Universiteit Antwerpen

ICT-gedragscode voor studenten

Universiteit Antwerpen

Inhoudsopgave

1 Inleiding

Informatie- en communicatietechnologie (ICT) krijgt een alsmaar belangrijkere rol binnen de samenleving en dus ook binnen de Universiteit Antwerpen. De goede werking van de universiteit wordt daardoor ook steeds afhankelijker van de vlotte en doeltreffende werking van de ICT-infrastructuur.

Deze vlotte en doeltreffende werking van ICT kan echter niet worden bereikt door louter technische maatregelen te nemen. Ook de gebruikers van ICT-middelen moeten hier hun steentje toe bijdragen. Deze standaard biedt een algemeen kader met waarden en principes die de studenten van de Universiteit Antwerpen moeten eerbiedigen wanneer zij gebruik maken van ICT-middelen, die gerelateerd zijn aan de Universiteit Antwerpen.

De intentie van deze standaard is niet om in te gaan tegen de cultuur van openheid, vertrouwen en integriteit van de Universiteit Antwerpen of tegen het principe van de academische vrijheid, maar om de studenten, werknemers, partners en de universiteit te beschermen tegen illegale of schadeberokkenende acties van individuen of groepen, bekend of onbekend.

De universiteit moedigt alle leden van de universitaire gemeenschap aan om de elektronische hulpmiddelen op een respectvolle manier te gebruiken. Iedere gebruiker heeft dan ook een aantal verantwoordelijkheden die samengaan met het gebruik van ICT-middelen aan de Universiteit Antwerpen.

2 Definities

ICT-middelen bestaan enerzijds uit ICT-systemen (i.e. hardware en software) en anderzijds uit de data die op ICT-systemen zijn opgeslagen. Voorbeelden hiervan zijn: e-mail faciliteiten, accounts, internet, computers, laptops, tablets, printers, USB-sticks, telefoons, gsm's, smartphones, opslagmedia (servers e.a.), routers, switches, etc. Het begrip **data** (informatie) omvat alle betekenisvolle gegevens.

Bedrijfsdata zijn alle betekenisvolle gegevens die eigendom zijn van de Universiteit Antwerpen. Het gaat bijvoorbeeld over data waar intellectuele eigendomsrechten op rusten, data die nodig zijn voor de uitvoering van bedrijfsprocessen, persoonsgegevens van personeelsleden en studenten, etc.

Een **verwerking** is een bewerking of een geheel van bewerkingen met betrekking tot data, al dan niet uitgevoerd via een geautomatiseerd proces, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, wissen of vernietigen van data.

Studenten zijn alle natuurlijke personen die zijn ingeschreven in de studentendatabank.

3 Doel en toepassingsgebied

De doelstelling van deze standaard is:

- De veiligheid en betrouwbaarheid te waarborgen van ICT-middelen die zijn gerelateerd aan de Universiteit Antwerpen en relevante derden;
- Een stabiele ICT-dienstverlening te garanderen;
- De persoonlijke levenssfeer en veiligheid van individuele gebruikers te beschermen en;
- De goede naam van de Universiteit Antwerpen als verantwoord internetgebruiker te waarborgen.

Deze standaard is van toepassing op iedere student bij het gebruik van ICT-middelen, die zijn gerelateerd aan de Universiteit Antwerpen (o.m. telefoon, GSM, fax, pc, e-mail, netwerkprogrammatuur, interne en externe netwerken, Internet, toets- en leerplatformen, administratieve systemen, informatiesystemen, bedrijfsdata op de ICT-systemen, etc.).

Deze standaard geldt dus evenzeer voor ICT-middelen, al dan niet eigendom van de Universiteit Antwerpen, die men in relatie met de Universiteit Antwerpen gebruikt (bijvoorbeeld e-mailadres Universiteit Antwerpen) of in combinatie met de ICT-middelen van de Universiteit Antwerpen (bijvoorbeeld toegang tot Blackboard).

Alle studenten worden verondersteld deze regels te kennen en hun gedrag hier overeenkomstig op af te stemmen.

