Bijlage bij agendapunt I.2. van de Raad van Bestuur van 13 december 2005.

Regels met betrekking tot het gebruik van de ICT-infrastructuur aan de VUB

I. Definities

Universiteit : de Vrije Universiteit Brussel, de VUB.

ICT : Informatie- en CommunicatieTechnologie.

ICT-infrastructuur : het geheel van informatica- en communicatiemiddelen onder de vorm van computerapparatuur en -programmatuur, communicatienetwerken, informatiesystemen en elektronische gegevens. Het kan gaan om een lokale infrastructuur, beperkt tot één of meerdere entiteiten binnen de Universiteit of om de gehele universiteitsinfrastructuur.

ICT-beheerder : éénieder die belast is met de goede werking, het onderhoud en de uitbouw van een lokale ICT-infrastructuur.

Algemene ICT-beheerder : de verantwoordelijke voor de hoofdeenheid DICT.

Gebruiker : elke medewerker van de VUB of student aan de VUB of occasionele derde, die op welke wijze dan ook de ICT-infrastructuur van de VUB gebruikt.

Bureau van de Raad van Bestuur van het Rekencentrum : belast met het dagelijks bestuur van het Rekencentrum en VUBNET (de eenheid die het netwerk van de VUB beheert).

Academische activiteiten : het geheel van taken en handelingen die kaderen binnen de uitoefening van de decretale opdrachten van de Universiteit, met name Onderwijs, Onderzoek en Maatschappelijk Dienstbetoon. Hieronder vallen ook alle sociale, culturele en sportactiviteiten die de gebruikers beoefenen in het kader van met de toestemming van de universitaire overheid georganiseerde evenementen.

II. Voorwerp

De Vrije Universiteit Brussel stelt haar gebruikers, lastens de werkingstoelage van de Vlaamse Overheid, een uitgebreide ICT-infrastructuur ter beschikking voor de logistieke ondersteuning van de academische activiteiten.

Wettelijke en morele verplichtingen enerzijds en economische overwegingen anderzijds vereisen dat de VUB de nodige voorzorgen neemt met betrekking tot het correcte gebruik van deze ICT-middelen. Het uitgangspunt is dat hiermee op een verantwoorde en passende wijze omgesprongen wordt. Elke gebruiker is daarom gehouden kennis te nemen van de hierna volgende gebruiksregels en deze in acht te nemen.
Omwille van de snelle evolutie in de ICT zullen deze gebruiksregels indien nodig aangepast worden.

De hierna volgende regels zijn niet van toepassing voor het gebruik van de ICT-infrastructuur in de studentenkamers onder VUB-beheer.

III. Regels voor het gebruik

De hier vermelde regels vormen een voorschrift voor het correct gebruik van de ICT-infrastructuur van de Universiteit. Elke afwijking op deze regels, bijvoorbeeld in het kader van bijzonder wetenschappelijk onderzoek of in naam van de academische vrijheid, dient vooraf schriftelijk aangevraagd te worden bij het Bureau van de Raad van Bestuur van het Rekencentrum dat over dergelijke aanvraag tot afwijking een gemotiveerde beslissing zal nemen. Het is mogelijk beroep aan te tekenen tegen deze beslissing bij het Bestuurscollege van de Universiteit.

Het niet op de hoogte zijn van deze regels kan niet ingeroepen worden om ze niet na te leven.

1. Oneigenlijk en ongeoorloofd gebruik

De ICT-infrastructuur dient te worden gebruikt in het kader van de academische activiteiten, met inachtneming van de normale deontologische regels. Het is dus, onder andere, niet toegestaan de ICT-infrastructuur te gebruiken om

a) informatie aan te maken, te verspreiden, ter beschikking te stellen of op te slaan die
   - in strijd is met de openbare orde of de goede zeden
   - indruist tegen de wetgeving op de bescherming van de persoonlijke levenssfeer
   - strijdig is met het auteursrecht
   - de goede naam van de VUB kan schaden of die haar economisch nadeel kan berokkenen
   - schade kan berokkenen aan derden

