Richtlijnen en toezicht inzake het gebruik van de ICT-middelen aan de hogeschool

Situering

De werkgever heeft de bevoegdheid om richtlijnen vast te stellen voor het gebruik van de ICT-middelen die hij ter beschikking stelt van zijn personeelsleden en van andere gebruikers. Deze richtlijnen zijn opgenomen in de punten 1 t/m 9.

Een commissie ICT-deontologie waakt over de uitvoering van deze richtlijnen: zo zal de commissie samenkomen telkens een actualisering van de richtlijn zich opdringt of telkens er twijfel rijst over de uitvoering er van.

De commissie wordt als volgt samengesteld: het diensthoofd Informatica, twee ombudspersonen voor personeel (één van de vroegere HUB-EHSAL en één van de vroegere KAHO Sint-Lieven), twee ombudspersonen voor studenten (één van de vroegere HUB-EHSAL en één van de vroegere KAHO Sint-Lieven), een jurist van de hogeschool en de personeelsdirecteur.

Het toezicht op het gebruik van de ICT-middelen is geregeld in punt 10. Voor personeelsleden met een arbeiders-of bediendestatuut geldt hier in het bijzonder CAO nr.81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens. O.w.v. de transparantie is het aangewezen om ook voor de andere personeelsleden deze CAO te volgen.

De CAO bepaalt dat controle door de werkgever op het gebruik van de online communicatiemiddelen door de werknemers toegestaan is. De controle moet wel gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt.

De organisatie van het toezicht moet volgens CAO nr. 81 niet goedgekeurd worden op de Ondernemingsraad, maar deze moet wel geïnformeerd worden en vervolgens ook de individuele personeelsleden. Overeenkomstig het hogescholendecreet wordt dit document overlegd (niet: onderhandeld) in het Hogeschoolonderhandelingscomité in de mate dat (vanuit artikel 302, §1 van het hogescholendecreet) toepassing wordt gemaakt van artikel 11 van de wet van 19 december 1974 tot regeling van de betrekkingen tussen de overheid en de vakbonden van haar personeel.

Om een werkbaar instrument te creëren, werd gekozen voor één tekst die zowel de richtlijnen als het toezicht bevat en die geldt voor alle gebruikers, zowel personeelsleden, studenten als externen. De tekst vormt tevens de noodzakelijke uitwerking van de principes inzake gebruik en toezicht, zoals opgenomen in de geldende arbeidsreglementen.

Mogelijke sancties bij overtreding van de richtlijnen door personeelsleden zijn de sancties opgenomen in de geldende arbeidsreglementen (voor benoemde personeelsleden spreken

we over tuchtmaatregelen i.p.v. sancties). Voor studenten is er een koppeling met de tuchtprocedure en de tuchtsancties opgenomen in de onderwijs-en examenregeling.

Dat betekent dat:

- de studiegebieddirecteur bevoegd is voor het gesprek met de student dat moet plaatsvinden vóór iedere beslissing die de student individueel kan raken en dat de studiegebieddirecteur een tuchtbeslissing kan nemen ten aanzien van de student (tenzij de student verkiest dat de tuchtcommissie een beslissing neemt, conform artikel 97 van de onderwijs-en examenregeling)
- de personeelsdirecteur bevoegd is voor het gesprek met het personeelslid dat moet plaatsvinden vóór iedere beslissing die het personeelslid individueel kan raken, en dat de personeelsdirecteur of de algemeen directeur een sanctie of tuchtmaatregel kan nemen ten aanzien van het personeelslid
- de algemeen beheerder of een ander lid van het DC bevoegd is voor externe gebruikers (zowel voor het gesprek als voor de beslissing tenzij de beslissing behoort tot de bevoegdheid van de afgevaardigd bestuurder).

1. Doel en toepassingsgebied

De hogeschool stelt heel wat ICT-middelen ter beschikking voor educatieve, wetenschappelijke, administratieve en communicatieve doeleinden. Het gebruik ervan wordt sterk aangemoedigd voor het verbeteren van de kwaliteit van de kernactiviteiten van de instelling: onderwijs, onderzoek en maatschappelijke dienstverlening. De hogeschool beslist welke ICT-middelen ondersteund worden en welke niet.