4 Algemene principes

4.1 Geoorloofd gebruik

Iedere student wordt geacht zich te gedragen als een goede huisvader wanneer hij/zij omgaat met ICT-middelen die zijn gerelateerd aan de Universiteit Antwerpen. Dit principe houdt concreet in dat iedere student zich moet gedragen als een normaal, vooruitziend en zorgvuldig persoon:

- **Vooruitziend** betekent dat men de nadelige gevolgen van zijn handelen redelijk probeert in te schatten en dat men er met andere woorden op probeert te anticiperen;
- **Zorgvuldig** houdt in dat men die nadelige gevolgen probeert te voorkomen door gepaste voorzorgsmaatregelen te nemen.

4.2 Ongeoorloofd gebruik

Het ongeoorloofd gebruik van ICT-middelen die in relatie staan tot de Universiteit Antwerpen, is verboden. Hieronder wordt een niet-limitatieve lijst met ongeoorloofde handelingen weergegeven:

- ICT-middelen aanwenden die gerelateerd zijn aan de Universiteit Antwerpen om handelingen te stellen of data te verwerken (opslaan, verspreiden, bewerken, etc.) die:
    - Beledigend, lasterlijk, aanstootgevend, bedreigend, discriminerend zijn of een schending van vertrouwen uitmaken;
    - Schade kunnen toebrengen aan derden;
    - In strijd zijn met de openbare orde en goede zeden;
    - Het imago, de morele of economische belangen van de Universiteit Antwerpen kunnen schaden;
    - In strijd zijn met wet- en regelgeving over de informatica misdrijven, de bescherming van de persoonlijke levenssfeer, het intellectuele eigendomsrecht, de bescherming van handelsnamen, etc. en/of;
    - In strijd zijn met de beleidsvisie en/of de interne regelgeving van de Universiteit Antwerpen.

4.3 Persoonlijk gebruik

De Universiteit Antwerpen laat binnen redelijke perken het persoonlijke gebruik van haar ICT-middelen toe. Hieronder wordt verstaan dat :

- Anderen door dit gebruik niet mogen gestoord worden bij de uitoefening van hun (beroeps- of studie)activiteiten;
- Er behoudens andere afspraken geen kosten aan verbonden zijn voor de Universiteit Antwerpen en;
- Er op ieder moment voorrang verleend wordt aan studiedoeleinden in het gebruik van gemeenschappelijke ter beschikking gestelde ICT-middelen.

Gebruikers die persoonlijke data op ICT-middelen van de Universiteit Antwerpen verwerken, moeten er zich bewust van zijn dat de Universiteit Antwerpen in uitzonderlijke gevallen kennis kan nemen van de informatie die verwerkt wordt op de ICT-middelen van de Universiteit Antwerpen. In elk geval wordt zoveel mogelijk de persoonlijke levenssfeer van de betrokkene beschermd.

De Universiteit Antwerpen is in geen geval aansprakelijk voor het eventueel verlies van private data, die op de ICT-middelen van de Universiteit Antwerpen worden bewaard.

5 Informatiebeheer en -beveiliging

5.1 Beveiliging

Alle (vertrouwelijke) informatie moet steeds met passende technische en organisatorische beveiligingsmaatregelen worden beschermd. Studenten moeten er dan ook op toezien dat vertrouwelijke informatie steeds op systemen wordt bewaard, waar passende beveiligingsmaatregelen voor werden getroffen (zoals antivirussoftware, een actieve firewall, etc.).

Daarnaast moeten studenten ook zelf steeds voldoende beveiligingsmaatregelen nemen die de mogelijkheid tot het inbreken op de systemen van de Universiteit Antwerpen en de diefstal en het verlies van ICT-middelen zo klein mogelijk maakt (gebruik maken van sterke wachtwoorden, niet onbeheerd achterlaten van laptops, geen wachtwoorden opslaan op computers (tenzij deze in een wachtwoordmanager zijn opgeslagen en de database zich niet op een gedeelde computer bevindt), etc.).

Studenten dienen erop toe te zien dat vertrouwelijke bedrijfsdata (zoals bijvoorbeeld persoonsgegevens die worden verwerkt in het kader van een thesis) die worden opgeslagen op draagbare media (harde schijven van laptops, USB-sticks, etc.) worden geëncrypteerd. Meer concrete afspraken omtrent de encryptie van ICT-middelen worden gepubliceerd op Blackboard.