b) ongevraagde elektronische post (spam), kettingbrieven of schadelijke computer-programma's zoals bijvoorbeeld virussen, wormen (trojans), spionnen (spyware) of adverteersoftware (adware) te ontwikkelen of te verspreiden

c) een valse identiteit aan te nemen op het netwerk

d) commerciële of politieke activiteiten te ontwikkelen of te ondersteunen ten persoonlijken titel of voor rekening van derden zonder voorafgaande toestemming van de universitaire overheid

e) vertrouwelijke informatie of gegevens ter beschikking te stellen van anderen die niet gerechtigd zijn deze te ontvangen

f) ongeoorloofde toegang proberen te verkrijgen tot interne of externe computer-systemen

g) kennis te nemen van communicatie tussen derden

h) bestanden of informatie te wijzigen indien men hiertoe niet gemachtigd is

i) internetsites te bezoeken die onwettig materiaal bevatten

j) andere gebruikers te hinderen door overmatig of onredelijk gebruik

k) zonder voorafgaande toelating van een ICT-beheerder apparatuur aan te sluiten (ook niet draadloos) op de ICT-infrastructuur van de VUB. De aansluiting van apparatuur

op het netwerk kan enkel indien vooraf een IP-adres of de gebruiker zelf werden geregistreerd.

2. Verantwoordelijkheid van de gebruiker

De gebruiker is verantwoordelijk voor het goede en veilige gebruik van de hem ter beschikking gestelde ICT-middelen. Hij dient als een goede huisvader zorg te dragen voor de door hem gebruikte of beheerde computerapparatuur (een persoonlijke werkpost, een server of een netwerkomgeving) en -programmatuur. De gebruiker treft de nodige maatregelen om de risico's op diefstal, inbraak of oneigenlijk gebruik tot een minimum te beperken. Dit impliceert de fysische beveiliging van de apparatuur, het up-to-date houden van antivirusprogramma's en van systeemconfiguraties en in het bijzonder van de veiligheidsvoorzieningen. Een computeraccount (gebruikersnaam en paswoord) of de netwerkidentiteit zijn strikt persoonlijk en informatie hierover mag dus niet aan derden verstrekt worden, zelfs niet met betrekking tot de eigen persoonlijke werkpost. De nodige voorzichtigheid is aangewezen bij het installeren van nieuwe apparatuur of programmatuur. Het downloaden en installeren van software waarvan de oorsprong en/of de werking onduidelijk zijn is ten zeerste af te raden.

De gebruiker zal ook omzichtig omspringen met het via het internet bekendmaken van zijn VUB elektronische postadres of persoonlijke webpagina.

Om de algemene veiligheid van de ICT-infrastructuur te verbeteren is de gebruiker ertoe gehouden eventuele incidenten of lacunes in de beveiliging te melden aan de (algemene) ICT-beheerder.
Samengevat dienen de volgende aanbevelingen naar best vermogen nageleefd te worden :

1) installeer enkel software (uitbatingssysteem en toepassingen) conform de auteursrechterlijke bepalingen (meestal zijn dit de licentievoorwaarden)
2) actualiseer de software wanneer nodig
3) installeer geen software waarvan de oorsprong of de werking onduidelijk zijn
4) activeer enkel de noodzakelijke diensten op de computer
5) wees discreet over computeraccounts, zelfs de persoonlijke; gebruik veilige paswoorden en hou ze geheim
6) gebruik de beschikbare beveiligingsvoorzieningen, zoals een antivirus-programma (te bekomen via de website http://softweb.vub.ac.be) en een persoonlijke firewall (beschikbaar als service via het uitbatingssysteem van de meeste PC's)
7) stel computerapparatuur of een toegang tot het netwerk niet ter beschikking van derden zonder voorafgaande toestemming van de ICT-beheerder.

3. Verantwoordelijkheid van de ICT-beheerder

De ICT-beheerder zorgt ervoor dat de hier vermelde gebruiksregels door de gebruikers van de door hem beheerde ICT-infrastructuur correct nageleefd worden. Indien hij een misbruik

vaststelt doet hij het nodige om dit onverwijld te doen stoppen. Desgevallend brengt hij de algemene ICT-beheerder op de hoogte zodat de nodige maatregelen kunnen getroffen worden.

