



Reglement inzake aanvaardbaar gebruik van de ICT-infrastructuur aan de Associatie Universiteit Gent & partnerinstellingen

Algemeen

De computernetwerken van de partnerinstellingen van de Associatie Universiteit Gent (AUGent) zijn bestemd voor onderwijs en onderzoek en voor activiteiten ter ondersteuning daarvan.

Het netwerk van de AUGent & partnerinstellingen is aangesloten op BELNET, het Belgische onderzoeksnetwerk. Er is een Acceptable Use Policy (AUP) die bepaalt wat wel en niet toegelaten is op BELNET. Deze AUP is beschreven in het document AUP Belnet (Aanvaardbaar gebruik van de BELNET toegang, zie bijlage). Wanneer men het netwerk gebruikt, dient men dus niet alleen rekening te houden met de regels voor goed gebruik van het netwerk van de AUGent & partnerinstellingen, maar ook met de AUP van BELNET.

1. Definities

De AUGent & partnerinstellingen:

De vzw. AUGent en de partnerinstellingen Universiteit Gent, Hogeschool Gent, Arteveldehogeschool en Hogeschool West-Vlaanderen.

Student: Elke student die ingeschreven is aan de partnerinstellingen van de AUGent.

Personeelslid: Iedereen die in statutair of contractueel verband werkt voor de AUGent & partnerinstellingen.

Gebruiker: Elke persoon en organisatie die op een of andere manier gebruik maakt van de ICT-infrastructuur van de AUGent & partnerinstellingen, in het bijzonder studenten en personeelsleden.

ICT-infrastructuur: hiermee wordt zowel de fysieke apparatuur als de ICT-diensten (inclusief thuisgebruik via VPN) bedoeld.

ICT-beheerder(s): verantwoordelijken voor het onderhoud en het goed functioneren van de ICT-infrastructuur.

2. Ongeoorloofd gebruik

2.1 De ICT-infrastructuur mag niet gebruikt worden om ongeoorloofde informatie te verwerven, te verwerken, te verspreiden of op te slaan. Hieronder wordt onder meer verstaan:

2.1.1 Informatie die in strijd is met de wet, in het bijzonder (doch niet beperkt tot):

- Informatie die in strijd is met de wetgeving op de bescherming van de persoonlijke levenssfeer;
- Informatie die in strijd is met de wetgeving over het auteursrecht en andere intellectuele rechten;
- Informatie die in strijd is met de wetgeving ter bestrijding van racisme of die beledigend of lasterlijk is voor anderen;
- Informatie die in strijd is met de wetgeving over de bescherming van de goede zeden.

2.1.2 Informatie die de AUGent & partnerinstellingen schaadt, in het bijzonder (doch niet beperkt tot):

- Informatie die het imago van de AUGent & partnerinstellingen schendt, of haar moreel of economisch kan schaden;
- Informatie die vertrouwelijk is of die wegens de aard ervan als vertrouwelijk moet beschouwd worden.

2.1.3 Informatie die hinderlijk is voor anderen, in het bijzonder (doch niet beperkt tot):

- Informatie die aanstootgevend is voor anderen omdat ze tegen de algemeen geldende fatsoenregels indruist;
- Aan grote groepen personen ongewenste elektronische post, berichten of kettingbrieven sturen.

2.2 Volgende handelingen zijn expliciet verboden:

2.2.1 Software installeren en/of te gebruiken waarvoor men geen licentie heeft of op een wijze die in strijd is met de licentievoorwaarden van die software. Dit is van toepassing op de apparatuur die deel uitmaakt van de ICT-infrastructuur van de AUGent & partnerinstellingen. Software die ter beschikking gesteld wordt door de AUGent & partnerinstellingen mag niet getransfereerd worden naar eigen apparatuur zonder expliciete toestemming van een ICT-beheerder. De partnerinstellingen van de AUGent kunnen autonoom optreden tegen gebruikers waarvan vermoed wordt dat zij illegale software gebruiken en/of verspreiden.

2.2.2 Het installeren van software op apparatuur die deel uitmaakt van de ICT-infrastructuur van de AUGent & partnerinstellingen, zonder voorafgaandelijke toestemming van de ICT-beheerder, verantwoordelijk voor het betreffende deel van de ICT-infrastructuur.

