Regeling Computer- en Netwerkgebruik TU/e

DATUM
01-01-2023

TU/e
EINDHOVEN UNIVERSITY OF TECHNOLOGY

Reglement computer- en netwerkgebruik TU/e

Samenvatting

Studenten en werknemers gebruiken vrijwel dagelijks een computer en internet voor hun studie en werk. De TU/e wil dit graag faciliteren door goede ICT-faciliteiten en -voorzieningen ter beschikking te stellen. Hieraan zijn echter ook risico's van oneigenlijk gebruik verbonden. Daarom zijn voor het gebruik van de TU/e ICT-faciliteiten en -voorzieningen gedragsregels nodig.

De TU/e heeft deze gedragsregels vastgelegd in een 'reglement computergebruik en netwerkgebruik'. Hierin staat omschreven hoe je als gebruiker (student of werknemer van de TU/e of derde) de beschikbare ICT-faciliteiten en -voorzieningen mag gebruiken, hoe de aansprakelijkheid geregeld is en welke maatregelen de TU/e neemt als er sprake is van misbruik van de ICT-faciliteiten en -voorzieningen.

Basisregels

In het genoemde reglement zijn de voorwaarden en procedures rondom het gebruik van de ICT-faciliteiten en -voorzieningen tot in detail vastgelegd. Met gezond verstand en het naleven van een aantal 'basisregels' kom je echter een heel eind. We zetten de belangrijkste spelregels op een rij:

1. Je mag de geboden ICT-faciliteiten en -voorzieningen van de TU/e (in beperkte mate) voor privédoeleinden gebruiken. Het spreekt voor zich dat je ervoor zorgt dat dit je normale werkzaamheden (en die van anderen) niet belemmert, en dat je de fatsoens- en wettelijke normen die normaal gesproken gelden, ook hanteert bij het gebruik van de ICT-faciliteiten en -voorzieningen van de TU/e.
2. Let erop dat je activiteiten de ICT-faciliteiten en -voorzieningen niet te zwaar belasten. Verstuur bijvoorbeeld geen grote hoeveelheden berichten of berichten van zo'n grote omvang dat ze het systeem kunnen vertragen.
3. Gebruik je gebruikersnaam, wachtwoord en e-mailadres alleen persoonlijk, geef deze gegevens niet aan iemand anders. Let er ook op dat je een computer waarop je ingelogd bent niet onbeheerd achterlaat. Bij misbruik van je account ben je zelf aansprakelijk.
4. Let erop dat boodschappen die je verstuurt niet kwetsend, beledigend, discriminerend, of op een andere wijze ongepast of onrechtmatig zijn.
5. Vanzelfsprekend gebruik je de ICT-faciliteiten en -voorzieningen niet voor illegale activiteiten, zoals hacken, kraken van beveiligingscodes, het plegen van fraude en het illegaal downloaden of kopiëren van files.
6. Natuurlijk verstuur je geen kettingbrieven, reclameboodschappen of andere 'spam' berichten.
7. Laat de systeeminstelling van de voorzieningen van de TU/e intact en ga zorgvuldig met de geboden voorzieningen om.
8. Je mag de hardware en de software die de TU/e je ter beschikking stelt niet gebruiken voor reclame-uitingen en voor commerciële doeleinden en je mag ze niet aan derden ter beschikking stellen. Als je dat toch doet en aan de TU/e wordt een boete opgelegd dan zal deze boete aan jou doorberekend worden.
9. Als je privéapparatuur gebruikt voor werk- of studiegerelateerde activiteiten, dan ben je gehouden aan het Mobile device and Teleworking beleid van de TU/e. Deze kun je vinden op het intranet.

Procedures en maatregelen

Als onjuist gebruik van de computer- en netwerkvoorzieningen van de TU/e wordt vermoed, kan de TU/e stappen hiertegen ondernemen. Zo is de TU/e onder bepaalde omstandigheden verplicht om gegevens en/of bestanden van een computer ter beschikking te stellen als de autoriteiten met een wettelijke basis hierom

vragen. Ook kan de TU/e een onderzoek instellen als zij onrechtmatig gebruik van de gebruikersnaam, wachtwoord of gegevens vermoedt. Als student of werknemer van de TU/e ben je verplicht om aan een dergelijk onderzoek mee te werken. Uiteraard houdt de TU/e zich daarbij aan de regels zoals die zijn omschreven in de Algemene Verordening Gegevensbescherming.

