REGLEMENT ICT-VOORZIENINGEN VOOR STUDENTEN VRIJE UNIVERSITEIT AMSTERDAM

Versie 1.0

IS VERDER KIJKEN

Reglement ICT-voorzieningen voor studenten Vrije Universiteit Amsterdam

Inhoudsopgave

HOOFDSTUK 1. INLEIDING

De Vrije Universiteit Amsterdam (hierna: **VU**) geeft studenten toegang tot haar ICT-voorzieningen zoals computers, internet, e-mail en andere applicaties. Het is van groot belang dat de ICT-voorzieningen op veilige en verantwoorde wijze worden gebruikt door studenten.

In dit 'Reglement ICT-voorzieningen voor studenten Vrije Universiteit Amsterdam' (hierna: **Reglement**) wordt beschreven welke gedragsregels gelden voor het gebruik van ICT-voorzieningen door studenten. Daarmee wil de VU duidelijk maken wat zij onder veilig en verantwoord gebruik verstaat en welk gedrag van studenten wordt verwacht. Het doel hiervan is:

- het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-Voorzieningen[1];
- het beheersbaar houden van kosten voor de VU; en
- ervoor zorgen dat de rechten en reputatie van de VU en anderen niet worden geschonden.

Daarnaast wordt in dit Reglement uiteengezet hoe de VU toezicht houdt op haar ICT-voorzieningen. De VU zorgt hierbij voor een goede verhouding tussen het bereiken van de hiervoor genoemde doelen enerzijds en privacybelangen van studenten anderzijds.

Logging en monitoring spelen een belangrijke rol in het toezicht op de ICT-voorzieningen. Logging en monitoring vinden geautomatiseerd plaats en zijn in principe niet gericht op individuele studenten. Vanzelfsprekend vindt logging en monitoring alleen plaats op ICT-voorzieningen van de VU en niet op de ICT-middelen van de student zelf.

Onderzoek naar individuele studenten is alleen mogelijk wanneer een gerechtvaardigd vermoeden bestaat van overtreding van de gedragscode of een ernstig verwijtbare andere gedraging. Uitgangspunt bij gericht onderzoek is dat alleen wordt gekeken naar verkeersgegevens (ook wel 'metadata' genoemd) en niet naar inhoud van bestanden of berichten. Alleen bij zwaarwegende redenen en wanneer dit noodzakelijk is, is het mogelijk dat inhoudelijke gegevens van individuele studenten, voor zover deze zijn opgeslagen op of binnen ICT-voorzieningen van de VU, worden onderzocht. De voorwaarden waaronder gericht en inhoudelijk onderzoek mogelijk zijn, worden in dit Reglement uiteengezet. Daarnaast wordt beschreven voor welke andere doeleinden verkeersgegevens worden gebruikt.

Individueel onderzoek richt zich niet op de ICT-middelen van de student zelf. De VU kan en zal geen onderzoek doen in bijvoorbeeld de privé e-mail, privé laptop of telefoon van een student. Wanneer een student gebruik maakt van bijvoorbeeld het netwerk van de VU (o.a. Eduroam of VU-campusnet) via een privé-apparaat zal dit gebruik wel gelogd en gemonitord worden. Hierbij gaat het om verkeersgegevens en niet om inhoudelijke gegevens.

Tot slot wordt vermeld hoe het toezicht op de naleving van dit Reglement is geregeld en welke slotbepalingen gelden.

[1] Deze begrippen komen uit de informatiebeveiliging en houden in dat systemen en de informatie die daarop staat toegankelijk zijn (beschikbaar), betrouwbaar zijn (integriteit) en alleen te raadplegen zijn door de juiste personen (vertrouwelijk).

HOOFDSTUK 2. ALGEMENE BEPALINGEN

Artikel 1. Begrippen

a. **Acceptabel gebruik**: gebruik van de ICT-voorzieningen waarbij de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-voorzieningen is gewaarborgd, de kosten beheersbaar zijn en de rechten en reputatie van de VU en derden niet worden geschonden.

b. **Bevoegde functionaris**: een Medewerker die vanuit zijn functie door de VU is geautoriseerd om toegang te hebben tot (bepaalde) gegevens die worden verzameld door middel van Logging en/of Monitoring.

c. **College van Bestuur (CvB)**: het College van Bestuur van de VU.