De hierna volgende regels waarborgen een waardig, gedisciplineerd en veilig gebruik van de ICT-middelen.

Deze richtlijnen gelden voor alle personeelsleden, externen met ICT-faciliteiten van de hogeschool, en voor de studenten ingeschreven aan de hogeschool. Hierna worden zij gezamenlijk aangeduid als de gebruiker(s).

De gebruiker is er zich van bewust dat de hogeschool het netwerkgedrag van alle ICT-middelen logt en dat de hogeschool de goede werking van de netwerken kan controleren op basis van die logs. Deze controles gebeuren binnen de geldende wettelijke omgeving.

Personeelsleden die voor de uitoefening van hun professionele werkzaamheden aan de hogeschool geen ICT-middel voorhanden hebben, hebben het recht om hun e-mailadres van de hogeschool en het intranet van de hogeschool regelmatig te raadplegen op de werkplaats. Hierover worden afspraken gemaakt tussen deze personeelsleden en hun direct leidinggevende.

Leidinggevenden kunnen een out-of-office boodschap op de mailbox van een gebruiker laten instellen indien de continuïteit van de dienstverlening dit vereist.

De richtlijnen gelden voor alle ICT-middelen, IT-infrastructuur en elektronische communicatiemiddelen en voor alle gegevens die door die systemen worden verzonden of

erin worden opgeslagen. De richtlijnen gelden evenzeer voor ICT-middelen, al dan niet eigendom van de hogeschool, die men in relatie met de hogeschool gebruikt (bijvoorbeeld e-mailadres van de hogeschool) of in combinatie met de ICT-middelen van de hogeschool (bijvoorbeeld toegang tot het WiFi netwerk op de campussen, ...).

De Commissie ICT-deontologie (hierna genoemd de commissie) waakt over de uitvoering van de richtlijnen[1]. Aangezien ICT-middelen en de wettelijke omgeving steeds evolueren, zal de commissie samen komen om de richtlijnen te toetsen en zo nodig aan te passen telkens de gewijzigde omstandigheden dit vereisen. Het aangepaste document zal aan de gebruikers worden meegedeeld.

Vragen, opmerkingen en suggesties in verband met deze richtlijnen kunnen gericht worden aan de commissie via het e-mailadres: ICTdeontologie@hubkaho.be. Bij hoogdringendheid wordt het diensthoofd Informatica gecontacteerd.

2. Omgaan met informatie

Elke gebruiker is verantwoordelijk voor de informatie die hij/zij in functie van zijn activiteit aan de hogeschool beheert en opvraagt.

De toegang tot de toepassingen en de gegevens op de computersystemen van de hogeschool wordt enkel verleend door de gebruiker die daarvoor bevoegd is. De toegang is individueel en niet overdraagbaar.

Alle informatie van de hogeschool gerelateerd aan personeel, studenten, onderzoek en administratieve systemen, is eigendom van de hogeschool en moet met de grootste voorzichtigheid behandeld worden.

Bepaalde informatie van de hogeschool is vertrouwelijk en moet met bijzondere aandacht worden benaderd. Om te bepalen in welke mate informatie vertrouwelijk is, moet men zich afvragen wat het risico is voor de hogeschool van een ongepaste verspreiding, zoals:

a. het verlies van economische waarde, bijvoorbeeld informatie over de ontwikkeling van nieuwe diensten, onderzoeksgegevens of meer algemeen informatie, ongeacht de vorm waarin deze is opgeslagen, waarvan de hogeschool rechthebbende is.
b. de aantasting van het imago van de hogeschool, bijvoorbeeld door de verspreiding van gevoelige informatie die leidt tot negatieve publiciteit;
c. een inbreuk op de wetgeving, bijvoorbeeld de wetgeving ter bescherming van de intellectuele rechten, in het bijzonder de auteursrechten of de wetgeving tot bescherming van de persoonlijke levenssfeer bij de verwerking van de persoonsgegevens (salaris-en andere betalingsgegevens, gegevens betreffende personeels-en studentenadministratie, medische persoonsgegevens,