Mocht er inderdaad sprake zijn van onrechtmatig gebruik van de ICT-faciliteiten of -voorzieningen van de TU/e, dan is de TU/e genoodzaakt vervolgstappen te nemen. Meldingen over misbruik lopen zoals beschreven in dit reglement. Sancties lopen, afhankelijk van de ernst van de overtreding, uiteen.

Meer informatie

Hieronder vind je de volledige regeling computer- en netwerkgebruik.

Regeling computer- en netwerkgebruik TU/e

Het College van Bestuur van de Technische Universiteit Eindhoven (TU/e), gelet op artikel 7.57h van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW), gelet op de regeling Universitaire gebouwen, terreinen en andere Voorzieningen,

BESLUIT in te trekken:

- Het reglement computer- en netwerkgebruik TU/e 2012;

VAST TE STELLEN:

- Het reglement computer- en netwerkgebruik TU/e 2022, luidende als volgt:

Artikel 1 Begripsomschrijvingen

In deze regeling wordt verstaan onder:

Beheerder:	De directeur bedrijfsvoering resp. het hoofd van de beheerseenheid door het College van Bestuur belast met het beheers mandaat voor de betreffende eenheid.
Bevoegd gezag:	Het College van Bestuur van de TU/e is het bevoegd gezag. Het College van Bestuur kan middels mandatering het faculteitsbestuur, de beheerder of enige andere als Bevoegd Gezag aanwijzen.
CERT:	Computer Emergency Response Team
CGC:	Commissie Gedragscode Computergebruik.
Derde:	Gebruiker die te gast is bij de TU/e of een tijdelijke medewerker, zoals uitzendkracht, stagiaire en ingehuurd personeel.
ESA:	Education and Student Affairs van de TU/e.
Gebruiker:	De natuurlijke persoon die van de ICT-faciliteiten en -voorzieningen gebruik maakt met instemming van het Bevoegd Gezag, welke instemming blijkt uit door het Bevoegd Gezag verstrekte gebruikersnaam, emailadres en/of andere toegangscode of door acceptatie van de gebruiksvoorwaarden in het geval van het gastennetwerk (wifi).
ICT-faciliteiten:	De door of namens de TU/e ter beschikking gestelde computer- en netwerkfaciliteiten, waaronder elektronische apparatuur, zoals (desktop-)computers, laptops, notebooks, tablets, mobiele telefoons en printers, , en software, (licenties) zoals programmatuur, computerbesturingssystemen en andere computer- en/of netwerkfaciliteiten, zoals het fysieke en wifi netwerk (het beveiligde netwerk en het gastennetwerk).
ICT-voorzieningen:	De door of namens de TU/e ter beschikking gestelde mogelijkheden voor elektronische informatie-uitwisseling, waaronder doch niet beperkt tot (toegang tot) internet, intranet, e-mail, bibliotheek informatiesystemen, , sociale media accounts en/of chatgroepen en alle andere elektronische mogelijkheden die al dan niet met een toegangscode of via een link toegankelijk zijn, alsmede aansluitmogelijkheden ten behoeve van elektronische apparatuur.
LIS:	Library & Information Services van de TU/e.

Melding:	Schriftelijk (waaronder elektronisch) ingediende mededeling over onjuist of onrechtmatig gebruik van de ICT-faciliteiten en -voorzieningen door een gebruiker.
Misbruik:	Gebruik van de ICT-faciliteiten en -voorzieningen in strijd met het Reglement en/of een ter zake doende (ongeschreven) rechtsregel ongeacht of dit in lichte of zware vorm is als bedoeld in Bijlage 1 bij het Reglement.
Opleidingsdirecteur:	De functionaris die door het College van Bestuur is aangewezen als zijnde belast met de uitvoering van het Reglement voor de studenten van de betreffende opleiding.
OST	Operational Security Team
Secretaris CGC:	De directeur van LIS of de door hem/haar gemandateerde tevens qualitate qua secretaris van de CGC.
Sociale media	Bijvoorbeeld doch niet uitsluitend Facebook, YouTube, Instagram, Skype, WhatsApp, Twitter of LinkedIn
Student:	Gebruiker die bij de TU/e als student staat ingeschreven (voltijd of deeltijd).
Reglement:	Het onderhavige Reglement Computer- en Netwerkgebruik.
Voorzitter CGC:	De directeur van ESA of de door hem/haar gemandateerde tevens qualitate qua voorzitter van de CGC.
Werknemer:	Gebruiker met een vast of tijdelijk dienstverband met de TU/e op grond van de CAO Nederlandse Universiteiten.

