Reglement omgang met ICT-voorzieningen en (persoons)gegevens door studenten Hogeschool Leiden

Dit reglement is op 14 oktober 2019 vastgesteld door het College van Bestuur van Hogeschool Leiden, nadat de Studentenraad op 8 oktober 2019 zijn instemming heeft verleend.

Inhoud

Toelichting 3
Hoofdstuk 1 Algemene bepalingen 4
Artikel 1 Begrippen 4
Artikel 2 Reikwijdte 5
Artikel 3 Doeleinden 5
Artikel 4 Rechten van medewerkers 6
Hoofdstuk 2 Gebruiks- en gedragsregels voor medewerkers 7
Artikel 5 (Persoons)gegevens 7
Artikel 6 E-mail en andere ICT-communicatiemiddelen 7
Artikel 7 ICT-middelen, applicaties en account 8
Artikel 8 Internet 9
Hoofdstuk 3 ICT-beheersmaatregelen en controle 11
Artikel 10 Algemene bepalingen 11
Artikel 11 Registreren van ICT-, e-mail- en internetgebruik (logging) 11
Artikel 12 Controleren van ICT-, e-mail- en internetgebruik (monitoring) 11
Artikel 13 Gericht onderzoek naar overtreding van dit reglement 12
Artikel 14 Maatregelen in geval van andere bijzondere situaties 13
Hoofdstuk 4 Overtreding van dit reglement 14
Artikel 15 Consequenties van overtreding 14
Hoofdstuk 5 Slotbepaling 15
Artikel 16 Slotbepalingen 15

Toelichting

Het verwerken van (persoons)gegevens en het gebruik van ICT-voorzieningen (zoals openbare computers, draadloze en bedrade netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen) worden aan de student beschikbaar gesteld ten behoeve van de studie.

Met dit reglement wil Hogeschool Leiden, hierna te noemen “de hogeschool”, regels stellen omtrent het aanvaardbaar en gewenst gebruik van ICT-voorzieningen en het gebruik van (persoons)gegevens. Het streven daarbij is een goede balans aan te brengen tussen verantwoord, veilig en werkbaar gebruik van ICT-voorzieningen en (persoons)gegevens en de privacy en veiligheid van de medewerkers en studenten.

Tegenwoordig communiceren medewerkers, studenten en de organisatie ook met elkaar en met derden via de sociale media en andere (openbare) communicatiekanalen waarover de hogeschool geen controle heeft. De gedragsregels in dit reglement op het gebied van de beschikbaarheid (continuïteit), de integriteit (betrouwbaarheid) en de vertrouwelijkheid (exclusiviteit) van gegevens gelden ook voor die kanalen voor zover de gegevens betrekking hebben op de hogeschool.

Om inzicht te krijgen in het technische gebruik van ICT-voorzieningen en om proactief op foutmeldingen in te kunnen gaan is registratie van gebruik in logbestanden essentieel en belangrijk voor het optimaliseren van onze ICT-voorzieningen. Bij zwaarwegende vermoedens van overtreding van dit reglement kunnen gelogde (persoons)gegevens gebruikt worden bij een onderzoek dat is gericht op een specifiek persoon. Betrokkenen dienen hierover goed geïnformeerd te worden. In dit reglement is daarom tevens beschreven op welke wijze en volgens welke procedures het verzamelen van gegevens van studenten, de controle op naleving en gericht onderzoek plaatsvindt.

Hogeschool Leiden is een goed georganiseerde hogeschool en houdt zich aan wet- en regelgeving. Naast de wet- en regelgeving is dit document gebaseerd op het Beleid verwerking persoonsgegevens, de Huisregels en de Regeling klachtenprocedure ongewenst gedrag,

Bronvermelding:

Dit reglement voor studenten van Hogeschool Leiden is gebaseerd op het Model reglement voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo.