4. Gebruik ten persoonlijken titel

Een persoonlijk gebruik van de VUB ICT-infrastructuur is in **zeer beperkte mate** toegelaten, voor zover

- andere gebruikers niet gehinderd worden bij hun academische activiteiten
- de individuele arbeidsprestaties (volume en kwaliteit) niet in het gedrang komen
- geen meerkosten gegenereerd worden ten laste van de Universiteit
- het imago van de Universiteit niet geschaad wordt
- dit niet in tegenspraak is met de bepalingen in paragrafen III. 1, III.2 en III.3.

De Universiteit kan op elk ogenblik

- deze mogelijkheid tot persoonlijk gebruik intrekken
- overdreven kosten te wijten aan persoonlijk gebruik verhalen op de gebruiker
- eventuele verloren arbeidstijd sanctioneren.

Verder zal de algemene ICT-beheerder alle nodige technische maatregelen nemen om er voor te zorgen dat dit persoonlijk gebruik zeer beperkt blijft. Dit kan zijn het reduceren van de bandbreedte voor een bepaald type netwerkverkeer of zelfs het totaal blokkeren ervan, of nog het verlagen van de prioriteit zodat het andere verkeer voorrang heeft. Zo kan ook de toegang tot bepaalde websites waarvan bekend is dat zij een veiligheidsrisico vormen afgesloten worden. De verspreiding van bepaalde bestanden (via elektronische post of andere methodes) die een groot veiligheidsrisico zoals virussen inhouden kan verhinderd worden.

Persoonlijke webpagina's dienen conform te zijn met de hier vermelde gebruiksregels. Zij moeten dus ook beperkt blijven tot de academische activiteiten van de auteur die als enige verantwoordelijk is.

Het is verder niet toegestaan via de ICT-infrastructuur van de VUB welke diensten dan ook aan te bieden aan derden zonder voorafgaandelijke overeenkomst met de VUB.

IV. Veiligheidsprofielen

Teneinde de globale ICT-infrastructuur zo goed mogelijk te beheren en een aanvaardbaar niveau van veiligheid te verzekeren worden zogenaamde veiligheidsprofielen gehanteerd. De veiligheid heeft immers voornamelijk te maken met de netwerkprotocollen die tussen de op het netwerk aangesloten machines mogelijk zijn.
Wat niet expliciet is toegestaan, is verboden : er zijn enkel een beperkt aantal netwerk-protocollen mogelijk. Veiligheidsprofielen zijn gebaseerd op twee karakteristieken : veiligheidsniveau en beheersverantwoordelijkheid. Er worden drie veiligheidsniveau's

onderscheiden : maximaal, gemiddeld en minimaal. De beheersverantwoordelijkheid kan centraal zijn (de algemene ICT-beheerder), lokaal (een lokale ICT-beheerder of een individuele gebruiker) of gedeeld.

Aan elk aangesloten toestel wordt aldus één van de volgende profielen geassocieerd :

veiligheid / beheer	maximaal	gemiddeld	minimaal
centraal	profiel 11	profiel 12	profiel 13
centraal / lokaal	profiel 21	profiel 22	profiel 23
lokaal	profiel 31	profiel 32	profiel 33

Deze algemene profielen worden verder onderverdeeld op basis van de toegelaten netwerk-protocollen en toepassingen. Dit resulteert in een aantal specifieke configuraties die dienen om de routers, switches, firewalls en netwerkservers te programmeren. Omdat het niet mogelijk is hiervan een uitputtende lijst op te stellen, en om veiligheidsredenen, wordt deze informatie niet publiek gemaakt maar slechts verstrekt waar en wanneer nodig.