Artikel 2 Toepasselijkheid van het Reglement en de Bevoegdheid tot gebruik

2.1 Het Reglement is van toepassing op al het gebruik van door de TU/e ter beschikking gestelde ICT-faciliteiten en -voorzieningen ongeacht waar en hoe daarvan gebruik wordt gemaakt of wordt ingelogd.

2.2 Het Reglement is van toepassing op alle gebruikers die op de TU/e werkzaam zijn, studeren, en/of gebruik maken van de ICT-faciliteiten en -voorzieningen ongeacht of ze op de TU/e aanwezig zijn.

2.3 Uitsluitend de Gebruiker, is gerechtigd gebruik te maken van de ICT-faciliteiten en -voorzieningen.

2.4 De Gebruiker is verplicht zich indien nodig bij het gebruik van de ICT-faciliteiten en -voorzieningen te identificeren met behulp van de door het Bevoegd Gezag aan hem verstrekte gebruikersnaam en/of emailadres, indien aan de orde met behulp van password. De Gebruiker is verplicht zijn gebruikersnaam en zijn password strikt geheim te houden en de gebruikersnaam noch het password aan enige andere bekend te maken.

2.5 Op verzoek van het Bevoegd Gezag dient iedere Gebruiker onverwijld zijn verblijfstitel op de TU/e aan te tonen met behulp van zijn/haar campuskaart.

2.6 Gebruiker dient geen misbruik te maken van de door het Bevoegd Gezag ter beschikking gestelde ICT-faciliteiten en -voorzieningen alsmede gebruikersnaam, password en emailadres.

2.7 De gebruikersnaam, het password en/of het emailadres zijn strikt persoonlijk. De Gebruiker die rechtmatig de gebruikersnaam, het password en/of het emailadres van het Bevoegd Gezag heeft

ontvangen dan wel gebruikt, is verantwoordelijk voor ieder gebruik dat van zijn gebruikersnaam, password en/of emailadres wordt gemaakt, waaronder door anderen.

Artikel 3 Aansprakelijkheid

3.1 De TU/e sluit iedere aansprakelijkheid uit voor schade die voortvloeit uit het gebruik van de ICT-faciliteiten en -voorzieningen, waaronder iedere aansprakelijkheid voor de kwaliteit en/of beschikbaarheid van de ICT-faciliteiten en -voorzieningen en/of de informatie die via de ICT-faciliteiten en -voorzieningen wordt verspreid en/of verkregen. Dit tenzij aan de TU/e opzet of grove schuld kan worden verweten.

3.2 De Gebruiker is aansprakelijk voor de schade die door onjuist, onzorgvuldig of onrechtmatig gebruik dat van gebruikersnaam, password en/of emailadres dan wel door het Bevoegd Gezag verstrekte andere toegangsgegevens wordt gemaakt, waaronder door anderen.

3.3 Gebruiker is aansprakelijk voor de schade die hij aan of in de ICT-faciliteiten en -voorzieningen toebrengt, onder meer ten gevolge van gebruik in strijd met artikel 2 en/of artikel 4, tenzij de schade aan Gebruiker niet kan worden toegerekend. Gebruiker dient de schade aan de TU/e te vergoeden.

3.4 Behalve voor de schade zoals genoemd in artikel 3.2 en 3.3 is Gebruiker aansprakelijk voor de schade die ontstaat voor de TU/e en/of anderen als gevolg van het gebruik van de ICT-faciliteiten en -voorzieningen door Gebruiker in strijd met artikel 2 en/of 4 dan wel anderszins in strijd met de zorgvuldigheid die van Gebruiker mag worden verwacht.

3.5 De Gebruiker vrijwaart de TU/e voor aanspraken en/of vorderingen op de TU/e van anderen in verband met inbreuk op de rechten van deze anderen, welke inbreuk aan Gebruiker kan worden toegerekend, waaronder inbreuk op intellectuele eigendomsrechten en/of onrechtmatig handelen jegens de anderen. Aanspraken en/of vorderingen van anderen op de TU/e worden aan Gebruiker doorgeleid.