Hoofdstuk 1 Algemene bepalingen

Artikel 1 Begrippen

- **Account**: hogeschool-account dat aan iedere student wordt verstrekt bij (een verzoek tot) inschrijving;
- **Applicatie**: computerprogramma of software, al dan niet aangeboden als clouddienst;
- **Beheerorganisatie:** is de term voor de functionarissen die bevoegd zijn ICT-voorzieningen te beheren en om logging, monitoring en eventueel tracking uit te voeren. In de praktijk zal dit per implementatie verschillen en o.a. belegd zijn bij functioneel beheer, technisch beheer of een specifiek aangewezen functionaris binnen een faculteit of dienst. Aan de hand van de richtlijn die het toegangsbeleid beschrijft, is vastgesteld wie per applicatie geautoriseerd is;
- **Primaire bedrijfsprocessen**: de activiteiten van de hogeschool op het gebied van onderwijs en onderzoek;
- **Crisis**: een situatie waarin (a) de veiligheid, gezondheid en/of het welzijn van studenten, medewerkers en/of bezoekers van Hogeschool Leiden geschaad wordt, of (b) gebouwen, infrastructuur of belangen van Hogeschool Leiden worden aangetast, of (c) er verstoring van het primaire onderwijsproces ontstaat, of (d) strategische belangen van de organisatie worden aangetast. In een dergelijke gevallen voldoen de bestaande normale hiërarchische besluitvormingsstructuur, procedures en protocollen niet voor het beheersen en bestrijden van de situatie;
- **Datalek**: een inbreuk in verband met persoonsgegevens die een risico inhoudt voor de rechten en vrijheden van degene wiens persoonsgegevens het betreft;
- **Diagnostische gegevens**: geregistreerde gegevens van activiteiten van gebruikers en systemen en van gebeurtenissen in ICT-voorzieningen;
- **ICT-communicatiemiddel**: alle middelen die de hogeschool beschikbaar stelt waarmee berichten kunnen worden verstuurd naar ontvangers binnen en buiten de hogeschool;
- **ICT-middel**: hardware die de hogeschool beschikbaar stelt, zoals computer, laptop en netwerkfaciliteiten. Privé-apparatuur valt in dit reglement niet onder deze definitie;
- **ICT-voorziening**: ICT-middelen, applicaties en ICT-communicatiemiddelen;
- **Logging**: het registreren van activiteiten of gebeurtenissen van gebruikers en systemen die plaats vinden in ICT-voorzieningen om het vervolgens op te slaan;
- **Monitoring**: het periodiek controleren en beoordelen van de diagnostische gegevens op de aanwezigheid van ongewenste gebeurtenissen en ongebruikelijke situaties zoals overtredingen van hogeschool beleid of dreigingen die de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens of systemen beïnvloeden;

- **Persoonsgegeven**: informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals bedoeld in artikel 4 lid 1 van de Algemene Verordening Gegevensbescherming;
- **Sociale media**: online platformen waarbij gebruikers, al dan niet met tussenkomst van een redactie, tekst en/of (audiovisueel) beeld publiceren, kennis, meningen en ervaringen uitwisselen en de dialoog met elkaar aangaan;
- **Vertrouwelijke informatie**: informatie waarvan de student de vertrouwelijkheid kent of behoort te kennen.

Artikel 2 Reikwijdte

2.1 Dit reglement stelt regels ten aanzien van verwerking van (persoons)gegevens en het gebruik van ICT-voorzieningen door studenten van Hogeschool Leiden.

2.2 Dit reglement informeert op welke wijze en volgens welke procedures geautomatiseerde verzameling van gegevens, de controle op naleving van dit reglement en gericht onderzoek naar individuele studenten plaatsvindt.

