige verantwoordelijkheid die de ICT professional draagt. Enerzijds heeft die de plicht het beste voor zijn eigen bedrijf te beogen anderzijds wordt ook verantwoordelijkheidszin ten opzichte van het algemeen welzijn of dat van een ander verwacht en vooral een professionele houding.

Een aantal resultaten van deze survey zijn opmerkelijk. Niet in het minst de commentaren die bij sommige cases als argumentatie werden toegevoegd. Deze bieden een uniek beeld van de redenering die men volgt om iets al dan niet onethisch te noemen. Daarnaast bevatten de commentaren ook suggesties om soortgelijke situaties te vermijden of op te lossen. In elk geval kunnen de resultaten een discussie op gang brengen en stofferen betreffende de professionaliteit van het ICT vakgebied in het algemeen en de ethische aspecten ervan in het bijzonder.

Een eerste belangwekkende observatie is dat in een aantal cases zeer grote verdeeldheid bestaat over het al dan niet onethisch zijn en de impact ervan. Meerbepaald in case 1 valt op dat wat voor sommigen diefstal is voor anderen dan weer de gewone gang van zaken betekent. Dit is een kwestie van intellectuele eigendom enerzijds maar heeft toch ook ethische implicaties, namelijk het niet vermelden van een broncode voor software.

In heel wat cases komt heel duidelijk naar voren dat de ICT professional zich vaak in een hachelijke situatie bevindt waar hij een inschatting moet maken of de ethische of economische belangen de doorslag moeten geven. Vaak wordt de professional onder druk gezet door de management hiërarchie. Onmiddellijk dringt zich de vraag op of ethische codes hierop een antwoord kunnen bieden. Managers hebben binnen hun vakgebied nochtans een houvast door de sterke invloed van tendensen als Maatschappelijk Verantwoord Ondernemen (MVO) en Corporate Social Responsibility (CSR). In enkele gevallen wordt de verantwoordelijkheid dan ook terecht doorgeschoven naar het management. Dan nog blijft de vraag overeind of managers opdrachten en voorwaarden opleggen aan de ICT professional binnen ethisch toelaatbare grenzen.

In heel veel commentaren komt het argument terug dat, indien de ICT professional de situatie rapporteert aan het management en in sommige gevallen ook aan de klant, hij niet meer de verantwoordelijkheid draagt van de gevolgen. Toch volstaat volgens bijvoorbeeld de ACM code<sup>2</sup> niet enkel het rapporteren van potentieel onethische situaties om vrijgepleit te zijn van de eventuele gevolgen.

Anderzijds is het opmerkelijk dat toch de helft van de bevroegden aangeeft dat er een soort code of richtlijn gehanteerd wordt in de organisatie. Men kan zich de vraag

---

<sup>2</sup> Zie appendix

stellen hoe deze codes eruit zien en of ze strikt toegepast worden. Daarbij komt het vraagstuk of bedrijfsspecifieke codes de voorkeur genieten op sectorspecifieke codes. De illustraties aan de hand van de ACM code bij de cases die in dit rapport besproken worden geven weer hoe een gedragscode kan toegepast worden en welke impact op de beslissingname die kan hebben.

## SAMENVATTING

Ethische inbreuk	ICT-onethisch (score 4-5)	Te bespreken (score 3)	ICT-ethisch (score 1-2)
1. Intellectuele eigendom	41%	35%	24%
2. Beveiliging van gegevens	31%	37%	32%
3. Bescherming van gevoelige gegevens	61%	26%	13%
4. Software fouten met potentiële morele schade	20%	30%	50%
5. Systematische Discriminatie	84%	11%	5%
6. Software fouten met risico op morele schade	71%	22%	7%
7. Bewust lage kwaliteit van software, kans op economische schade	32%	44%	24%
8. Belangenvermenging	83%	11%	6%
9. Onrechtmatige toegang voor persoonlijk voordeel	73%	18%	9%

## **APPENDICES**

- A. Literatuurlijst**
- B. Relevante websites**
- C. ACM gedragscode**
- D. Gedetailleerde vragenlijst 'Ethische aspecten van ICT'**

## **APPENDIX A: Referenties**

Anderson, R.E., Johnson, D.G., Gotterbarn, D. and Perrolle, J. (1993) "Using the new ACM code of ethics in decision making", in Communications of the ACM, February 1993, Vol.36, No.2

Association for Computing Machinery (ACM), (2008) ACM Code of Ethics and Professional Conduct, online beschikbaar op <http://www.acm.org/about/code-of-ethics>

Bentham, J. (1780) The Principles of Morals and Legislation

Berleur J., Duquenoy P., Holvast J., Jones M., Kimppa K., Sizer R., and Whitehouse D. (2004) Criteria and Procedures for Developing Codes of Ethics or of Conduct, On behalf of IFIP-SIG9.2.2, September 2004