d. **Datalek**: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens, zoals bedoeld in artikel 4.12 van de Algemene verordening gegevensbescherming (AVG).

e. **Functionaris voor Gegevensbescherming (FG)**: een interne functionaris zoals bedoeld in artikel 37 e.v. van de Algemene verordening gegevensbescherming (AVG). De FG houdt op onafhankelijke wijze toezicht op de naleving van wet- en regelgeving met betrekking tot gegevensbescherming en het beleid van de VU met betrekking tot de bescherming van persoonsgegevens.

f. **Gedragscode ICT studenten**: de regels zoals opgenomen in hoofdstuk 3 van dit Reglement.

g. **Gericht Onderzoek**: onderzoek naar een individuele Student of groep van Studenten waarbij gebruik wordt gemaakt van de Verkeersgegevens die de Student(en) betreffen.

h. **ICT-voorzieningen**: alle voorzieningen die de VU gebruikt en ter beschikking stelt in het kader van haar informatie- en communicatieprocessen. Deze voorzieningen kunnen rechtstreeks door de VU of via derden met wie de VU een overeenkomst heeft ter beschikking worden gesteld. Het gaat hierbij onder meer om: netwerken, internet, computers, programma's en applicaties, printers, kopieer- en scanapparatuur, informatiedragers, opslagruimte, e-mail, (mobiele) telefoons en andere communicatiemiddelen.

i. **Inhoudelijk Onderzoek**: onderzoek naar een individuele Student of groep van Studenten waarbij niet alleen gebruik wordt gemaakt van de Verkeersgegevens die de Student(en) betreffen, maar waarbij ook naar de inhoud van bestanden of berichten van individuele Student(en) wordt gekeken.

j. **Logging**: geautomatiseerde vastlegging van Verkeersgegevens.

k. **Medewerker**: degene die een dienstverband heeft met de VU of een persoon die werkzaam is onder het gezag en/of de verantwoordelijkheid van de VU zonder dienstverband (zoals een uitzendkracht, gedetacheerde of ZZP'er).

l. **Monitoring**: het geautomatiseerd verzamelen en analyseren van Verkeersgegevens. Monitoring vindt plaats op basis van algemene parameters en patronen en is niet gericht op individuele Studenten.

m. **Student**: degene die is ingeschreven bij de VU als student of extraneus in de zin van de Wet op het hoger onderwijs en wetenschappelijk onderzoek, een cursist, een contractstudent, een aanmelder die de VU heeft verzocht om inschrijving en een alumnus.

n. **Verkeersgegevens**: alle gegevens die samenhangen met of voortvloeien uit het gebruik van ICT-voorzieningen, die niet de inhoud van bestanden of berichten betreffen. Verkeersgegevens worden in de context van ICT-voorzieningen ook wel 'metadata' genoemd.

Artikel 2. Toepassingsbereik

2.1 Dit Reglement is van toepassing op elk gebruik van de ICT-voorzieningen door Studenten, ongeacht de aard van het gebruik (studie-gerelateerd of privé) en de wijze van gebruik.

2.2 Naast dit Reglement kan de VU bijzondere voorwaarden stellen aan het gebruik van (specifieke) ICT-voorzieningen door (bepaalde) Studenten (hierna: **Bijzondere Voorwaarden**).

Artikel 3. Doelstellingen

3.1 Het doel van dit Reglement is:

a. het bevorderen en handhaven van Acceptabel gebruik van ICT-voorzieningen door Studenten; en

b. het stellen van het normatief kader voor de omgang met gegevens die vastgelegd (kunnen) worden in het kader van het gebruik van ICT-voorzieningen.

HOOFDSTUK 3. GEDRAGSCODE ICT STUDENTEN

Artikel 4. Gedragsregels

4.1 Studenten maken zorgvuldig gebruik van de ICT-voorzieningen en handelen volgens de instructies die de VU hiervoor geeft.

4.2 Studenten houden zich bij het gebruik van de ICT-voorzieningen aan de geldende wet- en regelgeving, dit Reglement en eventuele Bijzondere Voorwaarden.

4.3 Studenten respecteren beveiligingsmaatregelen.

4.4 Studenten voorkomen onjuist of ongeoorloofd gebruik van ICT-voorzieningen en maken op verantwoorde wijze gebruik van ICT-voorzieningen. Waar mogelijk zorgt de VU ervoor dat onjuist en ongeoorloofd gebruik technisch onmogelijk wordt gemaakt.