2.3 Tot studenten van Hogeschool Leiden worden in het kader van dit reglement gerekend:

- Student of aspirant student: degene die voor een opleiding als student als bedoeld in artikel 7.32 van de WHW bij Hogeschool Leiden is ingeschreven; in dit reglement wordt degene die zich als student wil inschrijven ook als student aangeduid;
- Extraneus: degene die door de instelling is ingeschreven als extraneus als bedoeld in de artikelen 7.32 en 7.36 van de WHW voor een opleiding die voltijds of deeltijds is ingericht;
- Cursist: degene die anders dan student of extraneus bij Hogeschool Leiden is ingeschreven en deelneemt aan het onderwijs.

Artikel 3 Doeleinden

Met dit reglement worden de volgende doeleinden beoogd:

- beveiliging van ICT-voorzieningen, inclusief beveiliging tegen schade en misbruik;
- voorkomen dat de ICT-voorzieningen worden misbruikt voor seksuele intimidatie, discriminatie en ander ongewenst gedrag;
- bescherming van de (persoons)gegevens van onze medewerkers, studenten en derden;
- bescherming van vertrouwelijke informatie van de hogeschool, haar medewerkers, studenten en derden;
- bescherming van de intellectuele eigendomsrechten van de hogeschool en derden;
- voorkomen van het al dan niet moedwillig verspreiden van foutieve en/of niet-actuele gegevens en informatie;
- beheersing van beschikbaarheid, capaciteit en kosten van de ICT-voorzieningen van de hogeschool.

Artikel 4 Rechten van studenten

4.1 Informatie over de rechten van studenten met betrekking tot de verwerking van hun persoonsgegevens door de hogeschool is te vinden in het Privacy Statement Studenten op de website van de hogeschool.

4.2 Studenten kunnen ten aanzien van de verwerking van hun persoonsgegevens een verzoek indienen bij de Functionaris Gegevensbescherming van de hogeschool. Verzoeken worden conform de procedure "Behandeling verzoeken betreffende rechten van betrokkenen" afgehandeld.

Hoofdstuk 2 Gebruiks- en gedragsregels voor studenten

Artikel 5 (Persoons)gegevens en vertrouwelijke informatie

5.1 Indien de student in het kader van zijn studie of het uitvoeren van taken voor de hogeschool toegang krijgt tot vertrouwelijke informatie en persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen en adequate maatregelen (zie ook artikel 5.3) te treffen om de vertrouwelijkheid te waarborgen.

5.2 De student maakt geen inbreuk op de intellectuele eigendomsrechten van de hogeschool en derden en conformeert zich aan de licentievoorwaarden die van toepassing zijn op de applicaties van de hogeschool. Dit betekent onder andere dat het de student is verboden om onderwijsmateriaal van de hogeschool (zoals readers, modulehandleidingen, presentaties, tentamenvragen etc.) al dan niet tegen een vergoeding aan derden beschikbaar te stellen.

5.3 De student treft in de situatie als bedoeld in artikel 5.1 adequate maatregelen om een datalek te voorkomen. Onder adequate maatregelen worden in ieder geval de volgende maatregelen verstaan:

a. Vertrouwelijke informatie en (persoons)gegevens worden alleen opgeslagen, bewaard en verwerkt in de systemen van de hogeschool.
b. Het buiten de hogeschool verwerken van vertrouwelijke informatie en (persoons)gegevens, zoals het versturen van informatie naar externe e-mailadressen, het gebruik van cloud-toepassingen (bijvoorbeeld Google-drive, WeTransfer, Dropbox) die niet onder controle staan van de hogeschool of het opslaan van gegevens op externe opslagmedia of eigen apparatuur (USB-sticks, externe harddisks, tablets, etc.), is niet toegestaan.

5.4 De student leeft de voorschriften die de hogeschool met betrekking tot het waarborgen van de vertrouwelijkheid heeft opgesteld, waaronder de regels in dit reglement, strikt na.

Artikel 6 E-mail en andere ICT-communicatiemiddelen

6.1 De hogeschool biedt studenten generieke ICT-communicatiemiddelen waaronder internettoegang, een account, Office365 applicaties, een e-mailsysteem met bijbehorende mailbox en e-mailadres.