[1] De commissie is als volgt samengesteld: het diensthoofd Informatica, twee ombudspersonen voor personeel (één van de vroegere HUB-EHSAL en één van de vroegere KAHO Sint-Lieven), twee ombudspersonen voor studenten (één van de vroegere HUB-EHSAL en één van de vroegere KAHO Sint-Lieven), een jurist van de hogeschool en de personeelsdirecteur.

toetsen/examenopgaven, examenresultaten, e.a. zijn persoonsgegevens in de zin van deze wet);

d. overdracht van informatie afkomstig van derden waarmee een akkoord van niet-verspreiding werd afgesloten.

Vertrouwelijkheid van informatie geldt als uitgangspunt. Ook informatie die niet uitdrukkelijk als vertrouwelijk bestempeld wordt, mag niet zomaar openbaar of publiek gesteld worden. Bij twijfel kan advies worden ingewonnen bij de commissie en/of bij één van de juristen van de hogeschool.

Vertrouwelijke informatie mag niet buiten de hogeschool worden bijgehouden tenzij hierover afspraken bestaan zoals bij thuiswerk of gebruik van cloud. Indien die afspraken wijzigen of aflopen, moet de informatie al naar gelang van het geval, teruggebracht of vernietigd worden.
Speciale aandacht wordt besteed aan draagbare media die vertrouwelijke informatie bevatten, zoals informatie opgeslagen als back-up. Deze media moeten steeds veilig opgeborgen worden. Bij vernietiging en eventueel hergebruik ervan, moet er op gelet worden dat ze geen vertrouwelijke informatie meer bevatten.

Op het internet (vb. sociale media), op persoonlijke webpagina's en blogs, mag geen informatie onderhevig aan copyright van de hogeschool of vertrouwelijke informatie over andere gebruikers of over de hogeschool worden vrijgegeven tenzij hiervoor een uitdrukkelijke, voorafgaande toelating is gegeven.

3. Verantwoordelijkheden van de gebruiker

De gebruiker verbindt er zich toe om elk slecht functioneren of misbruik van ICT-middelen, IT-infrastructuur en elektronische communicatiemiddelen, of lacunes in de beveiliging, onmiddellijk te melden aan de dienst Informatica.

De gebruiker die merkt dat hij/zij toegang heeft tot informatie waarvoor hij/zij niet gemachtigd is, meldt dit onmiddellijk aan de dienst Informatica.

De gebruiker verbindt er zich toe om de door de hogeschool voorziene beveiligingsmiddelen te gebruiken en de opgelegde beveiligingsmaatregelen toe te passen (vb. wijziging van wachtwoord).

De gebruiker behandelt alle informatica-infrastructuur met de noodzakelijke zorg en voorzichtigheid. Alleen laptops en hun mobiele randapparatuur mogen door de gebruiker verplaatst worden, tenzij toelating wordt gegeven voor verplaatsing van andere infrastructuur.

De gebruiker dient de volgende regels in acht te nemen, voor zover ze toepasbaar zijn op de categorie waartoe de gebruiker behoort:

1. het gebruik van de ICT-middelen
    a. het juist registreren en opslaan van bestanden op gedeelde locaties zodat de gebruikers die als back up fungeren toegang hebben tot de documenten

b. in goede toestand bewaren van de ICT-middelen
c. niet onbeheerd achterlaten van de ICT-middelen en het nemen van voldoende veiligheidsmaatregelen om diefstal ervan te verhinderen;
d. enkel programmatuur installeren of gebruiken op het ICT-middel waarvoor de nodige licenties of gebruiksafspraken aanwezig zijn
e. nemen van voldoende veiligheidsmaatregelen die de mogelijkheid tot het inbreken op de systemen van de hogeschool en diefstal van informatie zo klein mogelijk maakt, bijvoorbeeld door:
   a. het afsluiten van de werkplek/de pc bij afwezigheid;
   b. het activeren van de schermbeveiliging van de pc/werkstation en andere ICT-middelen;
   c. het beveiligen van alle ICT-middelen die op het netwerk verbonden worden en alle vertrouwelijke en bedrijfsgevoelige informatie die op deze ICT-middelen bewaard worden
   d. inloggen vanop externe locaties via beveiligde protocollen