Crane, A., Matten, D. (2004) Business Ethics, Oxford University Press

Dahlin, L.A. (2007) Where have all the Ethics Gone? Business Ethics and Corporate Social Responsibility Through the Years, Proceedings of the Northeast Business & Economics Association; 2007, p360-366

Gotterbarn, D. (1999) Not all Codes are Created Equal: The Software Engineering Code of Ethics, a Success Story, Journal of Business Ethics 22: 81-89, 1999. Kluwer Academic Publishers

Healy, M. and Iles, J. (2002) The Establishment and Enforcement of Codes, Journal of Business Ethics 39: 117-124, 2002

Mather, K. (2006) "Codes of ethics: protecting whose interest?", Information Age 18/10/2006

Mill, John Stuart (1979) Utilitarianism, On Liberty. Essays on Bentham, London

Rawls, J. (1972) A Theory of Justice, Oxford, Oxford University Press

Rogerson, S. (1998) The Ethics of Information and Communication Technologies (ICT) in Business, IMIS Journal Volume 8 No 2, April 1998

Software Engineering Professional Ethics Project (2008) The International Standard for Professional Software Development and Ethical Responsibility, online beschikbaar op [http://seeri.etsu.edu/se\\_code\\_adopter/page.asp?Name=Benefits](http://seeri.etsu.edu/se_code_adopter/page.asp?Name=Benefits)

Svensson, G., Wood, G. (2008) A model of Business Ethics, Journal of Business Ethics 2008 77:303–322 Springer

Van Gerwen, J., Verstraeten, J. (1990) Business & Ethiek: spelregels voor het ethisch ondernemen, Lannoo

Valentine, S. R. and Rittenburg, T. L. (2007) Ethical Decision Making of Men and Women Executives, *Journal of Business Ethics* 71:125–134, Springer

## **APPENDIX B: Relevante websites**

- <http://www.acm.org/sigs/sigcas/codes.html>
- [www.vri.net](http://www.vri.net) 'Webportaal voor en door Nederlandse RegisterInformatici'
- IEEE: <http://www.computer.org>
- Online Ethics Center for Engineering and Science:  
<http://www.onlineethics.org>
- <http://www.info.fundp.ac.be/~jbl/IFIP/cadresIFIP.html>
- <http://www.ethicsweb.ca>

## **APPENDIX C: Gedragscode (ACM) <http://www.acm.org/about/code-of-ethics>**

### **ACM CODE OF ETHICS AND PROFESSIONAL CONDUCT**

Adopted by ACM Council 10/16/92.

#### **Preamble**

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4. The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondly, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards. It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

#### **1. GENERAL MORAL IMPERATIVES.**

As an ACM member I will ....

##### **1.1 Contribute to society and human well-being.**

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare. In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

### **1.2 Avoid harm to others.**

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5 regarding thorough evaluations.

### **1.3 Be honest and trustworthy.**

Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest. Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

### **1.4 Be fair and take action not to discriminate.**

The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors.

However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

**1.5 Honor property rights including copyrights and patent.**

Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

**1.6 Give proper credit for intellectual property.**

Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

**1.7 Respect the privacy of others.**

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

**1.8 Honor confidentiality.**

The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

**2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.**

As an ACM computing professional I will ....

### **2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.**

Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

### **2.2 Acquire and maintain professional competence.**

Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

### **2.3 Know and respect existing laws pertaining to professional work.**

ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

### **2.4 Accept and provide appropriate professional review.**

Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

### **2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.**

Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm, including the reporting of professional violations.

### **2.6 Honor contracts, agreements, and assigned responsibilities.**

Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority. A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed.

Regardless of the decision, one must accept the responsibility for the consequences. However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

### **2.7 Improve public understanding of computing and its consequences.**

Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

### **2.8 Access computing and communication resources only when authorized to do so.**

Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 - "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4). No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

## **3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.**

As an ACM member and an organizational leader, I will ....

**BACKGROUND NOTE:** This section draws extensively from the draft IFIP Code of Ethics, especially its sections on organizational ethics and international concerns. The ethical obligations of organizations tend to be neglected in most codes of professional conduct, perhaps because these codes are written from the perspective of the individual member. This dilemma is addressed by stating these imperatives from the perspective of the organizational leader. In this context "leader" is viewed as any organizational member who has leadership or educational responsibilities. These imperatives generally may apply to organizations as well as their leaders. In this context "organizations" are corporations, government agencies, and other "employers," as well as volunteer professional organizations.

### **3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.**

Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

**3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.**

Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

**3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.**

Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

**3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.**

Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

**3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.**

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

**3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.**

This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

**4. COMPLIANCE WITH THE CODE.**

As an ACM member I will ....