Enkel profiel 11, maximale veiligheid onder centraal beheer, wordt zonder voorafgaande toelating toegekend. Elk ander profiel dient expliciet aangevraagd worden aan de algemene ICT-beheerder via de hiertoe beschikbare intrawebtoepassing en zal desgevallend toegekend worden op basis van de vigerende veiligheidscriteria. Indien de aanvrager niet akkoord gaat met het aan zijn toestel toegekende profiel kan hij beroep aantekenen bij het Bureau van de Raad van Bestuur van het Rekencentrum en in tweede instantie bij het Bestuurscollege van de Universiteit. Hierbij zal uitgegaan worden van wat technisch mogelijk is, binnen de beschikbare financiële middelen.

Indien vastgesteld wordt dat een op het netwerk aangesloten toestel (PC, server, enz...) zonder toelating een ander profiel blijkt te vertonen dan het oorspronkelijk toegekende, kan de (algemene) ICT-beheerder ingrijpen. De aard van de interventie wordt bepaald door de ernst van de situatie. In extreme gevallen zal de betrokken machine van het netwerk afgekoppeld worden.

V. Toezicht op het gebruik

De Nationale Arbeidsraad heeft op vrijdag 26 april 2002 de collectieve arbeidsovereenkomst nr. 81 gesloten tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens. Deze CAO werd bekrachtigd in een Koninklijk besluit van 12 juni 2002 en is ook van toepassing op de universiteiten.
CAO 81 verzoent het recht van de werkgever om controle uit te oefenen op het gebruik van communicatiemiddelen door de werknemers met het recht van de werknemers op eerbiediging van hun persoonlijke levenssfeer conform de wet van 8 december 1992.

De personeelsleden worden eraan herinnerd dat deze CAO en de hier gestipuleerde regels niet als verzet kunnen aangevoerd worden tegen de gerechtelijke overheid die handelt in het kader van haar wettelijke opdracht. Het zoeken naar plegers van inbreuken door de gerechtelijke overheid kan bijgevolg aanleiding geven tot ondervragingen binnen de wettelijke procedures hetgeen deze regels niet zullen kunnen verhinderen.

> Om praktische redenen en om voor éénieder zoveel mogelijk dezelfde rechten en plichten te kunnen doen gelden, zullen de in CAO 81 gestipuleerde regels van toepassing zijn op alle gebruikers —personeelsleden, studenten en occasionele derden— van de ICT-infrastructuur van de VUB.

Behalve de eventuele sluiting van de computeraccount van een gebruiker of van zijn toegang tot het netwerk, conform de hier vermelde regels, zijn de sancties die desgevallend bij een abusief gebruik van de ICT-infrastructuur toegepast worden, de disciplinaire sancties vernoemd in de algemene reglementen die van toepassing zijn op respectievelijk de verschillende personeelsgeledingen en op de studenten. Occasionele derden zullen onmiddellijk de toegang tot de ICT-infrastructuur ontzegd worden. De VUB behoudt zich het recht voor om eventuele schade of kosten op de overtreders te verhalen, desgevallend via gerechtelijke weg.

1. controle op de inhoud van de communicatie : principieel verbod

Geen enkele controle kan uitgevoerd worden op de inhoud van de communicatie tussen gebruikers, behoudens uit absolute strafrechterlijke noodzaak. Onder dit verbod valt niet de geautomatiseerde verwerking in het kader van bijvoorbeeld een antivirus- en/of antispamfiltering daar deze enkel tot doel hebben de integriteit van de ICT-infrastructuur te bewaren.

2. controle op de communicatiegegevens

- grondbeginsel en finaliteit

Volgens de hieronder vermelde voorwaarden kan de VUB en met name de algemene ICT-beheerder overgaan tot de controle van de communicatie*gegevens* van de gebruikers. Dit betreft de gegevens die toelaten een afzender en/of ontvanger te identificeren, een op het Internet geconsulteerde site, tijdstip en duur van de communicatie, aantal berichten, volume enz... Dergelijke controle kan echter enkel uitgevoerd worden voor één van de volgende doeleinden:

1) het voorkomen van onwettige of lasterlijke feiten, van feiten strijdig met de goede zeden, van de aantasting van de waardigheid van derden (bv.: piraterij, kwaadaardigheid, onrechtmatig toeëigenen van rekeningen, misbruik van het netwerk, enz...)
2) de bescherming van de economische en financiële belangen van de VUB die een

vertrouwelijk karakter hebben

3) de veiligheid en/of de goede technische werking van de ICT-infrastructuur van de VUB, met inbegrip van het toezicht op de kosten die ermee gepaard gaan, evenals de materiële bescherming van de installaties van de VUB (vb.: interventie van de beheerder om overmatig gebruik van het netwerk vast te stellen en te beëindigen)
4) het te goeder trouw naleven van de aan de VUB geldende beginselen en deze gebruiksregels;

De hierboven beschreven controle mag geen systematisch karakter vertonen.

- directe en indirecte controle

Voor hogergenoemde punten 1) tot en met 3) kan de algemene ICT-beheerder een directe controle uitoefenen op de communicatiegegevens van een gebruiker, zonder deze voorafgaandelijk in te lichten. In geval van onregelmatigheid zal het diensthoofd van de gebruiker of de decaan van de student en het Bureau van de Studentenraad op de hoogte gebracht worden. Indien nodig wordt de computeraccount en/of de netwerktoegang afgesloten tot de normale situatie hersteld is. Het diensthoofd of de decaan zal de maatregelen nemen die hij opportuun acht. Disciplinaire maatregelen worden desgevallend genomen volgens de vigerende procedures.

In geval 4) kan de algemene ICT-beheerder enkel een indirecte controle uitoefenen volgens de hierna vermelde procedure :

- indien een onregelmatigheid vastgesteld wordt kan niet onmiddellijk tot individualisering overgegaan worden. Eerst dient de gehele gemeenschap van deze onregelmatigheid op de hoogte gebracht te worden en gewaarschuwd dat indien deze zich opnieuw voordoet, tot individualisering zal overgegaan worden.
- in geval er zich toch nog een onregelmatigheid voordoet na deze algemene waarschuwing, kan de algemene ICT-beheerder de ervoor verantwoordelijk geachte gebruiker individualiseren. Dan treedt de volgende procedure in werking :
    - voorafgaand aan elke sanctie of beslissing wordt de betrokken gebruiker met zijn diensthoofd/decaan en desgevallend een vertegenwoordiger van de Studentenraad uitgenodigd voor een gesprek waarbij hij de mogelijkheid krijgt zijn bezwaren te uiten met betrekking tot de evaluatie of voorgenomen beslissing en zijn gebruik van de hem ter beschikking gestelde ICT-middelen nader te verklaren;
    - na dit gesprek kan de algemene ICT-beheerder tijdelijk de computeraccount of de netwerktoegang van de gebruiker afsluiten tot de normale situatie hersteld is. Het diensthoofd/de decaan zal de maatregelen nemen die hij opportuun acht. Disciplinaire maatregelen worden desgevallend genomen volgens de vigerende procedures.

- evenredigheidsbeginsel

Welke ook de toegepaste procedure is, de controle op de communicatiegegevens van de gebruikers blijft onderworpen aan het evenredigheidsbeginsel dat deze controle beperkt tot

wat strikt noodzakelijk is om te voldoen aan de beoogde wettige finaliteit.

3. Systematische gegevensopslag om de veiligheid en de goede werking van de ICT-infrastructuur te verzekeren

De gebruikers worden ervan op de hoogte gebracht dat het gebruik van de ICT-infrastructuur van de VUB de systematische en automatische opslag en archivering met zich meebrengt van gegevens met betrekking tot de gebruikers (afzender en/of ontvanger), het tijdstip, de duur, de frequentie, het volume en de aard van bepaalde elektronische handelingen. Sommige gegevens kunnen een persoonlijk karakter bezitten. Deze gegevens zijn slechts toegankelijk voor een beperkt aantal personeelsleden, verantwoordelijk voor het beheer van de ICT-infrastructuur. Zij worden verzameld met als doel :

- de statistische verwerking met het oog op een optimaal beheer van de ICT-infrastructuur (lange termijnbeheer);
- de gebruikers te identificeren in geval van technische problemen of verkeerde configuratie van hardware of software (korte termijnbeheer);

De gebruikers worden er eveneens van op de hoogte gebracht dat gegevens die zich op hun persoonlijke werkpost of op de eigen ruimte van een multi-user server bevinden, opgeslagen kunnen worden in het kader van een regelmatige backup procedure. Deze opslag dient uitsluitend om eventueel verloren gegane bestanden te kunnen recupereren.