2. de veiligheid van de gegevens die bewaard worden op de systemen:
   a. verifiëren of de gegevens vrij zijn van virussen en andere kwaadaardige software, in het bijzonder:
      - de geïnstalleerde virusscanner niet uitschakelen;
      - een virus, een verdachte e-mail of een verdacht document, onmiddellijk verwijderen; eventueel moet er eerst contact opgenomen worden met de systeem- of netwerkbeheerder
      - programmatuur en gegevens verkregen via een extern netwerk of via draagbare media moeten door of op vraag van de gebruiker gecontroleerd worden op virussen en andere kwaadaardige software;
      - bij de installatie van programmatuur moet steeds met de grootste voorzichtigheid te werk gegaan worden;
      - programmatuur van illegale of twijfelachtige oorsprong mag niet geïnstalleerd worden;
   b. op regelmatige tijdstippen lezen van zijn/haar e-mail en het opruimen en eventueel archiveren van zijn/haar postbus. Indien nodig kunnen systeem-of netwerkbeheerders ingrijpen op de omvang van de mailboxen. Dit kan pas gebeuren na een voorafgaande mededeling waarbij de gebruiker de nodige tijd krijgt om de gegevens in zijn postbus zodanig te bewaren dat dit geen verder gevaar voor het systeem oplevert;
   c. naleven van de bestaande regels voor het maken van een reservekopie binnen de organisatorische eenheid; indien gegevens op lokale harde schijven geplaatst worden (bijvoorbeeld draagbare computer, USB-stick), moet de gebruiker zorgen voor de noodzakelijke reservekopie;

3. het voorzichtig omgaan met de vraag om persoonsgegevens door te geven zoals het e-mailadres;

4. het voorzichtig omgaan met bestanden van onbekende oorsprong zoals bijlagen;

5. het voorzichtig omgaan met inloggen op het netwerk van de hogeschool van op externe locaties

6. het niet versturen van virussen of virusmeldingen (hoaxen) vanop het netwerk van de hogeschool

7. het respecteren van de algemeen geldende beleefdheidsregels.

Bij twijfel moet steeds contact opgenomen worden met de systeem-of netwerkbeheerder, met de commissie en/of met één van de juristen van de hogeschool.

Wanneer noodzakelijk (vb. bij diefstal of verlies) mag de hogeschool alle of gedeeltelijke toegangen van de ICT-middelen die aangesloten zijn op het netwerk van de hogeschool, blokkeren. Zo nodig mogen data en applicaties op deze ICT-middelen gewist worden vanop afstand en mogen de toestellen onbruikbaar gemaakt worden. Bij externe ICT-middelen die geen eigendom zijn van de hogeschool, gebeurt dit in samenspraak met de eigenaar van het ICT-middel.

Wanneer dit om organisatorische, technische of wettelijke redenen vereist is, kan de hogeschool de toegang tot bepaalde websites, apps, betaalnummers en (interne en externe) toegangen afsluiten, al dan niet tijdelijk.

Voor externe, niet door de hogeschool ondersteunde, ICT-middelen is de eigenaar/gebruiker volledig en uitsluitend verantwoordelijk. Deze verantwoordelijkheid geldt zowel de implementatie van de noodzakelijke beveiliging, backup en restore, verlies en diefstal, het onderhoud en het beheer van het ICT-middel en de data opgeslagen op het externe ICT-middel.

4. Wachtwoorden en loginnamen

Iedere gebruiker is verantwoordelijk en aansprakelijk voor alles wat onder zijn/haar loginnaam en wachtwoord gebeurt. Alle draagbare computers die vertrouwelijke informatie over de hogeschool bevatten, moeten worden beschermd, bijvoorbeeld met een opstart-wachtwoord en een schermbeveiliging om de inhoud van de gegevens zo optimaal mogelijk te beveiligen.