2.2.3 Wijzigen van de structuur of de configuratie van de ICT-infrastructuur zonder voorafgaandelijke toestemming van de ICT-beheerder, verantwoordelijk voor het betreffende deel van de ICT-infrastructuur.

2.2.4 Acties ondernemen die strafbaar zijn in het kader van de wet van 28 november 2000 inzake informaticacriminaliteit. Onder andere vallen hieronder:

- Het omzeilen van interne en externe systeem- en netwerkbeveiligingen;
- Het ontwerpen en/of het installeren van schadelijke software op apparatuur die deel uitmaakt van de ICT-infrastructuur van de AUGent & partnerinstellingen;
- Willens en wetens ongeëigende en ongeoorloofde toegang forceren tot systemen waartoe men niet geautoriseerd is;
- Informatie onderscheppen (of pogingen daartoe) die niet voor zichzelf bedoeld is;
- Een valse identiteit aannemen op het netwerk.

2.2.5 De ICT-infrastructuur van de AUGent & partnerinstellingen gebruiken voor commerciële of politieke activiteiten.

2.2.6 Het actief opsporen van zwakheden in de beveiliging of het testen van de maximum capaciteit van gelijk welk onderdeel van de ICT-infrastructuur van de AUGent & partnerinstellingen. In het algemeen, het opzettelijk genereren van extreme belastingen zonder functionele noodzaak.

2.2.7 Systeeminformatie, systeemconfiguratie, toepassingsprogramma's of bestanden wijzigen of doorgeven aan derden indien men daarvoor vanwege de aard van zijn functie niet is gerechtigd.

3. Verantwoordelijkheden van de gebruiker

3.1 Het in goede toestand bewaren van de ICT-infrastructuur die ter beschikking wordt gesteld, inclusief een actieve deelname aan de beveiliging van deze ICT-infrastructuur.

3.1.1 Wanneer een gebruiker meent een defect of slecht functionerend onderdeel van de ICT-infrastructuur van de AUGent & partnerinstellingen te kennen, moet hij dit zo snel mogelijk melden aan de ICT-beheerder verantwoordelijk voor het betreffende deel van de ICT-infrastructuur. Hetzelfde geldt als een gebruiker een tekortkoming in de beveiliging van de ICT-infrastructuur van de AUGent & partnerinstellingen ontdekt. Anderen mogen hiervan niet op de hoogte gebracht worden. Het uitbuiten van deze zwakheden wordt beschouwd als ongeoorloofd gebruik.

3.1.2 Het niet onbeheerd achterlaten van de ter beschikking gestelde ICT middelen en het nemen van voldoende veiligheidsmaatregelen om diefstal ervan maximaal te verhinderen. Bij het verlaten van apparatuur waarop men ingelogd is, moet de gebruiker uitloggen of de apparatuur op zodanige manier vergrendelen dat enkel de gebruiker zelf of een ICT-beheerder er terug kan op inloggen. Dit om te voorkomen dat anderen zijn/haar identiteit kunnen aannemen.

3.1.3 Het steeds werken met een operationele recente virusscanner.

3.1.4 Het respecteren van de limieten vastgelegd op mailbox of file-server waarbij er, op regelmatig basis door de gebruiker, overbodige mails/files opgeruimd of gearchiveerd worden.

3.2 Bij communicatie zal de gebruiker altijd duidelijk zijn naam vermelden. Tevens moet de gebruiker, die beschikt over een e-mail adres van de AUGent & partnerinstellingen, dit adres gebruiken bij communicatie en de corresponderende postbus op een regelmatige basis controleren.

3.3 Indien gegevens op lokale harde schijven geplaatst worden, moet zelf gezorgd worden voor de noodzakelijke reservekopie (backup) en beveiliging.

4. Gebruikersnamen en wachtwoorden

Toegang tot de ICT-infrastructuur wordt verleend op basis van een gebruikersnaam en een wachtwoord. Hierbij moeten volgende regels in acht genomen worden:

4.1 Het wachtwoord mag niet eenvoudig te achterhalen zijn en moet regelmatig veranderd worden.

4.2 Verspreiding van het wachtwoord is verboden. Wie onvoorzichtig omspringt met zijn paswoord, kan voor de misbruiken verantwoordelijk gesteld worden.

4.3 Niemand mag zijn wachtwoord aan derden doorgeven en/of door derden laten gebruiken. Het is verboden wachtwoorden van anderen te proberen achterhalen.