6.2 Verboden bij elk gebruik van ICT-communicatiemiddelen is:

- het verzenden of plaatsen van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende, (seksueel) intimiderende of anderszins aanstootgevende inhoud;
- het versturen of plaatsen van ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven te versturen of kwaadaardige software zoals virussen, Trojaanse paarden of spyware te versturen.

6.3 De student heeft als enige toegang tot zijn eigen hogeschool-mailbox. De enige uitzondering hierop staat in Hoofdstuk 3 van dit Reglement omschreven.

6.4 Voor het gebruik van e-mail in de situatie als bedoeld in artikel 5.1 gelden de volgende regels:

a. De student verstuurt geen e-mails met daarin vertrouwelijke informatie of persoonsgegevens, maar maakt hiervoor gebruik van andere -veiliger- manieren om dergelijke informatie te delen, zoals een persoonlijk gesprek.
b. De student verwijst in de e-mail waar mogelijk naar de (bron)systemen waar de ontvanger de betreffende vertrouwelijke informatie of persoonsgegevens zelf kan vinden. Hiermee wordt voorkomen dat onnodig kopieën van vertrouwelijke informatie of persoonsgegevens in de organisatie terecht komen en bewaard blijven.
c. Indien de opties uit sub a en b niet volstaan neemt de student de informatie niet op in de e-mail of in bijlagen maar deelt een beveiligd bestand met daarin de vertrouwelijke informatie of persoonsgegevens met de ontvanger.
d. De student controleert altijd de link van het gedeelde bestand en het e-mailadres van de geadresseerde voor het versturen van de e-mail. Hiermee wordt voorkomen dat -per abuis- de verkeerde informatie met de verkeerde persoon wordt gedeeld.
e. De student gebruikt bcc (blind carbon copy=verborgen adressen) als een groep aangeschreven wordt van externe personen die elkaars gegevens mogelijkerwijs niet hebben of niet nodig hebben;
f. De student gebruikt de e-mailapplicatie niet om vertrouwelijke informatie of persoonsgegevens te bewaren en verwijdert daarom regelmatig de betreffende e-mails.

Artikel 7 ICT-middelen, applicaties en account

7.1 Computer- en netwerkfaciliteiten (ICT-middelen) zijn voor de student beschikbaar ten behoeve van de studie. Beperkt privégebruik van ICT-middelen is toegestaan, mits dit niet storend is voor de goede orde of de ICT-middelen van de hogeschool. Studenten dienen te allen tijde zorgvuldig om te gaan met de verstrekte ICT-Middelen.

7.2 Het aansluiten van eigen apparatuur zoals, laptops, tablets en telefoons op het netwerk is alleen toegestaan op de daarvoor beschikbaar gestelde (draadloze) netwerkaansluitingen. De beheerorganisatie kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging. Het aansluiten van servers en netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van de Beheerorganisatie. Neem hiervoor altijd contact op met de Servicedesk.

7.3 De bepalingen in dit reglement gelden onverkort voor studenten die in hun woonruimte gebruik maken van een netwerkfaciliteit van de hogeschool. Er worden geen extra beperkingen opgelegd aan het gebruik, behoudens voor zover noodzakelijk om de integriteit en de veiligheid van het netwerk te kunnen bewaren, of om (de snelheid van) het netwerkverkeer te waarborgen. Indien de beheerorganisatie ingrijpt, zullen gelijke soorten netwerkverkeer gelijk worden behandeld.

7.4 Het opslaan van privébestanden of -informatie op de persoonlijke opslaglocatie van de hogeschool is toegestaan, mits dit niet leidt tot overbelasting van de ICT-voorzieningen of de goede orde op de werkvloer verstoort. Bovendien mag de inhoud van de bestanden en informatie niet in strijd zijn met wet- en regelgeving.
De hogeschool is niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen. Het gebruiken van de persoonlijke opslaglocatie van de hogeschool voor privédoeleinden geschiedt dan ook op eigen risico.