Wachtwoorden mogen niet in zichtbare (post-it, ...) vorm worden opgeslagen. Het ingeven van wachtwoorden gebeurt met de nodige voorzichtigheid (vb. niet als iemand toekijkt).

Gebruikers mogen hun wachtwoord niet doorgeven aan andere gebruikers of derden.

Gebruikers die inzage hebben in dossiers betreffende de boekhouding, het personeel, kandidaat-werknemers of de studenten van de hogeschool, en gebruikers die inzage kunnen hebben in de elektronische online communicatiegegevens van personeelsleden of studenten, of kennis krijgen van andere vertrouwelijke gegevens, mogen hun wachtwoord niet doorgeven aan andere gebruikers of derden, tenzij wegens uitzonderlijke omstandigheden en

met uitdrukkelijke toelating van hun leidinggevende. In dit geval wordt het wachtwoord zo snel mogelijk gewijzigd.

Voor sociale media en netwerken voor persoonlijke doeleinden moet de gebruiker een wachtwoord en loginnaam gebruiken die verschillend zijn van de login en het wachtwoord van de hogeschool.

5. Persoonlijk gebruik van ICT-middelen van de hogeschool

Bij persoonlijk gebruik blijven de richtlijnen voor het gebruik van de ICT-middelen aan de hogeschool van kracht.

Enkel voor personeelsleden-gebruikers: de hogeschool laat het persoonlijke gebruik toe van haar ICT-middelen voor zover dit geen nadelige invloed heeft op de arbeidsprestaties die van de gebruiker worden verwacht. Ook moet het persoonlijke gebruik op elk ogenblik ondergeschikt zijn aan het professionele gebruik. In voorkomend geval moet de gebruiker de niet geleverde (arbeids)prestaties inhalen.

Indien de hogeschool vaststelt dat er sprake is van overmatig persoonlijk gebruik, kan de hogeschool op eender welk ogenblik als ordemaatregel beslissen het persoonlijk gebruik voor een bepaalde periode te verbieden.

Enkel voor studenten-gebruikers: er wordt altijd voorrang verleend aan studiedoeleinden in het gebruik van de gemeenschappelijk ter beschikking gestelde ICT-middelen.

Voor alle gebruikers: de andere gebruikers mogen door het persoonlijke gebruik niet gestoord worden, de IT-infrastructuur van de hogeschool mag niet overdreven belast worden en er mogen geen kosten aan verbonden zijn voor de hogeschool. Zo niet worden de gemaakte kosten voor persoonlijk gebruik op de gebruiker verhaald.

Gebruikers die persoonlijke gegevens op ICT-middelen van de hogeschool opslaan en verwerken, moeten er zich bewust van zijn dat de hogeschool de bevoegdheid heeft om in uitzonderlijke gevallen kennis te nemen van informatie die door een gebruiker verwerkt wordt op ICT-middelen van de hogeschool. Ten aanzien van personeelsleden mogen leidinggevenden dit doen indien dit voor de opdracht van de hogeschool absoluut noodzakelijk is. De commissie wordt in dat geval altijd op de hoogte gebracht. Tenzij dit onmogelijk is, wordt ook de betrokken gebruiker geïnformeerd. In elk geval wordt zoveel mogelijk de persoonlijke levenssfeer van de betrokken gebruiker beschermd.

Ter bescherming van persoonlijke gegevens die door de gebruiker worden opgeslagen op ICT-middelen van de hogeschool, is het aan te bevelen om deze gegevens in een map op de persoonlijke schijf (de H-schijf)[2] te bewaren met een referentie naar persoonlijk gebruik.

[2] De persoonlijke schijf is bedoeld voor professioneel gebruik en niet voor strikt persoonlijk gebruik. Het onderscheid met de gemeenschappelijke schijven of de collaboration op het intranet, bestaat erin dat de toegang tot de persoonlijke schijf beperkt is tot het individuele personeelslid.

De hogeschool is niet verantwoordelijk voor eventueel verlies van persoonlijke data die op de ICT-middelen van de hogeschool worden bewaard.