Artikel 4 Wijze van gebruik

4.1 De ICT-faciliteiten en -voorzieningen waarvan Gebruiker gebruik maakt, dienen primair en overwegend voor het onderwijs van en onderzoek voor de opleiding waarvoor Gebruiker is ingeschreven, of ten behoeve van de uitoefening van de functie van Gebruiker, of voor het doel waarvoor de Gebruiker op de TU/e aanwezig is. Het is Gebruiker daarnaast toegestaan in beperkte mate de ICT-faciliteiten en -voorzieningen voor privédoeleinden te gebruiken mits dit de normale werkzaamheden van hen of anderen niet belemmerd en anderen hieraan geen aanstoot kunnen nemen. Tevens mag genoemd privé gebruik geen onevenredige belasting vormen voor de ICT-faciliteiten en -voorzieningen van de TU/e en niet in strijd zijn met licenties die de TU/e heeft of met (intellectuele eigendoms-)rechten van TU/e en/of anderen.

4.2 Het is bij gebruik van de ICT-faciliteiten en -voorzieningen niet toegestaan om:

a. De TU/e of anderen materiele of immateriële schade te berokkenen;
b. Inbreuk te maken op rechten van de TU/e of anderen;
c. Overlast of hinder te veroorzaken of de openbare orde te verstoren;
d. In strijd te handelen met het geldende recht, onder meer voortvloeiend uit intellectuele eigendomsrechtwetten, o.a. de Auteurswet, de Benelux Merkenwet, de Wet op de Naburige rechten, de Databankenwet alsmede rechten voortvloeiend uit het Wetboek van Strafrecht, de Algemene verordening gegevensbescherming of met rechten voortvloeiend uit het Burgerlijk Wetboek, meer in het bijzonder artikel 6:162 e.v.;
e. In strijd te handelen met hetgeen volgens het ongeschreven recht in het maatschappelijk verkeer betaamt;
f. Gebruik te maken van andermans gebruikersnaam, password en/of mailadres of andere persoonlijke toegangsgegevens van anderen. Indien dit wel gebeurt wordt dit gebruik door de ander aan de rechtmatige houder van de gebruikersnaam, password en/of mailadres of

andere toegangsgegevens toegerekend;

g. Gebruik te maken van een andere of geveinsde gebruikersnaam, password en/of mailadres, of op andere wijze zijn identiteit trachten te verhullen;
h. Zich al dan niet door middel van hacken, w.o. het doorbreken of kraken van een beveiligingscode, ongeoorloofd de toegang te verschaffen tot andermans gegevens, bestanden en/of computersystemen (w.o. ook wardriving, het sturen van cookies, enz.);
i. Een beveiliging of beveiligingscode te doorbreken of te kraken;
j. Berichten of mededelingen te verzenden, te plaatsen, toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken, waarvan de inhoud aanstootgevend, onzedelijk, discriminerend, opruiend, lasterlijk, beledigend, kwetsend, onbetamelijk of op andere wijze in strijd is met de openbare orde of goede zeden dan wel anderszins onrechtmatig kan worden beschouwd;
k. Grote hoeveelheden berichten of berichten van grote omvang te verzenden, te plaatsen, toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken, waarvan de gebruiker weet dan wel kon of behoorde te weten dat dit storing, overlast en/of vertraging kan veroorzaken binnen het systeem, of bij de ontvanger(s);
l. Ongevraagd berichten te verzenden, te plaatsen, toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken, waarvan de Gebruiker weet, dan wel kon of behoorde te weten dat de berichtgeving niet ten behoeve van ontvanger(s) is noch is gedaan in het kader van de opleiding of de uitoefening van de functie.
m. Opzettelijk berichten of mededelingen te verzenden, te plaatsen, toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken waarvan Gebruiker weet, kon of behoorde te weten dat de inhoud ervan niet juist is.
n. Kettingbrieven, reclameboodschappen en daarmee vergelijkbare berichten te verzenden, te plaatsen toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken.
o. De ICT-faciliteiten en -voorzieningen beschikbaar te stellen aan anderen.
p. De ICT-faciliteiten en -voorzieningen onnodig bezet te houden. Hieronder wordt niet alleen verstaan het in gebruik houden van een faciliteit of voorziening zonder dat gebruiker daarbij lijfelijk aanwezig is, maar ook het gebruik van de ICT-faciliteiten en -voorzieningen voor een ander doel dan het doel als omschreven in artikel 4.1.
q. De ICT-faciliteiten en -voorzieningen zodanig te verlaten, achter te laten of open te laten dat anderen in de gelegenheid worden gesteld gebruik of Misbruik te maken van de Faciliteit en/of Voorziening.
r. De ICT-faciliteiten en -voorzieningen voor illegale of onrechtmatige doeleinden te gebruiken.
s. Wijzigingen aan te brengen in (systeem)instellingen van de ICT-faciliteiten en -voorzieningen van de TU/e.
t. De ICT-faciliteiten en -voorzieningen besmetten met een virus.
u. De ICT-faciliteiten en -voorzieningen te gebruiken voor reclame uitingen en voor commerciële doeleinden. In het geval deze bepaling wordt overtreden en aan de TU/e een boete wordt opgelegd zal deze boete worden doorberekend aan degene die zich niet gehouden heeft aan deze bepaling.