**4.1 Uphold and promote the principles of this Code.**

The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

**4.2 Treat violations of this code as inconsistent with membership in the ACM.**

Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

## APPENDIX D: 'Ethical Aspects of ICT' Survey

\* **Case 1: Intellectual Property** Jean, a statistical database programmer, is trying to write a large statistical program needed by her company. Programmers in this company are encouraged to write about their work and to publish their algorithms in professional journals. After months of tedious programming, Jean has found herself stuck on several parts of the program. Her manager, not recognizing the complexity of the problem, wants the job completed within the next few days. Not knowing how to solve the problems, Jean remembers that a coworker had given her source listings from his current work and from an early version of a commercial software package developed at another company. On studying these programs, she sees two areas of code which could be directly incorporated into her own program. She uses segments of code from both her coworker and the commercial software, but does not tell anyone or mention it in the documentation. She completes the project and turns it in a day ahead of time.

1  
There is little or no unethical behaviour in this case

2  
There is a slight concern but no actions are required.

3  
The ethical impact of this case is to be discussed, reactions might follow.

4  
Slightly unethical behaviour, some consequences in terms of sanctions and policies.

5  
Clearly unethical behaviour, serious consequences on involved persons and internal policies.

Your comments (optional)?

\* **Case 2: Privacy** Three years ago Diane started her own consulting business. She has been so successful that she now has several people working for her and many clients. Their consulting work included advising on how to network microcomputers, designing database management systems, and advising about security. Presently she is designing a database management system for the personnel office of a medium-sized company. Diane has involved the client in the design process, informing the CEO, the director of computing, and the director of personnel about the progress of the system. It is now time to make decisions about the kind and degree of security to build into the system. Diane has described several options to the client. Because the system is going to cost more than they planned, the client has decided to opt for a less secure system. She believes the information they will be storing is extremely sensitive. It will include performance evaluations, medical records for filing insurance claims, salaries, and so forth. With weak security, employees working on microcomputers may be able to figure out ways to get access to this data, not to mention the possibilities for on-line access from hackers. Diane feels strongly that the system should be much more secure. She has tried to explain the risks, but the CEO, director of computing and director of personnel all agree that less security will do.

1  
There is little or no unethical behaviour in this case.

2  
There is a slight concern but no actions are required.

3  
The ethical impact of this case is to be discussed, reactions might follow.

4  
Slightly unethical behaviour, some consequences in terms of sanctions and policies.

5  
Clearly unethical behaviour, serious consequences on involved persons and internal policies.

**Your comments (optional)?**

\* **Case 3: Confidentiality** Max works in a large state department of alcoholism and drug abuse. The agency administers programs for individuals with alcohol and drug problems, and maintains a huge database of information on the clients who use their services. Some of the data files contain the names and current addresses of clients. Max has been asked to take a look at the track records of the treatment programs. He is to put together a report that contains the number of clients seen in each program each month for the past five years, length of each client's treatment, number of clients who return after completion of a program, criminal histories of clients, and so on. In order to put together this report, Max has been given access to all files in the agency's mainframe computer. After assembling the data into a new file that includes the client names, he downloads it to the computer in his office. Under pressure to get the report finished by the deadline, Max decides he will have to work at home over the weekend in order to finish on time. He copies the information onto several disks and takes them home. After finishing the report he leaves the disks at home and forgets about them.

1  
There is little or no unethical behaviour in this case.

2  
There is a slight concern but no actions are required.

3  
The ethical impact of this case is to be discussed, reactions might follow.

4  
Slightly unethical behaviour, some consequences in terms of sanctions and policies.

5  
Clearly unethical behaviour, serious consequences on involved persons and internal policies.

**Your comments (optional)?**

\* **Case 4: Quality In Professional Work** A computer company is writing the first stage of a more efficient accounting system that will be used by the government. This system will save taxpayers a considerable amount of money every year. A computer professional, who is asked to design the accounting system, assigns different parts of the system to her staff. One person is responsible for developing the reports; another is responsible for the internal processing; and a third for the user interface. The manager is shown the system and agrees that it can do everything in the requirements. The system is installed, but the staff finds the interface so difficult to use that their complaints are heard by upper-level management. Because of these complaints, upper-level management will not invest any more money in the development of the new accounting system and they go back to their original, more expensive system.

1  
There is little or no unethical behaviour in this case.

2  
There is a slight concern but no actions are required.

3  
The ethical impact of this case is to be discussed, reactions might follow.

4  
Slightly unethical behaviour, some consequences in terms of sanctions and policies.

5  
Clearly unethical behaviour, serious consequences on involved persons and internal policies.

Your comments (optional)?

\* **Case 5: Fairness and Discrimination** In determining requirements for an information system to be used in an employment agency, the client explains that, when displaying applicants whose qualifications appear to match those required for a particular job, the names of white applicants are to be displayed ahead of those of nonwhite applicants, and names of male applicants are to be displayed ahead of those of female applicants.