6. Ongeoorloofd gebruik

Onder meer in de volgende situaties is er sprake van ongeoorloofd gebruik:

1. informatie verspreiden, opslaan of invoeren die:
   a. het imago, de morele of economische belangen van de hogeschool kan schaden;
   b. beledigend, lasterlijk, aanstootgevend of discriminerend is;
   c. schade kan toebrengen aan derden;
   d. strijdig is met de geldende wetgeving, openbare orde of goede zeden;
2. vertrouwelijke informatie, zoals bedrijfsgeheimen, persoonlijke gegevens, e.a., doorgeven aan personen die niet gerechtigd zijn om deze informatie te ontvangen;
3. vertrouwelijke informatie onbeschermd bewaren, zowel elektronisch als op papier;
4. bedrijfsdata kopiëren voor andere doeleinden dan professionele –of studiedoeleinden naar locaties buiten het netwerk van de hogeschool zonder voorafgaandelijke, schriftelijke toestemming. Alle data moeten teruggegeven worden aan de hogeschool bij het beëindigen van de (medewerking aan de) opdracht waaraan de data gerelateerd zijn;
5. persoonlijk verkregen gebruiksrechten en licenties van de hogeschool doorgeven aan derden;
6. wachtwoorden en gebruikersgegevens van andere gebruikers proberen te verkrijgen;
7. een valse identiteit aannemen op het netwerk;
8. de beveiliging van systemen of informatie in het gedrang brengen door
   a. interne of externe systeem-en netwerkbeveiliging te omzeilen
   b. programmatuur te installeren of te gebruiken waarvoor geen toestemming is verleend of geen licentie is[3]
   c. de wetgeving over het auteursrecht en andere intellectuele rechten te schenden (vb. programmatuur kopiëren tenzij dit door de licentie van de leverancier of door de wet is toegestaan)
   d. ICT-apparatuur die geen eigendom is van de hogeschool, aankoppelen zonder uitdrukkelijke toestemming van de systeem-of netwerkbeheerder
   e. de toegang te forceren tot systemen waartoe men niet gerechtigd is
   f. het netwerk af te luisteren
   g. derden op de hoogte te brengen van lacunes in de beveiliging;
9. een groot aantal ongewenste of ongevraagde elektronische berichten [4]of kettingbrieven verspreiden;
10. andere gebruikers storen bij het uitoefenen van hun activiteiten of pogingen ondernemen om een dienst, netwerk of computer te verstoren vb. door een netwerk of computer te overbelasten;

[3] Informatica streeft naar 3 gescheiden systemen in de toekomst (3 layers): layer 1, dit is een onbeveiligd netwerk, waar alle gebruikers op kunnen (Bring Your Own Device) maar geen toegang is tot de back office (operationele omgeving); layer 2, dit is een semi-beveiligd systeem toegankelijk voor de personeelsleden, dus met toegang tot de back office; layer 3, dit is een zwaar beveiligd systeem toegankelijk voor de informatici die instaan voor de back up en de apparatuur. Het verbod in 8.b. slaat enkel op de layers 2 en 3.

[4] Spamming

11. systeeminformatie, systeemconfiguratie, toepassingsprogramma's of bestanden wijzigen, verwijderen of doorgeven aan derden, tenzij men daarvoor bevoegd is;
12. intern ontwikkelde programmatuur, die deel uitmaakt van het patrimonium van de hogeschool en die binnen het kader van de beroeps-of opleidingsactiviteit werd ontwikkeld, commercialiseren voor persoonlijke doeleinden of handelingen stellen die het verder gebruik of de exploitatie van de software kunnen hinderen tenzij het programmatuur betreft die specifiek ontwikkeld werd om onbeperkt verspreid te worden zoals bijvoorbeeld programmatuur met een open broncode licentie.[5]

Als één of meerdere vormen van gebruik, die hierboven als ongeoorloofd gebruik worden betiteld, onderwerp uitmaken van wetenschappelijk onderzoek en daarom een afwijking van deze richtlijnen gewenst wordt, moet een aanvraag bij de commissie worden ingediend via het e-mailadres: ICTdeontologie@hubkaho.be.