7.5 De hogeschool kan voor onderwijsprocessen systemen of applicaties voorschrijven, zoals een Digitale Leer- en Werkomgeving (DLWO), een e-mailsysteem, (mobiele) applicaties, apps, cloud-voorzieningen of multimediadiensten. De faculteit of opleiding kan aanvullende voorwaarden stellen voor het gebruik van systemen of applicaties.

7.6 Het zelfstandig installeren van software op de computer- en netwerkfaciliteiten van de hogeschool is niet toegestaan als de Beheerorganisatie beperkingen heeft ingesteld, die installatie tegenhouden.

7.7 Het omzeilen van beveiligingsvoorzieningen op ICT-voorzieningen van de hogeschool is niet toegestaan.

7.8 De student dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende hogeschoolaccount, inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals One-Time-Passwords of sms authenticatie). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld.

7.9 Het gebruik van ICT-middelen door de student ten behoeve van commerciële activiteiten is uitsluitend toegestaan wanneer de hogeschool hiervoor schriftelijk toestemming heeft verleend.

Artikel 8 Internet

8.1 De toegang tot internet en bijbehorende faciliteiten worden aan de student beschikbaar gesteld ten behoeve van de studie. Beperkt privégebruik van

internet is toegestaan, mits dit niet storend is voor de goede orde bij de hogeschool of de ICT-middelen van de hogeschool.

8.2 Verboden bij elk internetgebruik is echter:

- sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- filesharing- of streamingdiensten te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de ICT-voorzieningen in gevaar kan brengen;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de student daadwerkelijk weet dat dit in strijd met auteursrechten is;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

Hoofdstuk 3 ICT-beheersmaatregelen en controle

Artikel 10 Algemene bepalingen

10.1 De Beheerorganisatie verschaft zich slechts toegang tot het account of de ICT-middelen van een student, als de student daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in uitzonderlijke gevallen en volgens de procedures zoals beschreven in dit hoofdstuk.

10.2 Het geautomatiseerd verzamelen van gegevens over, controle op en gericht onderzoek naar gebruik van de ICT-voorzieningen en internetgebruik vindt slechts plaats in het kader van handhaving van de regels uit dit reglement voor de doelen genoemd in artikel 3. Verboden of ongewenst gebruik wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Artikel 11 Registreren van ICT-, e-mail- en internetgebruik (logging)

11.1 Ten behoeve van een goed en efficiënt beheer van de ICT-voorzieningen van de hogeschool worden gegevens waar mogelijk geautomatiseerd verzameld (gelogd), te weten:

- Datum, tijdstip
- gebruikersnaam/identificatie
- werkstation/locatie informatie
- activiteit/gebeurtenis
- het object waarop de activiteit werd uitgevoerd
- indien relevant, het resultaat van de activiteit

11.2 Deze gelogde gegevens zijn toegankelijk voor de Beheerorganisatie. De gelogde gegevens worden alleen aan andere functionarissen beschikbaar gesteld op basis van de richtlijn die het toegangsbeleid bepaalt.

11.3 De gelogde gegevens blijven maximaal 6 maanden bewaard en worden daarna vernietigd. Bij incidenten worden gelogde gegevens zo lang bewaard als noodzakelijk voor het afhandelen van het incident + 1 jaar om eventuele controlerende of corrigerende analyses te kunnen doen.

Artikel 12 Controleren van ICT-, e-mail- en internetgebruik (monitoring)

12.1 Met monitoring wordt bedoeld het periodiek controleren en beoordelen van de diagnostische gegevens op de aanwezigheid van ongewenste gebeurtenissen en ongebruikelijke situaties zoals overtredingen van hogeschoolbeleid of dreigingen die de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens of systemen beïnvloeden. De uitkomst van de beoordeling wordt omgezet in een signalering voor de Beheerorganisatie en mogelijk in rapportage aan relevante functionarissen.

12.2 Naar aanleiding van een signalering kan de Beheerorganisatie preventieve maatregelen op de ICT voorzieningen nemen om de dreigingen weg te nemen.

