UNIVERSITEIT GENT

REGLEMENT VOOR CORRECT GEBRUIK VAN DE ICT-INFRASTRUCTUUR VAN DE UNIVERSITEIT GENT[1]

(goedgekeurd door het Bestuurscollege van 19 mei 2017)

(Voor definities en terminologie: zie onderaan punt 6)

1. GEOORLOOFD EN ONGEOORLOOFD GEBRUIK VAN DE ICT-INFRASTRUCTUUR VAN DE UGENT

1.1. De ICT-infrastructuur van de UGent mag gebruikt worden **voor rechtmatige activiteiten die kaderen binnen de normale werking van de UGent, in het bijzonder voor onderzoek, onderwijs en dienstverlening, en voor activiteiten ter ondersteuning daarvan**. Dit impliceert het volgende (niet-limitatieve opsomming):

- Extensief gebruik voor persoonlijke of recreatieve doeleinden is niet toegestaan;
- De ICT-infrastructuur mag niet gebruikt worden voor commerciële activiteiten, behoudens wanneer dit noodzakelijk is in het kader van de normale werking van de UGent;
- Ieder gebruik dat de toepasselijke wet- en regelgeving schendt, is verboden;
- De ICT-infrastructuur mag niet gebruikt worden om wetens en willens vertrouwelijke informatie[2] verder te verspreiden dan aan daartoe gerechtigde ontvangers (tenzij in gevallen waarin dat bij beslissing van het universiteitsbestuur wel is toegelaten, bv. in het kader van de klokkenluidersregeling);
- Het is enkel toegelaten toegang te verschaffen tot het UGentNet aan personen of systemen die daar overeenkomstig beslissingen van het universiteitsbestuur toe gerechtigd zijn;
- Inbreuken op (veiligheids)policies of gebruiksvoorwaarden van interne of externe informaticasystemen zijn verboden.

1.2. De ICT-infrastructuur mag niet gebruikt worden om **ongeoorloofde informatie** te verspreiden. Als ongeoorloofde informatie wordt beschouwd (niet-limitatieve opsomming):

[1] aka “Acceptable Use Policy”
aka “Regels voor het goed gebruik van het netwerk van de UGent en van de computers beheerd door DICT”

[2] Zoals gedefinieerd in het beleidsdocument “Richtlijn voor classificatie van informatie en data” (BC 10.7.2015), in afwachting van een breder debat over classificatie en vertrouwelijkheid van informatie. https://www.ugent.be/intranet/nl/op-het-werk/ict/informatieveiligheid/classificatie-data.pdf

- Informatie die oproept tot racisme, xenofobie, discriminatie,…;
- Informatie die in strijd is met de openbare orde of de goede zeden;
- Informatie die beledigend, lasterlijk of kwetsend is;
- Pesten, haatboodschappen of oproepen tot geweld;

1.3. Bij het gebruik van de ICT-infrastructuur van de UGent moet de Europese en Belgische **privacywetgeving** gerespecteerd worden. Dit houdt mede in dat de persoonlijke levenssfeer en de privacy van gebruikers, meer bepaald de vertrouwelijkheid en integriteit van hun privé-gegevens en de privacy van hun communicatie niet geschonden mag worden:
   - Het is niet toegestaan de elektronische post op de persoonlijke mailbox of de niet-gedeelde bestanden (in het bijzonder die op de persoonlijke schijfruimte of "homedrive") van een andere gebruiker te lezen zonder diens ondubbelzinnige toestemming.
   - Indien gegevens van een bepaalde gebruiker door andere personen geraadpleegd moeten kunnen worden, moet ervoor gezorgd worden dat deze op gedeelde schijfruimte of in een gedeelde mailbox zitten, of moet van een andere proxy-functionaliteit gebruik gemaakt worden.
   - Toegang tot privé-gegevens is enkel toegestaan in individuele uitzonderingsgevallen op gerechtelijk bevel of op verzoek van de Staatsveiligheid.
   - Logging en monitoring van metadata van communicatie en de toegang tot de bijhorende gegevens wordt niet geregeld in voorliggend document. Hiervoor wordt een specifiek beleid vastgelegd.
   - Uitzonderlijke toegang tot data van personen die tijdelijk of definitief handelingsonbekwaam zijn (bv. in geval van zwaar ongeval, coma, overlijden,…) valt buiten het toepassingsgebied van voorliggend document. Hiervoor wordt een specifieke procedure vastgelegd.