4. Bewaartijd van de gegevens

De gegevens met betrekking tot de gebruikers worden maar zo lang bewaard als nodig voor de beoogde finaliteit, onverminderd de wettelijke bepalingen die de werkgever en bij extensie de ICT-beheerder een langere bewaartijd opleggen.
De hierna vermelde bewaartijden zijn slechts illustratief en betreffen enkel de centrale voorzieningen (Rekencentrum en VUBnet). Zij kunnen op elk ogenblik gewijzigd worden zonder voorafgaandelijke waarschuwing.

- gebruiksgegevens van de Web Proxy servers : een week;
- gedetailleerde accounting van de mail- en rekenservers : een week;
- toegangsgegevens tot de mail- en rekenservers en hun gecondenseerde accounting : onbeperkt;
- tijdstip van verzenden/ontvangen van email, grootte van het bericht, identiteit van verzender/ontvanger : 12 tot 18 maanden;
- modemgebruik, inclusief nummer: 12 tot 18 maanden;
- toegang tot Web en FTP servers, naam van bestanden en URL's : 12 tot 18 maanden;

De gegevens die verzameld worden in toepassing van CAO 81 worden slechts zolang bewaard als nodig voor de controle en voor de duur van een eventuele disciplinaire procedure.

TITEL I - ALGEMEEN BELEID

De VOORZITTER verwelkomt allen en in het bijzonder dhr. Ebinger die voor het eerst als ZAP-afgevaardigde van de faculteit GF de vergadering bijwoont.

Goedkeuring agenda.

Op verzoek van de Vice-Rector Onderwijs worden de punten IV.11, IV.12, IV.13 en IV.14 van de agenda afgevoerd.

Punt I.1.
Goedkeuring van het verslag van de Raad van Bestuur van 25 oktober 2005 (nr. 554).

Beslissing : code: RVB.555/A3/01

De Raad van Bestuur keurt het verslag van de Raad van Bestuur van 25 oktober 2005 (nr. 554) goed.

Punt I.2.
ICT-reglement.

Dhr. RAEYMAEKERS argumenteert dat het vorige ICT-reglement niet langer toereikend is wegens de evolutie qua techniek en informatica. Vandaag zijn nieuwe clausules noodzakelijk geworden ter wille van een correcte behandeling van de veiligheidsaspecten. Ter illustratie bij die nieuwe filosofie plukt hij enkele relevante zinnen uit het reglement:
Een eerste voorbeeld is de definitie van de gebruikers die zeer breed is, inclusief de occasionele derde die op welke wijze dan ook de ICT-infrastructuur van de VUB gebruikt, met één restrictie hierop zodat dit reglement niet van toepassing is op de studentenkamers. Op die locaties is het de bedoeling een ander aanbod te verzekeren om de kotbewoners wat meer soepelheid te bieden. PC-zalen vallen dus wel binnen de toepassing van dit reglement.
Verder is de opsomming van het oneigenlijk gebruik een niet-exhaustieve waslijst van activiteiten waaronder het verspreiden van informatie die in strijd is met de openbare orde en goede zeden, of die de goede naam van de VUB kan schaden of de instelling economisch nadeel berokkenen. Het aannemen van een valse identiteit is in deze ook belangrijk en helaas zijn er nogal wat inbraakpogingen van hackers op en via interne systemen tot in externe computers.
In een tweede paragraaf wordt de nadruk gelegd op de verantwoordelijkheid van de gebruiker. Deze mag geen informatie in verband met de eigen account doorspelen en hoort de verdere aanbevelingen met betrekking tot de installatie van software in acht te nemen. Een nieuw element in vergelijking met het voorgaande reglement is dat persoonlijk gebruik conform de realiteit beperkt toegelaten wordt onder enkele voorwaarden.
De belangrijkste nieuwigheid is de invoering van de veiligheidsprofielen.
Vandaag is alles toegelaten behalve dat wat expliciet verboden is, iets wat in een netwerkomgeving zeer gevaarlijk is. Daarom wordt hier het omgekeerde voorgesteld, dus is de lijst veel korter en zijn ook de formele uitzonderingen makkelijker beheersbaar. De verschillende veiligheidsprofielen worden in een matrix duidelijk gemaakt. Het meest veilige profiel wordt automatisch toegekend, alle andere kunnen pas na aanvraag en dus registratie toegestaan worden.
Een laatste punt betreft het toezicht conform de CAO 81, die de bedoeling heeft om het recht op privacy van de werknemer te verzoenen met het recht op controle van de werkgever. De tekst daarvan wordt hier samengevat en uitgewerkt. De controle slaat op de communicatiegegevens, niet op de inhoud en is beperkt tot het strikt noodzakelijke. Deze gegevens worden afhankelijk van hun natuur gedurende een zekere tijd bewaard, zoals bepaald in het reglement.