5.2 Opslaan, delen of kopiëren van bedrijfsdata

Bij voorkeur worden de bedrijfsdata (zoals onderzoekdata) opgeslagen op systemen die worden beheerd door het departement ICT. Het opslaan van data op lokale media (zoals externe harde schijven, de harde schijf van een laptop, etc.) moet zoveel mogelijk vermeden worden.

Wanneer dit niet mogelijk is dan dienen de betrokken studenten erop toe te zien dat er een voldoende hoog beschermingsniveau wordt gewaarborgd voor de alternatieve ICT-systemen. Deze beschermingsmaatregelen hebben o.a. betrekking op het regelmatig nemen van back-ups, gebruik maken van beveiligingssoftware en voldoende sterke authenticatie methoden (zoals een complex wachtwoord), encrypteren van draagbare media, etc.

Het is niet toegestaan om bedrijfsdata (zoals cursusmateriaal, maar ook onderzoeksdata) te verspreiden naar of te delen met personen die niet gerechtigd zijn om deze data te verwerken (ontvangen, raadplegen, verspreiden, publiceren, etc.).

5.3 Persoonsgegevens

Persoonsgegevens mogen worden verwerkt op de ICT-systemen van de Universiteit Antwerpen in de mate dat dit in overeenstemming is met de vigerende privacywetgeving en het privacyreglement van de Universiteit Antwerpen.

Voor meer informatie over de verwerking van persoonsgegevens wordt verwezen naar de daarvoor bestemde communicatiekanalen van de Dienst Gegevensbescherming (bijv. de helpdesk privacy).

5.4 Cloud

Alleen de cloudtoepassingen die door het Departement ICT van de Universiteit Antwerpen werden weerhouden mogen worden gebruikt voor de opslag van bedrijfsdata (zoals cursusmateriaal en onderzoeksdata).

Voor de opslag van persoonsgegevens in cloudtoepassingen moeten steeds de richtlijnen van de Dienst Privacy worden gevolgd. Voor meer informatie over de verwerking van persoonsgegevens in cloudtoepassingen wordt

verwezen naar de daarvoor bestemde communicatiekanalen van de Dienst Gegevensbescherming (bijv. de helpdesk privacy).

5.5 Toegangsrechten

Het verlenen van toegangsrechten gebeurt uitsluitend op basis van de *need-to-have* en *need-to-know* principes. Concreet betekent dit dat studenten alleen die toegangsrechten mogen krijgen die noodzakelijk zijn in het kader van hun studieactiviteiten binnen de Universiteit Antwerpen. Het is de verantwoordelijkheid van de data-eigenaren om er op toe te zien dat de toegangsrechten correct zijn en beperkt zijn tot wat strikt noodzakelijk is.

Op regelmatige basis moet er een evaluatie worden uitgevoerd van de toegangsrechten door de data-eigenaren tot de informatie waarvoor zij verantwoordelijk zijn.

Wanneer een student merkt dat hij of zij toegang heeft tot informatie waarvoor men niet gemachtigd is, moet de student dit onmiddellijk melden bij de data-eigenaar en/of de ICT-verantwoordelijke, zodat de toegangen beperkt kunnen worden.

De aanvraag voor het verkrijgen van toegangsrechten wordt steeds ingediend of ingesteld door de data-eigenaar van de betreffende informatie.

6 ICT-systemen

6.1 Algemeen

Het is verboden om te trachten de beveiliging van een host, netwerk of account te omzeilen. Dit houdt in, maar is niet beperkt tot: het opvragen van gegevens die niet bestemd zijn voor de gebruiker, gebruik van een dienst of account waarvoor de gebruiker geen toestemming heeft, gebruik van sniffing en scanning tools, etc.

Evenzeer is het verboden om te trachten eender welke dienst, host of netwerk te verstoren (denial of service). Dit houdt in, maar is niet beperkt tot, uitdrukkelijke pogingen om een netwerk of host te overbelasten (flooding), en pogingen om een systeem te doen crashen.