4.5 Studenten voorkomen dat de rechten en reputatie van de VU worden geschonden.

4.6 Studenten gaan zorgvuldig om met hun inloggegevens en verstrekken deze niet aan anderen.

4.7 Studenten bieden anderen geen toegang tot de ICT-voorzieningen en lenen deze niet uit.

4.8 Studenten respecteren de intellectuele eigendomsrechten van de VU en die van derden.

4.9 Studenten behandelen vertrouwelijke informatie, waaronder persoonsgegevens waar zij in het kader van hun studie toegang toe hebben, strikt vertrouwelijk.

Artikel 5. Ongeoorloofd gebruik

5.1 De volgende handelingen gelden in elk geval als ongeoorloofd gebruik van de ICT-voorzieningen:

a. het verstoren, beschadigen, hinderen, vertragen of anderszins op oneigenlijke wijze beïnvloeden van de beoogde beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-voorzieningen;
b. het bewust verspreiden of bevorderen van verspreiding van virussen, trojans, spyware, malware of andere schadelijke software;
c. het bewust verspreiden of bevorderen van verspreiding van (ongevraagde) berichten voor commerciële doeleinden;
d. het omzeilen van beveiligingsmaatregelen;
e. een onjuiste hoedanigheid of identiteit aannemen;
f. het bewust ter beschikking hebben, stellen of kopiëren van auteursrechtelijk of door een ander intellectueel eigendomsrecht beschermd materiaal zonder toestemming van de rechthebbende(n), waaronder illegale, vervalste of gestolen exemplaren van software;
g. elk gebruik van de ICT-voorzieningen dat ertoe leidt dat anderen gediscrimineerd, (seksueel) geïntimideerd of bedreigd worden;
h. het bewust bezoeken van websites die pornografisch of racistisch dan wel anderszins discriminerend materiaal bevatten of het (laten) plaatsen van dit materiaal op of binnen de ICT-voorzieningen, tenzij dit noodzakelijk is in het kader van de studie van de Student;
i. het bewust opslaan, verspreiden of anderszins verwerken van materiaal waarvan het bezit strafbaar is; en
j. het bewust (laten) lekken van persoonsgegevens of andere vertrouwelijke data van de VU.

Artikel 6. Studie-gerelateerd en privégebruik

6.1 De VU stelt haar ICT-voorzieningen aan Studenten beschikbaar ten behoeve van hun studie aan de VU. De ICT-voorzieningen zijn daarmee primair bedoeld voor studie-gerelateerd gebruik.

6.2 Beperkt privégebruik van ICT-voorzieningen binnen de kaders zoals vastgelegd in dit Reglement is toegestaan, mits:

a. dit binnen de grenzen van de redelijkheid gebeurt;
b. andere Studenten of medewerkers van de VU daardoor niet worden gehinderd;
c. dit geen onevenredige technische of financiële belasting vormt van de ICT-voorzieningen van de VU; en
d. dit niet gebeurt voor commerciële doeleinden.

6.3 Studenten zorgen ervoor dat bestanden en berichten die privé zijn, als ‘privé’ worden gemarkeerd.

Artikel 7. Melding incidenten

7.1 Een Student meldt een incident met betrekking tot de ICT-voorzieningen direct - zonder enige vertraging - bij de IT Servicedesk via servicedesk.it@vu.nl of 020-5980000.

7.2 Onder een incident wordt in elk geval verstaan (een vermoeden van):

a. verlies of diefstal van inloggegevens;
b. verlies of diefstal van ICT-voorzieningen, zoals een computer, tablet of USB-stick;
c. ongeautoriseerde toegang tot ICT-voorzieningen;
d. ongeoorloofde of onopzettelijke vernietiging, openbaarmaking of wijziging van dan wel onbedoelde toegang tot persoonsgegevens of anderszins vertrouwelijke of gevoelige (bedrijfs- of onderzoeks)gegevens;
e. aanwezigheid van schadelijke software, zoals een virus, trojan, spyware, malware; of
f. een phishing-aanval.