1.4. Bij het gebruik van de ICT-infrastructuur van de UGent moeten het **auteursrecht en andere intellectuele rechten** gerespecteerd worden. Dit houdt mede in dat auteursrechtelijk beschermd materiaal en software niet verder verspreid of gekopieerd mogen worden als dat in strijd is met de auteursrechten of de licentievoorwaarden.

1.5. Het is enkel toegelaten **software te installeren en te gebruiken** op apparatuur die deel uitmaakt van de ICT-infrastructuur van de UGent onder deze voorwaarden:
   - aan alle van toepassing zijnde auteursrechten en/of licentievoorwaarden is correct voldaan, m.a.w. het effectieve gebruik moet in overeenstemming zijn met de licentievoorwaarden (bv. sommige educatieve licenties mogen niet gebruikt worden in een onderzoekscontext);
   - de ermee verbonden informatieveiligheidsrisico's werden met gepaste zorg ingeschat en aanvaardbaar geacht, of werden met gepaste zorgvuldigheid tot een aanvaardbaar niveau teruggebracht (bv. door veilige configuratie of veiligheidstests)[3];
   - indien men software wil gebruiken die niet aan deze voorwaarden voldoet, moet op zoek gegaan worden naar alternatieven die daar wel aan voldoen.

1.6. Het is verboden **inbreuken te plegen op de beveiliging** van de ICT-infrastructuur van de UGent, van systemen aangesloten op Belnet, of van andere externe informaticasystemen

[3] https://www.ugent.be/informatieveiligheid

en het Internet[4]. Voorbeelden hiervan (niet-limitatieve opsomming):

- Toegang forceren tot systemen waartoe men niet geautoriseerd of gerechtigd is (ook al zijn die systemen onvoldoende beveiligd), en ook pogingen daartoe;
- Omzeilen van interne en externe systeem- en netwerkbeveiligingen;
- Informatie onderscheppen die voor anderen bedoeld is, bv. door netwerktraffiek te capteren via een vaste netwerkverbinding of met draadloze apparatuur;
- Zich voordoen als een andere gebruiker, bv. door met de accountgegevens van iemand anders in te loggen en te werken zonder diens toestemming (met dien verstande dat de gebruiker die zijn accountgegevens wetens en willens deelt het informatieveiligheidsbeleid overtreedt (zie punt 2.3));
- Met kwade bedoelingen schadelijke software (bv. computervirussen) op de ICT-infrastructuur van de UGent ontwerpen, installeren, (proberen) uitvoeren of (proberen) verspreiden;
- Kwaadaardige acties die leiden tot gedeeltelijke of complete vernietiging van (confidentialiteit, integriteit of beschikbaarheid van) informaticagegevens;

NB. Voor onderwijs- (bv. practica) en onderzoeksdoeleinden kunnen bepaalde activiteiten wel toegelaten worden, binnen een duidelijk afgelijnd kader en op een afgeschermd netwerk dat niet of niet rechtstreeks aan het UGentNet gekoppeld is.

1.7. Het is **verboden kwetsbaarheden** in de beveiliging van de ICT-infrastructuur van de UGent **op te sporen**, zelfs met goede bedoelingen (zgn. ethical hacking).

- Uitzondering: ICT-beheerders (zowel centraal als decentraal) hebben de verantwoordelijkheid om wel zelf voor systemen en toepassingen die onder hun bevoegdheid vallen actief kwetsbaarheden op te sporen (of te laten opsporen) en te remediëren (of te laten remediëren)[5].
- Als toch (bv. bij toeval) een kwetsbaarheid in de beveiliging van de ICT-infrastructuur van de UGent ontdekt wordt, dan moet de kwetsbaarheid zo snel mogelijk gemeld wordt aan de helpdesk van DICT en desgevallend aan de beheerder, ontwikkelaar of leverancier van het betreffende systeem. Het uitbuiten of onmiddellijk verder bekend maken van dergelijke kwetsbaarheden wordt beschouwd als ongeoorloofd.