Het is niet toegestaan om eigen netwerkapparatuur (switches, routers, firewalls, vpn-servers, dialin-servers, wireless access points, ...) te installeren zonder overleg en expliciete toestemming van de Netwerkdienst van het Departement ICT.

Studenten dienen er steeds op toe te zien dat hun activiteiten op het netwerk of de systemen van de Universiteit Antwerpen in geen geval schade of ongemak (van welke aard ook) veroorzaken aan andere gebruikers of derden.

Studenten dienen ten allen tijde voorzichtig om te gaan met het inloggen op het Universiteit Antwerpen netwerk van op andere, externe (publieke) locaties (bijvoorbeeld inloggen via cybercafés, open/publieke draadloze netwerken, etc.).

Studenten moeten er mee op toezien dat alle programmatuur en gegevens die zijn verkregen via een extern netwerk, via webtoepassingen (zoals webmail, webhosting, etc.) of via draagbare media (zoals CD-ROM's, DVD's, USB-sticks, etc.) gecontroleerd worden op virussen en andere kwaadaardige programmatuur.
Het is niet toegestaan om niet-professionele data op te slaan op centrale ICT-systemen (zoals servers en de centrale storage) van de Universiteit Antwerpen.

Het is verboden om het netwerk van de Universiteit Antwerpen te gebruiken voor winstgevende of handelsdoeleinden, of voor activiteiten die niet kaderen in de opdracht van de universiteit, of voor andere activiteiten die in strijd zijn met de AUP van Belnet.

Het is expliciet verboden voor studenten om illegale downloads (zoals o.a. programmatuur, bestanden, muziekbestanden, filmbestanden, etc.) uit te voeren via of te installeren op ICT-middelen, die zijn gerelateerd aan de Universiteit Antwerpen. Indien een student deze bepaling niet eerbiedigt dan is dit de volledige verantwoordelijkheid van het student zelf. Eventuele gerechtelijke onderzoeken en de bijhorende financiële gevolgen zullen steeds worden doorgestuurd naar de betrokken student.

De Universiteit Antwerpen behoudt ten allen tijde het recht om wanneer dit noodzakelijk blijkt (bv. bij diefstal, verlies, etc.) alle of gedeeltelijke toegangen tot netwerk door bepaalde ICT-middelen (zoals bv. smartphones, tablets, laptops…) te blokkeren.

6.2 ICT-systemen van de Universiteit Antwerpen

Studenten hebben de verantwoordelijkheid om veilig om te gaan met ICT-middelen, die ter beschikking worden gesteld.

Om diefstal en verlies te voorkomen dienen studenten steeds voldoende beveiligingsmaatregelen te nemen. Zo dient de schermbeveiliging van de ICT-systemen steeds te worden geactiveerd wanneer de ICT-systemen onbeheerd worden achtergelaten.

Studenten mogen op ICT-middelen van de UAntwerpen uitsluitend programmatuur installeren en gebruiken, waarvoor de nodige licenties of gebruiksafspraken aanwezig zijn. Het is verboden om persoonlijk verkregen gebruikersrechten en licenties van de Universiteit Antwerpen door te geven aan derden.

De ICT-systemen van de Universiteit Antwerpen moeten voorzien zijn van actieve beveiligingssoftware. Het is verboden om de door het departement ICT geïnstalleerde beveiligings- en beheersoftware (bijvoorbeeld antivirussoftware) uit te schakelen.

Indien de student, ondanks verschillende beveiligingsmaatregelen, wordt geconfronteerd met een virus, verdachte e-mail of een verdacht bestand moet er onmiddellijk worden gestopt met werken op het ICT-systeem en moeten deze eerst worden verwijderd. In bovenstaande gevallen moet steeds contact worden opgenomen met het Departement ICT.

6.3 Externe ICT-systemen

Het is verboden om ICT-systemen die geen eigendom zijn van de Universiteit Antwerpen en die niet voldoen aan de beveiligingsregels die worden opgelegd door de interne reglementering van de Universiteit Antwerpen, te koppelen aan het fysieke campusnetwerk. Zo dienen externe ICT-systemen (zoals laptops, tablets, smartphones, etc.) steeds te beschikken over een actieve firewall en antivirussoftware.