Elke gebruiker dient er zich bewust van te zijn dat de hogeschool in het kader van een gerechtelijk onderzoek verplicht is om met de gerechtelijke autoriteiten mee te werken.

7. Vertrouwelijkheidsverklaring

- Minstens de volgende gebruikers dienen een vertrouwelijkheidsverklaring te ondertekenen: gebruikers die inzage hebben in gegevens van de boekhouding, het personeel, kandidaat-werknemers of de studenten van de hogeschool
- gebruikers die inzage kunnen hebben in de elektronische online communicatiegegevens van de andere gebruikers zoals de lokale systeem-en netwerkbeheerders
- gebruikers die door hun onderzoeksactiviteit kennis krijgen van persoonsgegevens.

Zij ondertekenen deze verklaring bij de inwerkingtreding van deze richtlijnen, of vanaf het ogenblik dat zij de inzage/kennis kunnen hebben.

8. Toegangsrechten voor externen

Externen die toegangsrechten tot ICT-middelen, IT-infrastructuur of elektronische communicatiemiddelen van de hogeschool nodig hebben voor het uitvoeren van hun opdracht aan de hogeschool (vb. gastsprekers) verkrijgen deze slechts na het ondertekenen en dateren van een verklaring dat ze de richtlijnen voor het gebruik van ICT aan de hogeschool hebben ontvangen en zullen naleven. Op de verklaring vermelden zij hun volledige naam, adres en telefoonnummer. [6]

De toegangsrechten worden zuiver ten persoonlijke titel toegekend en gelden slechts voor de periode noodzakelijk voor de uitvoering van de opdracht.

[5] Met externe medewerkers die in het kader van hun werkzaamheden binnen de hogeschool programmatuur ontwikkelen, worden contractuele afspraken gemaakt.
[6] Treedt in werking vanaf het academiejaar 2014-2015.

9. Uitdiensttreding van een gebruiker (enkel voor personeelsleden)

Het personeelslid dat uit dienst treedt, leeft de voorschriften na van het document "ICT-gebruik bij en na uitdiensttreding". Dit document kan worden geraadpleegd op het intranet of kan worden opgevraagd bij de personeelsdienst.

10. Toezicht op het gebruik van de ICT-middelen

De controle wordt uitgevoerd door personen die in het kader van hun functie belast zijn met het beheer van systemen, netwerken of onderdelen daarvan, met name de systeem-en netwerkbeheerders. De controle gebeurt op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt. Individuele controle kan gebeuren naar aanleiding van incidenten of een vraag om medewerking van de gerechtelijke autoriteiten.

Ten aanzien van gebruikers-personeelsleden
Voor de personeelsleden met een arbeiders-of bediendestatuut geldt CAO nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens (hierna genoemd de CAO).[7] Ook voor de andere personeelsleden wordt deze CAO gevolgd.

De CAO bepaalt dat controle door de werkgever op het gebruik van de online communicatiemiddelen door de werknemers toegestaan is. De controle moet wel gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt.

Over het invoeren van de mogelijkheid van algemene controle worden de personeelsleden collectief (via het HOC) en individueel (via het intranet) geïnformeerd. Individuele controle kan gebeuren naar aanleiding van incidenten of een vraag om medewerking van de gerechtelijke autoriteiten.

De uitoefening van het toezicht gebeurt i.f.v. alle doelstellingen van de CAO, conform de geldende arbeidsreglementen:
1. het voorkomen van ongeoorloofde feiten
2. de bescherming van de (vertrouwelijke) belangen van de onderneming
3. de veiligheid en de goede technische werking van de IT-netwerksystemen
4. het te goeder trouw naleven van de richtlijnen voor ICT-gebruik aan de hogeschool.

Indien het enkel gaat over niet-naleving van doelstelling 4, kan individuele controle slechts gebeuren nadat de richtlijnen opnieuw in herinnering zijn gebracht.