4.3 Gebruik van de ICT-faciliteiten en -voorzieningen in strijd met artikel 4.1 en/of gebruik dat valt onder artikel 4.2 wordt aangemerkt als Misbruik.

Artikel 5 Maatregelen in het kader van beheer

5.1 LIS heeft de bevoegdheid om in het belang van de ICT-faciliteiten en -voorzieningen dan wel onderdelen daarvan, of in het belang van het verkeer over de ICT-faciliteiten en -voorzieningen feitelijke maatregelen te treffen die nadelig kunnen zijn voor de Gebruiker en/of het gebruik van de ICT-faciliteiten en -voorzieningen zonder dat dit aanleiding kan zijn voor aansprakelijkheid van de TU/e.

5.2 De directeur LIS heeft discretionaire bevoegdheid ter zake van mededelingen omtrent het bepaalde in artikel 5.1 en/of toelichting over de getroffen maatregelen.

Artikel 6 Gegevensverstrekking op basis van Wet en Regelgeving

6.1 Het Bevoegd Gezag heeft de bevoegdheid om, indien wettelijke regelingen (w.o. algemene maatregelen van bestuur of verordeningen w.o. van lagere overheden of publiekrechtelijke organen of organisaties) en/of (uitvoerbaar bij voorraad zijnde) uitspraken van een rechterlijke instantie het Bevoegd Gezag nopen, gegevens en/of gegevensbestanden van Gebruiker opgeslagen in dan wel toegankelijk via de ICT-faciliteiten en -voorzieningen, ter inzage te geven aan, of te (doen) verveelvoudigen, (doen) downloaden of te (doen) kopiëren t.b.v. bevoegde functionaris; Gebruiker dient aan het desbetreffende verzoek onmiddellijk te voldoen en de verveelvoudigingen aan de bevoegde functionaris mee te geven.

6.2 Ingeval één of meerdere personen met een beroep op wet of regelgeving zoals bedoeld in artikel 6.1 het Bevoegd Gezag verzoekt om inzage en/of toegang enz. als bepaald in artikel 6.1 tot de gegevens van een Gebruiker in de ICT-faciliteiten en -voorzieningen zal het Bevoegd Gezag daartoe niet overgaan dan nadat de functionaris en/of functionarissen zich formeel hebben gelegitimeerd en mits de daartoe wettelijke dan wel rechtens verplichte formaliteiten in acht zijn genomen.

6.3 Het Bevoegd Gezag neemt de bepalingen van de Algemene Verordening Gegevensbescherming in acht.

6.4 Het handelen van de TU/e op basis van dit artikel kan nimmer aanleiding zijn voor aansprakelijkheid van de TU/e jegens de Gebruiker.

Artikel 7 Monitoring en Onderzoek n.a.v. verdachte aanwijzingen

7.1 De TU/e zal in het kader van handhaving van de in dit reglement vastgelegde regels en uitsluitend voor de in de Basisregels (die op pagina 2 vermeld staan) genoemde doeleinden toezicht en controle houden op de ICT-faciliteiten en -voorzieningen. Inzage in privacygevoelige informatie of persoonsgegevens van individuen zal zoveel mogelijk worden beperkt. Waar mogelijk, zal slechts geautomatiseerd gecontroleerd of gefilterd worden, zonder daarbij inzage in het gedrag van individuen te verkrijgen. Er zal telkens een belangenafweging plaatsvinden tussen het bewaken van de veiligheid en integriteit van de ICT-faciliteiten en -voorzieningen en de bescherming van de persoonlijke levenssfeer van de Gebruiker.