12.3 Bij een vermoeden van misbruik van een wachtwoord, account en/of inloggegevens heeft de hogeschool de mogelijkheid om per direct het betrokken account ontoegankelijk maken.

12.4 Op basis van de uitkomsten van de monitoring kan een gericht onderzoek worden gestart naar naleving van de regels van dit reglement als bedoeld in artikel 13.1.

Artikel 13 Gericht onderzoek naar overtreding van dit reglement

13.1 Van gericht onderzoek is sprake wanneer diagnostische gegevens of persoonsgegevens betreffende een specifieke student worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die student.

13.2 Gericht onderzoek door de Beheerorganisatie vindt uitsluitend plaats na schriftelijke opdracht van de faculteitsdirecteur onder wiens verantwoordelijkheid de student valt. Het College van Bestuur ontvangt een afschrift van deze opdracht en de schriftelijke resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen worden de opdracht en de resultaten direct vernietigd door de Beheerorganisatie.

13.3 Gericht onderzoek beperkt zich in eerste instantie tot diagnostische gegevens van het gebruik van ICT-voorzieningen. Als gericht onderzoek nader bewijs van overtreding van dit reglement oplevert, kan de Beheerorganisatie met toestemming van de opdrachtgevende directeur zoals bedoeld in 13.2 en het College van Bestuur overgaan tot het kennisnemen van de inhoud van berichten of opgeslagen bestanden indien dit noodzakelijk is voor het onderzoek. Alleen gegevens die duidelijk gemarkeerd zijn als ‘vertrouwelijk’ zullen door de hogeschool als zodanig behandeld worden.

13.4 De student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur van zijn faculteit over de aanleiding, de uitvoering en het resultaat van het onderzoek. De student wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens (hoor en wederhoor). Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

13.5 Voor gericht onderzoek wordt uitgegaan van een meer-ogen principe bij het uitvoeren van het onderzoek. Hierbij zijn dus altijd meerdere personen betrokken.

Artikel 14 Maatregelen in geval van andere bijzondere situaties

14.1 Naast de in dit hoofdstuk genoemde maatregelen met betrekking tot beheer, controle en gericht onderzoek, verschaft de Beheerorganisatie zich alleen in de volgende bijzondere situatie en volgens de in dit artikel beschreven procedure toegang tot het account of de ICT-middelen van een student.

14.2 In geval van een mogelijke crisis kan het College van Bestuur of het crisisteam toestemming verlenen aan de Beheerorganisatie om zich toegang te verschaffen tot het account (zoals e-mails en bestanden) van een of meerdere studenten, indien dit noodzakelijk is voor waarborging van de continuïteit en kwaliteit van de primaire bedrijfsprocessen van de hogeschool. Vertrouwelijke bestanden worden niet gelezen als deze als zodanig gemarkeerd zijn.

14.3 De student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur van zijn faculteit over de maatregelen die zijn of worden genomen op basis van dit hoofdstuk.

14.4 Voor het uitvoeren van maatregelen in bijzondere situaties wordt altijd uitgegaan van een meer-ogen principe bij het uitvoeren van het onderzoek. Hierbij zijn dus altijd meerdere personen betrokken.

Hoofdstuk 4 Overtreding van dit reglement

Artikel 15 Consequenties van overtreding

Wanneer handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels wordt geconstateerd, kan het College van Bestuur en/of de verantwoordelijk directeur afhankelijk van de aard en de ernst van de overtreding passende maatregelen treffen.

Hoofdstuk 5 Slotbepaling

Artikel 16 Slotbepalingen

16.1 Dit Reglement wordt iedere twee jaar onder leiding van de afdeling Informatiemanagement geëvalueerd en waar nodig herzien.

16.2 Dit Reglement kan met instemming van de Studentenraad tussentijds worden gewijzigd als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de studenten en Studentenraad bekend gemaakt.

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