Het gebruik van eigen ICT-systemen gebeurt op eigen risico. Hierdoor is en blijft de student die een eigen extern ICT-systeem meeneemt naar de Universiteit Antwerpen zelf verantwoordelijk voor: de back-up en restore bij verlies of diefstal, het onderhoud en het beheer van het ICT-systeem en de data die zich op het systeem bevinden.

6.4 Accounts en wachtwoorden

Voor iedere student wordt er bij de inschrijving aan de Universiteit Antwerpen een account aangemaakt. Via deze account wordt er aan studenten toegang verleend tot verschillende ICT-diensten van de Universiteit Antwerpen zoals e-mail, internet, VPN, centrale netwerkschijven voor documentopslag, etc.

Gezien deze uitgebreide toegangsrechten tot ICT-faciliteiten van de Universiteit Antwerpen heeft ieder student de verantwoordelijkheid om zijn of haar account te beschermen met een veilig wachtwoord. De principes waar wachtwoorden aan moeten voldoen, worden gepubliceerd via Blackboard. Daarnaast moeten wachtwoorden iedere zes maanden worden gewijzigd.

Wachtwoorden vormen de unieke toegangscode tot de UAntwerpen accounts en bijgevolg ook tot de virtuele identiteit van studenten. Het is daarom verboden om wachtwoorden bewust of onbewust door te geven aan ouders, familieleden, medestudenten of andere personen of om te trachten het wachtwoord van iemand anders te weten te komen. Evenzeer is het verboden om met het account van iemand anders in te loggen.

Studenten dienen hun wachtwoord onverwijld te wijzigen wanneer iemand anders het wachtwoord kent of het vermoeden bestaat dat iemand anders het te weten is gekomen.

UAntwerpen accounts mogen uitsluitend worden gebruikt om zich te registreren voor activiteiten die kaderen binnen de werking van de Universiteit Antwerpen. Een student mag nooit het wachtwoord van zijn of haar UAntwerpen account gebruiken voor andere persoonlijke of professionele ICT-systemen. Voorbeelden van andere persoonlijke of professionele ICT-systemen zijn: Facebook, LinkedIn, persoonlijk e-mailaccount, Dropbox, etc.

Bovenstaande principes zijn naar analogie van toepassing op andere accounts, die toegang verlenen tot bedrijfsdata of andere vertrouwelijke informatie of systemen, die zijn gerelateerd aan de Universiteit Antwerpen.

7 Communicatie

7.1 E-mail

Het is verboden om, buiten de gevallen van de normale bedrijfscommunicatie, massaal ongevraagde en ongewenste elektronische post (ook gekend als SPAM), virussen, kettingbrieven of hoaxen te versturen via of aan ICT-middelen van de Universiteit Antwerpen.

Indien een student alle studenten van de universiteit wil bereiken, dient hij een aanvraag te doen via het formulier op Blackboard. Het bericht van de student zal in eerste instantie op Blackboard worden gepubliceerd.

Een student hoort niet te mailen aan grote groepen studenten, tenzij het onderwerp onderwijs- of studiegerelateerd is in het kader van de opleiding. Voorbeelden van wat niet kan zijn mails over: de verkoop van tweedehands boeken, zoekertjes, examenwissels, kopen of verhuren van een kot, etc.

Studenten dienen hun mailbox regelmatig te raadplegen en op te ruimen of archiveren. De Universiteit Antwerpen behoudt zich het recht voor om in te grijpen op de beschikbare individuele capaciteit van de mailboxen.

Het verzenden van persoonlijke e-mails is slechts toegestaan voor zo ver dit in overeenstemming is met de bepaling omtrent het persoonlijk gebruik van ICT-middelen.

7.2 Internet

Voor meer informatie over het gebruik van internet wordt verwezen naar de secties van deze standaard die gaan over het persoonlijk gebruik en de ICT-systemen.

Wat betreft het toezicht op het internetgebruik van studenten wordt verwezen naar de sectie toezicht en controle.

7.3 Telefonie

Voor meer informatie over het gebruik van telefonie van de Universiteit Antwerpen wordt verwezen naar de secties van deze standaard die gaan over het persoonlijk gebruik en de ICT-systemen.