1.8. **Systemen die op UGentNet mogen aansluiten**:

- Binnen de gebouwen van UGent kunnen computers en andere systemen via een UTP- kabel aansluiten op UGentNet, met een IP-adres dat automatisch of door DICT wordt toegekend volgens de bestaande procedures[6].
- Om de goede werking van het netwerk te garanderen, wordt het toewijzen van vaste IP-adressen en hostnamen centraal beheerd door DICT. Als er wijzigingen zijn in die registratiegegevens moet dit door de verantwoordelijke voor het systeem aan DICT gemeld worden (bv. een nieuw systeem wordt in dienst genomen, een toestel met een geregistreerd IP-nummer wordt uit dienst genomen, er is een wijziging van verantwoordelijke,…)
- Zowel geregistreerde als niet-geregistreerde systemen (bv. eigen toestellen zoals

[4] Zie ook de wet van 28 november 2000 inzake informaticacriminaliteit
[5] https://www.ugent.be/intranet/nl/op-het-werk/ict/informatieveiligheid/veilig-beheren-servers-services.pdf
[6] http://helpdesk.ugent.be/ugentnet/ip-registratie.php

laptops, smartphones, tablets) mogen binnen de gebouwen van de UGent draadloos aansluiten op de ICT-infrastructuur van de UGent via Eduroam[7].

- Zowel geregistreerde als niet-geregistreerde systemen (bv. eigen toestellen zoals laptops, smartphones, tablets) mogen van buiten de gebouwen van de UGent (bv. in
- het kader van telewerk) gebruik maken van de ICT-infrastructuur van de UGent via Athena[8] of erop aansluiten via VPN[9].
- In de studentenhomes mogen studenten hun eigen systemen via UTP-kabel aansluiten zonder voorafgaande registratie[10]. Op deze aansluitingen zijn een aantal beperkingen van toepassing. Uitgebreide functionaliteit is mogelijk via VPN.
- Alle systemen die gebruik maken van de ICT-infrastructuur van de UGent of die erop aansluiten, zowel bekabeld als draadloos, moeten voldoende beveiligd zijn overeenkomstig het informatieveiligheidsbeleid van de UGent[11]. Toestellen die hier niet aan voldoen (bv. legacy systemen die niet ge-update kunnen worden), moeten losgekoppeld zijn van het UGentNet.
- Met het oog op de goede werking en de beveiliging van de ICT-infrastructuur en in het bijzonder UGentNet, is het enkel toegelaten de structuur of de configuratie van het UGentNet te wijzigen mits toestemming van het functiedomein ICT. Het plaatsen van bijkomende actieve netwerkcomponenten vereist dus toestemming van het functiedomein ICT.
- Het functiedomein voorziet in, en beheert, alle WiFi draadloze toegangspunten; het plaatsen van eigen draadloze toegangspunten is niet toegelaten[12].

1.9. De werking van de ICT-infrastructuur van de UGent is aangewezen op **beperkte middelen** qua opslagcapaciteit, rekenkracht, bandbreedte, ondersteunend personeel, etc. Daarom moeten die middelen **zo efficiënt mogelijk** aangewend worden:

- Limieten vastgelegd op mailbox[13] of centrale schijfruimte[14] moeten in acht genomen worden, waarbij de gebruiker overbodige mails en files opruimt (rekening houdend met kosten en baten van dergelijke acties), en de informatie organiseert volgens de principes van goede digitale hygiëne[15].
- Het is verboden de goede werking van het universitaire netwerk en van de andere diensten en computers beheerd door DICT wetens en willens te schaden, bv. door het netwerk of bepaalde toepassingen met opzet overmatig te belasten (zgn. denial of service), of door ongewenste e-mails aan grote aantallen ontvangers te versturen (zgn. spam). Deze paragraaf legt een verbod op het verstoren van de goede werking van de ICT-diensten van de UGent, maar enkel in technische zin - deze paragraaf spreekt zich niet uit over het al dan niet opportuun zijn van bepaalde vormen van massacommunicatie.
- Efficiënt gebruik van de ICT-infrastructuur van de UGent vereist dat waar mogelijk