HOOFDSTUK 4. LOGGING EN MONITORING

Artikel 8. Logging

8.1 Studenten moeten zich bij het gebruik van ICT-voorzieningen bewust zijn van het feit dat bepaalde gegevens, waaronder persoonsgegevens, vastgelegd kunnen worden. In sommige gevallen is dit een bewuste, gegronde keuze en in andere gevallen is dit een technisch-functionele noodzaak of onvermijdelijkheid.

8.2 De VU zal zich inspannen om zowel het aantal categorieën als de totale hoeveelheid van de gegevens die in het kader van het gebruik van ICT-voorzieningen worden verzameld, te minimaliseren. De verzamelde gegevens worden zoveel mogelijk geanonimiseerd c.q. gepseudonimiseerd.

8.3 De volgende gebeurtenissen worden in ieder geval gelogd:

a. handelingen van Studenten, zoals inlogpogingen, systeemtoegang, e-mailgebruik, toegang tot bestanden en bezoek websites;

b. het gebruik van technische beheerfuncties, zoals het wijzigen van configuratie of instellingen, het uitvoeren van een systeemcommando, starten en stoppen van services, uitvoering van een back-up of restore;

c. gebruik van functies voor functioneel beheer, zoals het wijzigen van configuraties en instellingen, release van nieuwe functionaliteiten, ingrepen in gegevenssets (waaronder databases);

d. handelingen in beveiligingsbeheer, zoals het opvoeren en afvoeren van gebruikers, toekennen en intrekken van rechten en wachtwoordwijzigingen;

e. beveiligingsincidenten, zoals de aanwezigheid van malware, testen op (potentiële) zwakheden, inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet-operationele systeemservices, het starten en stoppen van beveiligingsbeheer; en

f. verstoringen in het dagelijks proces, zoals systeemfouten, afbreken tijdens het uitvoeren van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of -systemen.

8.4 De VU zorgt ervoor dat de gegevens die worden verzameld door middel van Logging goed zijn beschermd. Dit betekent in ieder geval dat:

a. de logfaciliteiten en informatie in logbestanden zijn beschermd tegen inbreuk en onbevoegde toegang;

b. het (automatisch) aanpassen, overschrijven en verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log; en

c. de logbestanden alleen kunnen worden geraadpleegd door Bevoegde functionarissen. De toegang is beperkt tot leesrechten.

Artikel 9. Monitoring

9.1 De VU past Monitoring uitsluitend toe indien dit strikt noodzakelijk is om één of meerdere gerechtvaardigde doelen te bereiken zoals vermeld in artikel 9.2. Indien alternatieven beschikbaar zijn met minder (privacy)risico's, zal de VU de voorkeur geven aan deze alternatieven of uitleggen waarom deze niet toegepast kunnen worden.

9.2 De VU past Monitoring uitsluitend toe voor de volgende doelen:

a. het voorkomen, signaleren en oplossen van capaciteits-, performance- of beschikbaarheids-problemen van de ICT-voorzieningen;

b. controle of de ICT-voorzieningen correct worden gebruikt, goed worden beheerd en naar behoren functioneren;

c. het voorkomen, signaleren en oplossen van beveiligingsincidenten, in het bijzonder een Datalek;

d. het creëren van 'bewijs' (audit trail) ter waarborging van de bedrijfsvoering, naleving van wet- en regelgeving en om intern en extern verantwoording af te kunnen leggen over het gebruik en de beveiliging van de ICT-voorzieningen. Denk bij dit laatste aan de accountantscontrole, externe of interne audits en de informatievoorziening voor toezichthouders zoals de Autoriteit Persoonsgegevens;

e. het verschaffen van managementinformatie met betrekking tot de beschikbaarheid, integriteit, vertrouwelijkheid en kosten van de ICT-voorzieningen;

f. het verbeteren van (de toegankelijkheid tot) de ICT-voorzieningen;

g. wetenschappelijke of statistische doeleinden, voor zover privacywetgeving dit toestaat; en

h. controle op naleving van dit Reglement.

9.3 Indien Monitoring noodzakelijk is en geen redelijke alternatieven beschikbaar zijn, is Monitoring uitsluitend mogelijk met inachtneming van de volgende voorwaarden:

a. de Monitoring vindt zoveel mogelijk systeembreed plaats op basis van algemene parameters en patronen. Er wordt in beginsel géén onderscheid gemaakt per individuele Student; en

b. de Monitoring wordt zoveel mogelijk voorafgaand kenbaar gemaakt in het kader van de informatievoorziening rondom die specifieke ICT-voorziening, bijvoorbeeld via VUnet of via Bijzondere Voorwaarden of andere instructies.