Dhr. RAEYMAEKERS vraagt de goedkeuring van de Raad van Bestuur en zijn akkoord om een afgevaardigde van de Studentenraad op te nemen in de Raad van Beheer van het Rekencentrum, de opdracht aan de Directeur ICT om een regeling voor de studentenkamers uit te werken en een meer transparante communicatiestrategie op te zetten, plus de opdracht aan de Algemeen Directeur om het Rekencentrum te verzoeken een student op te nemen in zijn Raad van Beheer.

Dhr. BENICHOU verklaart namens de Studentenraad zeer tevreden te zijn met de oplossing aangaande het gebruik in studentenkamers, en begrijpt de beperkingen voor de PC-zalen. Wel zou hij graag een deadline zien qua implementatie van een reglement voor de studentenkamers.

Dhr. RAEYMAEKERS stelt dat dit afhankelijk zal zijn van het type infrastructuur waarvoor gekozen wordt. De twee extremen zijn of de huidige VUB-service of een commerciële met een externe provider waarbij dan diens reglement zal gelden. Ook een tussenoplossing is mogelijk maar dit moet onder andere nog bekeken worden met de dienst Huisvesting. Er zijn al prijzen gevraagd maar die zijn nogal uiteenlopend. Begin volgend jaar zal hij genoeg gegevens verzameld hebben om de discussie te voeren met de STR. Hij hoopt tegen eind februari de principsbeslissing te hebben zodat dan zo snel mogelijk met de implementatie kan gestart worden. Bedoeling is dat alles zeker rond is voor het begin van het volgende academiejaar.

Beslissing : code: RVB.555/L12/01

Overwegende

- het voorstel van reglement in bijlage aan de agenda;

- het overleg met de studentenvertegenwoordiging, en meer in het bijzonder dat overeengekomen werd om in gezamenlijk overleg een oplossing te zoeken voor het gebruik van de ICT-infrastructuur op de studentenkamers onder beheer van de Vrije Universiteit Brussel;

- de versoepelingen die reeds werden toegepast voor de studentenkamers,

beslist de Raad van Bestuur

- de "Regels met betrekking tot het gebruik van de ICT-infrastructuur aan de Vrije Universiteit Brussel", in bijlage aan de agenda, goed te keuren;

- principieel akkoord te gaan dat een afgevaardigde van de Studentenraad wordt opgenomen in de Raad van Beheer van het Rekencentrum;

- opdracht te geven aan de Directeur ICT
  - om in samenwerking met de Studentenraad een bijzondere regeling uit te werken voor het gebruik van de ICT-infrastructuur op de studentenkamers onder beheer van de Vrije Universiteit Brussel teneinde deze uiterlijk tegen volgend academiejaar te implementeren;
  - een meer transparante communicatiestrategie naar personeel en studenten op te zetten;

- opdracht te geven aan de Algemeen Directeur een verzoek te richten aan het Rekencentrum om een student op te nemen in zijn Raad van Beheer.