[7] http://helpdesk.ugent.be/eduroam
[8] http://helpdesk.ugent.be/athena
[9] http://helpdesk.ugent.be/vpn
[10] http://helpdesk.ugent.be/ugentnet/studentenhomes.php
[11] https://www.ugent.be/informatieveiligheid
[12] Bij beslissing BC 13 mei 2004, uitzonderingen zijn dus enkel mogelijk bij beslissing van het universiteitsbestuur.
[13] http://helpdesk.ugent.be/email
[14] http://helpdesk.ugent.be/netdisk
[15] http://www.ugent.be/nl/univgent/collecties/archief/informatiebeheer/informatiebeheer-2-digitale-hygiene

centraal aangeboden infrastructuur wordt aangesproken vooraleer de inzet van decentrale infrastructuur in overweging wordt genomen. In het laatste geval kan er best overlegd worden met het functiedomein ICT om te zien in hoeverre de nodige functionaliteit centraal voorzien is of (eventueel op termijn) kan voorzien worden. ICT-projecten van meer dan 30.000 euro worden in principe voorgelegd aan de ICT-Commissie van de UGent.

2. VERANTWOORDELIJKHEDEN VAN DE GEBRUIKERS

2.1. Gebruikers met een **UGent account**[16] krijgen toegang tot de ICT-infrastructuur van de UGent op basis van een gebruikersnaam en een wachtwoord[17]. De UGent account is een belangrijk onderdeel van de digitale identiteit van de gebruiker en moet met gepaste zorg beschermd worden, overeenkomstig het informatieveiligheidsbeleid van de UGent en in het bijzonder de bijhorende praktische richtlijnen[18].

2.2. Aan de UGent account is een **persoonlijk UGent e-mailadres** gekoppeld. Dit e-mail adres is het officiële communicatiekanaal tussen de gebruiker en de UGent. De corresponderende mailbox moet door de gebruiker op regelmatige basis geraadpleegd worden.

2.3. Een UGent account is strikt persoonlijk. De gebruiker is verantwoordelijk voor de aan hem/haar toegekende account en voor wat er onder de account gebeurt, behalve indien de gebruiker ondanks gepaste zorg zelf slachtoffer is van misbruik van de betreffende account. Voor de **bescherming van de UGent account** moeten in overeenstemming met het informatieveiligheidsbeleid o.a. de volgende regels in acht genomen worden[19]:

- Er moet een sterk wachtwoord (of een sterke wachtwoordzin20) gekozen worden, dat minstens jaarlijks gewijzigd wordt21.
- Het wachtwoord moet strikt geheim gehouden worden. Aanmeldgegevens van de eigen account mogen niet aan anderen doorgegeven worden, ook niet aan naaste medewerkers. Indien er toepassingen zijn die in naam van een gebruiker door andere personen moeten kunnen gebruikt worden, moet dit gebeuren via een proxy-functionaliteit.
- Wanneer het vermoeden bestaat dat het wachtwoord bekend geraakt is, moet het gecompromitteerde wachtwoord onmiddellijk gewijzigd worden7.
- Het hergebruik van hetzelfde wachtwoord van de UGent account voor andere diensten, intern of extern, is verboden.
- Het is niet toegelaten anderen onder het persoonlijke account te laten werken. Indien om praktische redenen een inbreuk op deze regel niet kan vermeden worden, kan tijdelijk een uitzondering gedoogd worden in afwachting van een correcte oplossing. Deze uitzonderingen moeten vooraf aangemeld worden bij de

[16] http://helpdesk.ugent.be/account
[17] http://helpdesk.ugent.be/account/wachtwoord.php
[18] https://www.ugent.be/intranet/nl/op-het-werk/ict/informatieveiligheid/veilig-werken-met-it.pdf
[19] Niet-limitatieve opsomming en in afwachting van eventuele bijkomende veiligheidsmaatregelen, bv. 2-factor authentication voor kritische toepassingen en kritische accounts.
[20] https://www.safeonweb.be/nl/tips/wat-je-moet-weten-over-het-veiliger-maken-van-wachtwoorden
[21] Dit wordt ook technisch afgedwongen, overeenkomstig beslissing BC 11 december 2015.

informatieveiligheidsconsulent.
Aan medewerkers of studenten kan niet gevraagd worden om hun accountgegevens verplicht door te geven.