HOOFDSTUK 5. INDIVIDUEEL ONDERZOEK

Artikel 10. Gericht en inhoudelijk onderzoek

10.1 Bij onderzoek naar een individuele Student is Gericht Onderzoek het uitgangspunt. Alleen wanneer duidelijk is dat Gericht Onderzoek ontoereikend is om de vermoede gedraging voldoende te kunnen onderzoeken, kan Inhoudelijk Onderzoek plaatsvinden.

10.2 Gericht onderzoek en Inhoudelijk Onderzoek zijn uitsluitend mogelijk wanneer voldaan wordt aan de volgende voorwaarden:

a. er is sprake van een gerechtvaardigd vermoeden van:

- overtreding van de Gedragscode;

- ongewenst gedrag zoals bedoeld in de regeling Ongewenst Gedrag van de VU; of

- een (andere) ernstig verwijtbare gedraging van een Student;

b. het gericht onderzoek vindt plaats door twee Bevoegde functionarissen (vier-ogenprincipe) onder strikte geheimhouding;

c. een daartoe bevoegde persoon schriftelijk opdracht heeft gegeven tot het onderzoek. In de opdracht wordt vermeld wat het gerechtvaardigd vermoeden is zoals bedoeld in artikel 10.2(a) en indien het Inhoudelijk onderzoek betreft waarom niet met Gericht onderzoek kan worden volstaan. De opdracht wordt gegeven door de decaan van de Faculteit waar de betreffende Student studeert. Het College van Bestuur ontvangt gelijktijdig een afschrift van de betreffende opdracht; en

d. de betreffende Student wordt zo spoedig mogelijk geïnformeerd over de aanleiding, de uitvoering en de resultaten van het onderzoek en in de gelegenheid gesteld om nadere uitleg te geven. Het verstrekken van informatie aan de Student kan worden uitgesteld indien het onderzoek daardoor zou kunnen worden geschaad.

10.3 Voor Inhoudelijk Onderzoek gelden de volgende aanvullende regels:

a. bestanden en berichten die als ‘privé’ gemarkeerd zijn worden buiten beschouwing gelaten, tenzij een gerechtvaardigd vermoeden bestaat dat zij informatie bevatten over de (vermoede) ongewenste gedraging van de Student;

b. geprivilegieerde informatie die betrekking heeft op de Student - waaronder communicatie met een studieadviseur, studentenpsycholoog, Ombudsman, vertrouwenspersoon en een advocaat worden buiten beschouwing gelaten, tenzij (het gerechtvaardigde vermoeden van) de ongewenste gedraging van de Student direct betrekking heeft op het contact met één of meer van de hiervoor bedoelde personen en instanties.

10.4 Het gerechtvaardigd vermoeden zoals bedoeld in artikel 10.2(a) kan gebaseerd zijn op de resultaten van Monitoring, Logging, eigen waarneming van de VU en/of een melding door een derde.

10.5 De verzamelde gegevens en resultaten van het Gericht Onderzoek en/of Inhoudelijk Onderzoek zijn uitsluitend - onder strikte geheimhouding - toegankelijk voor de decaan van de Faculteit waar de betreffende Student studeert, het College van Bestuur, de leden en de ambtelijk secretaris van de klachtencommissie zoals bedoeld in de regeling Ongewenst Gedrag voor zover het onderzoek is verricht op verzoek van deze commissie, en eventueel de ter ondersteuning betrokken (onderwijs)jurist.

10.6 De resultaten van Gericht onderzoek en/of Inhoudelijk onderzoek worden onmiddellijk vernietigd indien het vermoeden van overtreding van de Gedragscode en/of een ernstige verwijtbare gedraging onterecht blijkt. Zodra geen noodzaak meer bestaat om de resultaten te bewaren, worden deze vernietigd. De resultaten van Gericht onderzoek en/of Inhoudelijk onderzoek kunnen (langer) worden bewaard indien noodzakelijk voor bepaalde bewijsvoering in rechte of in het belang van een strafrechtelijk onderzoek of aangifte.