8 Meldplicht

8.1 Incidenten

Inbreuken op de ICT-gedragscode, incidenten en bijna incidenten die betrekking hebben op de ICT-middelen moeten steeds worden gemeld aan de helpdesk van het departement ICT.

Een incident kan de fysieke diefstal van een ICT-middel uitmaken, maar ook het inbreken op systemen en diefstal van informatie vormen incidenten, die moeten worden gemeld aan de helpdesk van het departement ICT.

De helpdesk ICT kan worden gecontacteerd via het e-mailadres helpdesk@uantwerpen.be of via het telefoonnummer 03 265 48 08.

8.2 Incidenten met persoonsgegevens

Alle incidenten met ICT-middelen, waarbij persoonsgegevens zijn betrokken moeten onverwijld worden gemeld aan de dienst Gegevensbescherming via het meldingsformulier voor datalekken.

9 Toezicht en controle

Binnen de wettelijke grenzen kan de Universiteit Antwerpen controle uitoefenen op gegevens die een student opslaat, verstuurt of ontvangt binnen het toepassingsgebied van deze standaard. De controle zal gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt.

Behoudens in het geval van incidenten mogen ICT-medewerkers het gebruik van de elektronische communicatiemiddelen slechts op een globale wijze controleren. Zo mag een globaal overzicht gemaakt worden, eventueel per organisatorische entiteit, van de gedurende een bepaalde periode bezochte websites met de frequentie en het volume van de doorgezonden informatie, doch zonder daarin op enige wijze gegevens over het individueel gebruik op te nemen.

Wanneer er echter een vermoeden bestaat dat een student illegale activiteiten uitoefent op het netwerk van de Universiteit Antwerpen of een inbreuk pleegt op deze standaard, behoudt de Universiteit Antwerpen het recht om de individuele activiteiten te controleren.

10 Maatregelen bij inbreuk

De Universiteit Antwerpen heeft het recht om, wanneer dit om bedrijfsredenen vereist of wettelijk bepaald is, de voorwaarden voor het ter beschikking stellen van ICT-middelen te herzien en eventueel te beperken. Zo behoudt de Universiteit Antwerpen zich het recht voor om studenten die met opzet deze standaard overtreden de toegang tot het netwerk te ontzeggen.

De Universiteit Antwerpen heeft tevens het recht om de gemaakte kosten en/of veroorzaakte schade te verhalen op de student.

De Universiteit Antwerpen kan steeds optreden tegen inbreuken op deze standaard met alle gepaste middelen overeenkomstig de tuchtmaatregelen die zijn voorzien in het Statuut van de UAntwerpen Student.

Als er bij controles illegale activiteiten of informatie worden ontdekt dan kan de Universiteit Antwerpen hiervan aangifte doen bij de gerechtelijke autoriteiten. Bij twijfel zal er in eerste instantie verder onderzoek worden gevoerd, waarbij de individuele activiteiten en informatie kan worden gecontroleerd. De Universiteit Antwerpen zal steeds haar medewerking verlenen bij het opsporen van misdrijven, en zal eventuele gebruikersgegevens en logfiles overmaken aan de gerechtelijke autoriteiten wanneer zij hierom verzoeken. Wanneer komt vast te staan dat een gebruiker illegale handelingen heeft uitgevoerd in relatie tot ICT-middelen dan wordt de betrokkene daar persoonlijk voor verantwoordelijk gesteld.

11 Uitzonderingsregeling

Uitzonderingsregelingen op deze standaard kunnen uitsluitend worden toegestaan, indien er gegronde redenen bestaan om een tijdelijk uitzondering te verlenen.

Uitzonderingsregelingen kunnen slechts voor een bepaalde duur worden toegestaan.

Om een uitzonderingsregeling aan te vragen moet de student een gemotiveerd schriftelijk verzoek richten aan de departementsverantwoordelijken ICT, Paul Fremau en Geert Vera. Wanneer er wordt besloten om over te gaan tot het verlenen van een uitzonderingsregeling, wordt dit schriftelijk meegedeeld aan het betreffende student.