- Wanneer een computer onbeheerd achtergelaten wordt, zelfs voor korte tijd, moet afgemeld of vergrendeld worden. Dit geldt zowel voor computers beheerd door DICT (bv. auditorium PC, PC-klas PC, publieke desktop,…) als voor eigen en andere toestellen.

2.4. De ICT-infrastructuur die door de UGent ter beschikking wordt gesteld, moet door de gebruikers met **gepaste zorg** behandeld worden. Dit houdt o.a. in:

- Wanneer een gebruiker vaststelt dat er een defect is of een slecht functioneren van een onderdeel van de ICT-infrastructuur, dan moet dit gemeld worden aan de daarvoor verantwoordelijke ICT-beheerder, of aan de helpdesk van DICT.
- ICT-middelen van de UGent mogen niet op onverantwoorde manier achtergelaten en zo blootgesteld worden aan het risico op diefstal of misbruik.
- Overeenkomstig de praktische richtlijnen van het informatieveiligheidsbeleid moeten alle gebruikers en ICT-beheerders actief verantwoordelijkheid nemen voor de beveiliging van de ICT-infrastructuur die ter beschikking staat.
- Alle informatieveiligheidsincidenten (bv. misbruik van account, infectie met malware, diefstal van apparatuur of data, datalek met persoonsgegevens of vertrouwelijke informatie,… (niet-limitatieve opsomming)) moeten zo snel mogelijk aan de helpdesk van DICT22 gemeld worden.

3. VERANTWOORDELIJKHEDEN TOV. SERVICE PROVIDER BELNET

Het universitaire netwerk UGentNet is aangesloten op Belnet[23], het Belgische onderzoeksnetwerk. Belnet heeft een Acceptable Use Policy (“AUP”)[24], die mede bepaalt wat wel en niet toegelaten is op netwerken aangesloten op Belnet.

Belnet onderschrijft de Gedragscode voor Service Providers[25] van de Belgische Internet Service Providers Association (ISPA), en het Belgische “Samenwerkingsprotocol ter bestrijding van ongeoorloofd gedrag op internet”. Draadloze WiFi toegang tot UGentNet via Eduroam valt onder de voorwaarden van de “Overeenkomst voor toetreding tot de Eduroam dienst van Belnet”[26].

4. NALEVING

Door een account te aanvaarden of door gebruik te maken van de ICT-infrastructuur van de UGent, verbindt de gebruiker er zich toe dit reglement na te leven. Dit reglement geldt dus ook voor externe, occasionele gebruikers van Eduroam via UGent access points.

---

[22] http://helpdesk.ugent.be/extra
[23] http://www.belnet.be
[24] Zie de voorschriften voor aanvaardbaar gebruik (“AUP”) van de BELNET internetdiensten, versie 01.02.2012
[25] http://www.ispa.be/code-conduct-nl
[26] Zie de overeenkomst voor toetreding tot de Eduroam dienst van Belnet

5. TOEZICHT, CONTROLE EN SANCTIES

5.1. De ICT-infrastructuur van de UGent wordt door ICT-systeembeheerders gecontroleerd (logging en monitoring) om de goede werking ervan te kunnen verzekeren en om misbruik op te sporen en te voorkomen. Het niveau van detail mag niet meer en de bewaarduur niet langer dan nodig zijn om dit doel te bereiken.

Het toezicht en controles gebeuren conform de CAO 81[27].

5.2. De informatieveiligheidsconsulent van de UGent heeft controlerende bevoegdheid voor de veilige verwerking van persoonsgegevens aan de UGent.