Artikel 11. Bezwaar onderzoek

11.1 De Student die onderwerp is van Gericht onderzoek en/of Inhoudelijk onderzoek, zoals bedoeld in artikel 10, kan daartegen schriftelijk en gemotiveerd bezwaar aantekenen bij het College van Bestuur binnen vier weken nadat hij is ingelicht over het onderzoek.

11.2 Het College van Bestuur neemt zo spoedig mogelijk en in ieder geval binnen vier weken na ontvangst van het bezwaar een schriftelijk en met redenen omkleed besluit. Indien het bezwaar gegrond wordt verklaard, wordt lopend onderzoek per direct gestaakt en worden de door middel van Gericht onderzoek en/of Inhoudelijk onderzoek verkregen gegevens terstond vernietigd. Daarnaast worden eventuele maatregelen ingetrokken indien deze ten onrechte zijn genomen.

11.3 Het aantekenen van bezwaar laat onverlet dat de VU maatregelen kan treffen zoals bedoeld in artikel 12.

Artikel 12. Maatregelen

12.1 De VU behoudt zich het recht voor om Studenten die in strijd handelen of hebben gehandeld met de Gedragscode de toegang tot bepaalde ICT-voorzieningen te ontzeggen of deze te beperken.

12.2 Wanneer blijkt dat een Student in strijd heeft gehandeld met de Gedragscode kan het College van Bestuur afhankelijk van de aard en ernst van de overtreding jegens hem passende maatregelen treffen, waarbij het definitief beëindigen van de inschrijving de meest vergaande maatregel is.

12.3 Indien sprake is van (een gerechtvaardigd vermoeden van) een strafbaar feit, kan de VU aangifte doen.

Artikel 13. Rapportage Universitaire Studentenraad

13.1 Het CvB rapporteert jaarlijks aan de Universitaire Studentenraad over het aantal individuele onderzoeken dat in een bepaald jaar heeft plaatsgevonden en de algemene uitkomsten hiervan. Hierbij zullen geen tot personen herleidbare gegevens worden gedeeld.

HOOFDSTUK 6. GEBRUIK VERKEERSGEGEVENS EN BEWAARTERMIJN

Artikel 14. Gebruik Verkeersgegevens

14.1 De VU gebruikt Verkeersgegevens die betrekking hebben op Studenten alleen overeenkomstig dit Reglement.

14.2 De VU gebruikt Verkeersgegevens voor:

a. Logging zoals beschreven in artikel 8;

b. Monitoring zoals beschreven in artikel 9;

c. individueel onderzoek zoals beschreven in hoofdstuk 5; en

d. het volgen van werk- of leerprocessen.

Artikel 15. Bewaartermijnen

15.1 De gegevens die worden verzameld en verwerkt in het kader van Logging en Monitoring worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor deze zijn verzameld en (verder) worden verwerkt.

15.2 De VU houdt zich aan de wettelijke bewaartermijnen die gelden voor persoonsgegevens en andere gegevens. Voor zover geen sprake is van een wettelijke bewaartermijn, heeft de VU bewaartermijnen vastgesteld.

HOOFDSTUK 7. SLOTBEPALINGEN

Artikel 16. Toezicht

16.1 De Functionaris Gegevensbescherming (FG) van de VU is belast met het toezicht op de naleving van dit Reglement. De FG van de VU wordt door de VU in staat gesteld zijn toezichthoudende taak onafhankelijk en naar behoren uit te oefenen. Dit betekent dat hij wat betreft de uitoefening van zijn functie geen aanwijzingen kan ontvangen van (het CvB van) de VU en dat hij geen nadeel ondervindt van de uitoefening van zijn functie. De FG van de VU heeft een adviserende rol ten opzichte van het CvB.

16.2 Alle Studenten zijn verplicht aan de FG alle medewerking te verlenen die de FG redelijkerwijs bij de uitoefening van zijn bevoegdheden kan vragen.

Artikel 17. Slotbepalingen

17.1 In gevallen waarin dit Reglement niet voorziet beslist het College van Bestuur.

17.2 Dit Reglement is aangeboden aan de Universitaire Studentenraad van de VU ter advisering.

17.3 Dit Reglement wordt gepubliceerd op de website van de VU en intranet (VUnet).

17.4 Dit Reglement is vastgesteld door het CvB en is in werking getreden op 1 september 2019.

17.5 De toepassing van dit Reglement wordt twee jaar na de inwerkingtreding ervan geëvalueerd en besproken met de Universitaire Studentenraad.