1  
There is little or no unethical behaviour in this case.

2  
There is a slight concern but no actions are required.

3  
The ethical impact of this case is to be discussed, reactions might follow.

4  
Slightly unethical behaviour, some consequences in terms of sanctions and policies.

5  
Clearly unethical behaviour, serious consequences on involved persons and internal policies.

Your comments (optional)?

\* **Case 6: Liability for Unreliability** A software development company has just produced a new software package that incorporates the new tax laws and figures taxes for both individuals and small businesses. The president of the company knows that the program has a number of bugs. He also believes the first firm to put this kind of software on the market is likely to capture the largest market share. The company widely advertises the program. When the company actually ships a disk, it includes a disclaimer of responsibility for errors resulting from the use of the program. The company expects it will receive a number of complaints, queries, and suggestions for modification. The company plans to use these to make changes and eventually issue updated, improved, and debugged versions. The president argues that this is general industry policy and that anyone who buys version 1.0 of a program knows this and will take proper precautions. Because of bugs, a number of users filed incorrect tax returns and were penalized by the IRS.

1  
There is little or no unethical behaviour in this case.

2  
There is a slight concern but no actions are required.

3  
The ethical impact of this case is to be discussed, reactions might follow.

4  
Slightly unethical behaviour, some consequences in terms of sanctions and policies.

5  
Clearly unethical behaviour, serious consequences on involved persons and internal policies.

Your comments (optional)?

\* **Case 7: Software Risks** A small software company is working on an integrated inventory control system for a very large national shoe manufacturer. The system will gather sales information daily from shoe stores nationwide. This information will be used by the accounting, shipping, and ordering departments to control all of the functions of this large corporation. The inventory functions are critical to the smooth operation of this system. Jane, a quality assurance engineer with the software company, suspects that the inventory functions of the system are not sufficiently tested, although they have passed all their contracted tests. She is being pressured by her employers to sign off on the software. Legally she is only required to perform those tests which had been agreed to in the original contract. However, her considerable experience in software testing has led her to be concerned over risks of the system. Her employers say they will go out of business if they do not deliver the software on time. Jane contends if the inventory subsystem fails, it will significantly harm their client and its employees. If the potential failure were to threaten lives, it would be clear to Jane that she should refuse to sign off. But since the degree of threatened harm is less, Jane is faced by a difficult moral decision.

1  
There is little or no unethical behaviour in this case.

2  
There is a slight concern but no actions are required.

3  
The ethical impact of this case is to be discussed, reactions might follow.

4  
Slightly unethical behaviour, some consequences in terms of sanctions and policies.

5  
Clearly unethical behaviour, serious consequences on involved persons and internal policies.

**Your comments (optional)?**

\* **Case 8: Conflict of Interests** A software consultant is negotiating a contract with a local community to design their traffic control system. He recommends they select the TCS system out of several available systems on the market. The consultant fails to mention that he is a major stockholder of the company producing TCS software.

1 There is little or no unethical behaviour in this case.	2 There is a slight concern but no actions are required.	3 The ethical impact of this case is to be discussed, reactions might follow.	4 Slightly unethical behaviour, some consequences in terms of sanctions and policies.	5 Clearly unethical behaviour, serious consequences on involved persons and internal policies.
--	---	--	--	---

Your comments (optional)?

\* **Case 9: Unauthorized Access** Joe is working on a project for his computer science course. The instructor has allocated a fixed amount of computer time for this project. Joe has run out of time, but he has not yet finished the project. The instructor cannot be reached. Last year Joe worked as a student programmer for the campus computer center and is quite familiar with procedures to increase time allocations to accounts. Using what he learned last year, he is able to access the master account. Then he gives himself additional time and finishes his project.

1 There is little or no unethical behaviour in this case.	2 There is a slight concern but no actions are required.	3 The ethical impact of this case is to be discussed, reactions might follow.	4 Slightly unethical behaviour, some consequences in terms of sanctions and policies.	5 Clearly unethical behaviour, serious consequences on involved persons and internal policies.
--	---	--	--	---

**Your comments (optional)?**

**\* Your organisation has ...**

- 0-100 employees.
- 100-500 employees.
- 500-1000 employees.
- more than 1000 employees.

**What is your gender?**

- Female
- Male

**What is your age group?**

- 21-30
- 31-40
- 41-50
- 51-60
- 60+

\* **Please indicate your industry.**

- Manufacturing
- Utilities
- Finance/insurance
- Government
- Consulting
- ICT
- Healthcare
- Other, please specify  
.....

**Have you ever encountered situations in which ethical issues arised regarding ICT?**

- Yes
- No

\* **Does your organisation have an internal policy on ICT ethics?**

- Yes
- No

\* **In your organisation, ICT is ...**

- a supporting function.
- a strategic driver.