5.3. Het melden van incidenten gebeurt bij de helpdesk van DICT, die fungeert als eerste aanspreekpunt en tevens als doorverwijspunt naar andere bevoegde kanalen, bv. de informatieveiligheidsconsulent.

5.4. Bij incidenten kan DICT beslissen om bewarende technische maatregelen te nemen met als finaliteit en daartoe beperkt de ICT-infrastructuur en de goede werking ervan te beschermen.

5.5. Mogelijke maatregelen en sancties die tegen personen kunnen worden genomen bij vaststelling van actieve, bewuste en herhaaldelijke inbreuken op dit reglement en rekening houdend met de ernst van de inbreuk zijn:

- Ordemaatregelen door de Rector: de tijdelijke opheffing van een account of de tijdelijke beperking van de toegang tot (delen van) de ICT-infrastructuur (waarbij een evenwicht wordt gezocht tussen het belang van de dienst, de bescherming van de systemen en de rechten van de betrokkene, aangezien het account in veel gevallen noodzakelijk is voor het uitvoeren van de job of voor de studies);
- Maatregelen en sancties zoals voorzien in de toepasselijke (bv. arbeidsrechtelijke) regelgeving en in de interne reglementen van de UGent, o.a. de tuchtreglementen.

6. DEFINITIES

6.1. **ICT-infrastructuur**: hiermee wordt bedoeld zowel de netwerkinfrastructuur en de andere fysieke IT-gerelateerde apparatuur in eigendom van of in gebruik door de UGent (datacenters, servers, storage, desktops, laptops, printers, telefonie,…). Ten behoeve van dit reglement worden ook alle interne en externe ICT-toepassingen en diensten beheerd door de UGent of in opdracht van de UGent daarin inbegrepen. Dit omvat dus o.m. de diensten voor toegang en gebruik van op afstand (bv. Athena of VPN), diensten voor draadloze toegang in het kader van Eduroam,…

6.2. **UGentNET**: het door het functiedomein ICT beheerde computernetwerk van de Universiteit Gent en alle actieve en passieve componenten ervan.

[27] https://www.privacycommission.be/sites/privacycommission/files/documents/cao-081.pdf

6.3. **ICT-beheerders**: alle verantwoordelijken voor het onderhoud en het goed functioneren van de ICT-infrastructuur, zowel centraal (verbonden aan het functiedomein ICT) als decentraal (verbonden aan faculteiten en vakgroepen of andere universiteitsdiensten)

6.4. **Gerechtigde gebruiker**: Elke persoon die gebruik mag maken van de ICT-infrastructuur van de UGent. Er kan onderscheid gemaakt worden tussen:

- gebruikers met een normale UGent account[28] (studenten, personeelsleden en onbezoldigde medewerkers van de UGent, geregistreerde bezoekers aan de UGent,…)
- gebruikers van Eduroam zonder UGent account, maar met een account bij een andere instelling die aangesloten is op Eduroam
- gebruikers met een tijdelijke UGentGuest account voor WiFi
- andere gebruikers die op basis van bestuursbeslissingen specifieke toegang krijgen

[28] http://helpdesk.ugent.be/account/hoe.php
Beslissingen van het universiteitsbestuur ivm. toekennen van UGent accounts (niet-limitatieve opsomming):

- BC 20 september 2007: UGent accounts algemeen
- BC 28 februari 2008: accounts voor examencontractors en gepensioneerde ATP'ers
- BC 11 maart 2010: accounts voor loopbaanonderbrekers en jaarlijkse verlenging gepensioneerden
- BC 16 december 2010: accounts voor bezoekers en externe VSC gebruikers
- BC 27 oktober 2011: accounts voor externe onderwijsverstrekker, IVPV enkel indien in OASIS, beperkt account UCT, regeling voor personeel inkanteling
- BC 27 september 2012: "mini-accounts" OASIS voor herinschrijving, regeling voor studenten inkanteling
- BC 24 April 2014: schrappen accounts voor Degreeholders, volledig account UCT