5. Toezicht, controle en sancties

De ICT-infrastructuur van de AUGent & partnerinstellingen wordt gecontroleerd om de goede werking ervan te kunnen verzekeren en om misbruik op te sporen en te voorkomen. Elke partnerinstelling kan autonoom controle uitoefenen en mogelijke sancties bepalen. Het toezicht en controles gebeuren conform CAO81.

Mogelijke sancties bij vaststelling van een inbreuk op dit reglement zijn:

- Al dan niet tijdelijke beperking van de toegang tot bepaalde delen van de ICT-infrastructuur;

- Tijdelijk of definitief verbod tot het gebruik van de ICT-infrastructuur;
- Betaling van de kosten voortvloeiend uit het misbruik.;
- Indien het misbruik een strafrechtelijk feit betreft, kunnen de betrokkenen voor die feiten tevens gerechtelijk worden vervolgd, ongeacht eventuele schadevorderingen;
- Gegevens, onder gelijk welke vorm (bestanden, e-mails, gegevensdragers, databases,...) die toehoren aan de betreffende gebruiker kunnen worden geïnspecteerd en in beslag genomen;
- Alle andere sancties zoals vermeld in reglementeringen van de AUGent & partnerinstellingen.

AANVAARDBAAR GEBRUIK VAN DE BELNET-TOEGANG

a) De KLANT verbindt er zich toe conform de normen en protocols van Internet te handelen.

b) De KLANT mag het BELNET-netwerk uitsluitend met strikt wettelijke bedoelingen gebruiken. Ieder gebruik dat de Belgische of internationale wetgeving schendt, is verboden.

Als lid van de categorie A van ISPA België (Vereniging van de Internet Service Providers), onderschrijft BELNET het «Samenwerkingsprotocol ter bestrijding van ongeoorloofde handelingen op Internet» volledig. Indien er vermoedens bestaan van een onwettelijke actie door de KLANT, zal BELNET binnen het strikte kader dat door de wet wordt voorgeschreven, met de gerechtelijke macht samenwerken om haar onderzoeksplicht te vergemakkelijken.

c) Het is verboden om van de diensten van BELNET gebruik te maken voor iedere activiteit die :

- niet-geoorloofde toegang tot de gegevens van een derde mogelijk maakt;
- schade toebrengt aan de activiteit van BELNET of het Internet in het algemeen,
- het gebruik of de performantie van de internetdienst voor andere gebruikers in gevaar brengt;
- kan leiden tot de verspilling van middelen (personeel, netwerken, informatica);
- kan leiden tot de gedeeltelijke of complete vernietiging van de integriteit van de informaticagegevens;
- die de privacy van de gebruikers kan aantasten;
- die tot doel heeft om berichten over het netwerk te versturen die onder de categorie "lastigvallen" of "ongewenste post" vallen.

d) Het gebruik van BELNET is voorbehouden voor de openbare diensten, voor het onderwijs en voor onderzoeksdoeleinden. Het gebruik met commerciële bedoelingen en het intensieve gebruik voor persoonlijke doeleinden zijn verboden.

e) De KLANT is verantwoordelijk voor de levering van de Internet-dienst aan zijn eigen gebruikers, en dan meer bepaald voor de opstelling van interne toegangsprocedures tot BELNET via zijn lokaal netwerk.

Het beheer van dit lokaal netwerk valt eveneens onder de bevoegdheid van de KLANT. In dit kader moet de KLANT zichzelf beschermen tegen pogingen tot inbraak door een derde via BELNET.

f) De KLANT neemt de nodige maatregelen om ieder misbruik van BELNET door zijn eigen gebruikers tegen te gaan.

Hiertoe brengt hij hen op de hoogte van deze regels van aanvaardbaar gebruik.

Indien het BELNET-netwerk op een verkeerde manier wordt gebruikt, zal de KLANT op een actieve manier en zo snel mogelijk met BELNET samenwerken om de oorzaak van dit misbruik op te sporen en er een einde aan te stellen.

Indien het misbruik blijft voortduren, zullen er nadien acties worden ondernomen die kunnen leiden tot de schorsing van de dienstverlening aan de KLANT. De schorsing eindigt op het moment dat de voorgeschreven gebruikersregels terug worden gerespecteerd.