VRIJE UNIVERSITEIT BRUSSEL
Secretariaat van de Raad
Pleinlaan 2 - 1050 Brussel

UITTREKSEL UIT DE NOTULEN

Voor uitvoering:		Ter informatie aan:	Einde termijn CVR
- VO	- DP	Studentenbeleid	3. 1. 2006
- SR	- FB	DP	
- RT	- FA	-	De Algemeen Directeur
X AD	- TD	-	
X Paul Raeymaekers			J. VAN LEEMPUT
-	-		
-	-		

RAAD VAN BESTUUR VAN 13 DECEMBER 2005
Code: RVB.555/L12/01

Punt I.2.
ICT-reglement.

Overwegende

- het voorstel van reglement in bijlage aan de agenda;
- het overleg met de studentenvertegenwoordiging, en meer in het bijzonder dat overeengekomen werd om in gezamenlijk overleg een oplossing te zoeken voor het gebruik van de ICT-infrastructuur op de studentenkamers onder beheer van de Vrije Universiteit Brussel;
- de versoepelingen die reeds werden toegepast voor de studentenkamers,

beslist de Raad van Bestuur

- de "Regels met betrekking tot het gebruik van de ICT-infrastructuur aan de Vrije Universiteit Brussel", in bijlage aan de agenda, goed te keuren;
- principieel akkoord te gaan dat een afgevaardigde van de Studentenraad wordt opgenomen in de Raad van Beheer van het Rekencentrum;
- opdracht te geven aan de Directeur ICT
  - om in samenwerking met de Studentenraad een bijzondere regeling uit te werken voor het gebruik van de ICT-infrastructuur op de studentenkamers onder beheer van de Vrije Universiteit Brussel teneinde deze uiterlijk tegen volgend academiejaar te implementeren;
  - een meer transparante communicatiestrategie naar personeel en studenten op te zetten;
- opdracht te geven aan de Algemeen Directeur een verzoek te richten aan het Rekencentrum om een student op te nemen in zijn Raad van Beheer.

DE SECRETARIS VAN DE RAAD,

Nadina PEETERS

STUDENTENBELEID
Te behandelen door:
Ter info aan:
Opmerkingen:

Vrije Universiteit Brussel

ALGEMENE DIRECTIE

RAAD VAN BESTUUR 13 DECEMBER 2005, PUNT I.2.

UW BERICHT VAN	UW KENMERK	ONS KENMERK	DATUM
		DR.05/L6/268/JVL/cv	07.12.2005.

BETREFT | ICT-reglement.

Gelet op :

- het voorstel van reglement in bijlage aan de agenda ;

overwegende :

- het overleg met de studentenvertegenwoordiging ;
- m.i.b. dat overeengekomen werd in gezamenlijk overleg een oplossing te zoeken voor het gebruik van de ICT-infrastructuur op de studentenkamers onder beheer van de Vrije Universiteit Brussel;
- de versoepelingen die reeds werden toegepast voor de studentenkamers;

beslist de Raad van Bestuur :

- de "regels met betrekking tot het gebruik van de ICT-infrastructuur" aan de Vrije Universiteit Brussel goed te keuren;
- principieel akkoord te gaan dat een afgevaardigde van de studentenraad wordt opgenomen in de Raad van Beheer van het rekencentrum;
- opdracht te geven aan de directeur ICT :
  - in samenwerking met de studentenraad een bijzondere regeling uit te werken voor het gebruik van de ICT-infrastructuur op de studentenkamers onder beheer van de Vrije Universiteit Brussel;
  - een meer transparante communicatiestrategie naar personeel en studenten op te zetten;
- opdracht te geven aan de algemeen directeur een verzoek te richten aan het rekencentrum om een student op te nemen in zijn Raad van Beheer.

*****

Pleinlaan 2 - 1050 Brussel | Tel. +32 (0)2 629 21 42 | Fax. +32 (0)2 629 38 27 | jmvleemp@vub.ac.be