[7] De CAO is van toepassing op de controle op elektronische online communicatiegegevens in de ruime zin. Hierbij is het niet belangrijk of het interne online communicatie betreft, dan wel of deze extern gaat. Ook het e-mailverkeer van werknemers onderling tijdens de arbeidsuren valt dus onder de toepassing van deze CAO. De CAO nr. 81 stelt uitdrukkelijk dat zij een aantal elementen niet wenst te regelen met name de regels voor de toegang tot en/of het gebruik van de elektronische online communicatiemiddelen van de onderneming: dit blijft het prerogatief van de werkgever

Een incident wordt onderzocht:

- na vaststelling door ICT van een technisch incident
- na interne melding van een incident, dit is door een andere gebruiker
- na externe melding van een incident door contractuele partners van de hogeschool (vb. stageplaats)
- na officiële vraag om medewerking van de gerechtelijke autoriteiten.

Indien het onderzoek uitwijst dat één van de doelstellingen overtreden is, wordt de personeelsdirecteur op de hoogte gebracht van het resultaat van het onderzoek. De personeelsdirecteur voert een gesprek met het personeelslid. Dit gesprek heeft plaats voor iedere beslissing die het personeelslid kan raken. Het personeelslid krijgt de kans zijn/haar bezwaren met betrekking tot de voorgenomen beslissing uiteen te zetten.

Het personeelslid kan zich desgewenst door zijn/haar vakbondsafgevaardigde laten bijstaan. Er kan een ordemaatregel worden genomen (vb. tijdelijk verbod van persoonlijk gebruik) en/of een sanctie of tuchtmaatregel die is opgenomen in het arbeidsreglement. Strafrechtelijke feiten worden gemeld aan de bevoegde instanties.

Zo nodig kunnen bewarende maatregelen genomen worden om de veiligheid en integriteit van de ICT-systemen en de daarmee verwerkte informatie te waarborgen.

Ten aanzien van gebruikers-studenten

Een incident wordt onderzocht:

- na vaststelling door ICT van een technisch incident
- na interne melding van een incident, dit is door een andere gebruiker
- na externe melding van een incident door contractuele partners van de hogeschool (vb. stageplaats) na officiële vraag om medewerking van de gerechtelijke autoriteiten.

Indien het onderzoek uitwijst dat de ICT-gedragslijn of wetgeving overtreden is, wordt de studiegebieddirecteur op de hoogte gebracht van het resultaat van het onderzoek. De studiegebieddirecteur voert een gesprek met de student. Dit gesprek heeft plaats voor iedere beslissing die de student kan raken. De student krijgt de kans zijn/haar bezwaren met betrekking tot de voorgenomen beslissing uiteen te zetten. Er kan een tuchtprocedure gestart worden in overeenstemming met het onderwijs-en examenreglement. Strafrechtelijke feiten worden gemeld aan de bevoegde instanties.

Zo nodig kunnen bewarende maatregelen genomen worden om de veiligheid en integriteit van de ICT-systemen en de daarmee verwerkte informatie te waarborgen.

Ten aanzien van andere gebruikers (dan studenten en personeelsleden)

Een incident wordt onderzocht:

- na vaststelling door ICT van een technisch incident
- na interne melding van een incident, dit is door een andere gebruiker
- na externe melding van een incident door contractuele partners van de hogeschool (vb. stageplaats) na officiële vraag om medewerking van de gerechtelijke autoriteiten.

Indien het onderzoek uitwijst dat de ICT-gedragslijn of wetgeving overtreden is, wordt de algemeen beheerder op de hoogte gebracht van het resultaat van het onderzoek. De algemeen beheerder of een ander lid van het Directiecomité voert een gesprek met de gebruiker. Dit gesprek heeft plaats voor iedere beslissing die de gebruiker kan raken. De gebruiker krijgt de kans zijn/haar bezwaren met betrekking tot de voorgenomen beslissing uiteen te zetten. Strafrechtelijke feiten worden gemeld aan de bevoegde instanties.

Zo nodig kunnen bewarende maatregelen genomen worden om de veiligheid en integriteit van de ICT-systemen en de daarmee verwerkte informatie te waarborgen.