7.2 Ten behoeve van het bewaken van de veiligheid en integriteit van de ICT-faciliteiten en -voorzieningen worden doorlopend de activiteiten en gegevens van gebruikers van de ICT-faciliteiten en -voorzieningen geautomatiseerd verwerkt, aan de hand van monitoring en logging. Deze geautomatiseerde procedures kunnen, op basis van vooraf vastgestelde regels, leiden tot een systeemwaarschuwing. Een dergelijke waarschuwing kan aanleiding geven tot nader onderzoek.

7.3 Bij een gegrond vermoeden van een overtreding van de in dit Reglement genoemde regels of van andere wet- en regelgeving of in gevallen waarin een melding uit het systeem aanleiding geeft tot nader onderzoek, kan het Bevoegd Gezag opdracht geven tot het uitvoeren van een gericht onderzoek. Onder ‘gericht onderzoek’ wordt aldus verstaan het uitvoeren van een onderzoek naar een vermoede overtreding van het Reglement, een vermoede overtreding van wet- en regelgeving of een geautomatiseerde systeemmelding, waarbij doelgericht zal worden achterhaald of er daadwerkelijk sprake is van een overtreding, in welke mate en met welke maatregelen de eventuele risico’s mogelijk gemitigeerd kunnen worden.

7.4 Een gericht onderzoek kan worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt een gericht onderzoek op de inhoud plaats. De tijdens een gericht onderzoek verzamelde gegevens zijn alleen toegankelijk voor systeembeheerders van de betrokken dienst, externe of andere analisten die zijn ingeschakeld om de waarschuwing nader te analyseren. Aan andere beheerders of medewerkers

die bij de uitvoering van het onderzoek betrokken zijn, worden deze gegevens enkel volledig geanonimiseerd beschikbaar gesteld.

7.5 In noodgevallen of wanneer dat nodig is om ervoor te zorgen dat een risico van schade zich niet (verder) voordoet, kan het CERT besluiten om, al dan niet met behulp van de systeembeheerders, technische maatregelen te nemen, zoals het blokkeren van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van de betrokken apparatuur om het netwerk te kunnen gebruiken. Het zal altijd gaan om tijdelijke maatregelen welke niet langer dan noodzakelijk in stand worden gehouden. Indien de situatie dit toelaat, zal het OST vooraf beoordelen of de maatregel passend is, waarbij ook een belangenafweging zal plaatsvinden tussen het bewaken van de veiligheid en integriteit van de ICT-faciliteiten en -voorzieningen en de bescherming van de persoonlijke levenssfeer van de gebruiker. In geval van nood zullen het OST en het CERT zo spoedig mogelijk na het nemen van een maatregel in kennis worden gesteld.

7.6 Indien er een gegrond vermoeden bestaat dat een gebruiker een overtreding begaat of heeft begaan, kan gedurende een bepaalde (korte) periode gericht toezicht plaatsvinden. Dit toezicht zal alleen op de inhoud gericht zijn indien blijkt dat daar gerechtvaardigde en dwingende redenen voor zijn.

7.7 Ten behoeve van de naleving van dit Reglement, kan TU/e verschillende specifieke maatregelen nemen, namelijk:

a) Toezicht ter voorkoming van negatieve publiciteit en controle ten behoeve van de systeem- en netwerkbeveiliging vindt plaats op basis van geautomatiseerde scans van de inhoud, zoals e-mailfiltering en virusscanners.
b) Toezicht met het oog op kosten- en capaciteitsbeheer. Wanneer dergelijke bronnen leiden tot grote uitgaven of ongemak, zullen zij worden geblokkeerd of beperkt zonder dat de vertrouwelijkheid met betrekking tot de inhoud van de betrokken communicatie wordt geschonden.
c) Toezicht om de beveiliging van de ICT-faciliteiten en -voorzieningen te verbeteren en om incidenten op het gebied van cyberbeveiliging te voorkomen. Dit toezicht kan bijvoorbeeld plaatsvinden met behulp van aanvalssimulaties, zoals security penetratie testen en social engineering, zoals phishing-campagnes.

7.8 De Gebruiker is verplicht om aan een onderzoek dat door het Bevoegd Gezag of namens het Bevoegd Gezag wordt gedaan, volledige medewerking te verlenen en zo nodig de ICT-faciliteiten en -voorzieningen alsmede de gegevens ter beschikking te stellen en voorts onbeperkt toegang te verschaffen tot de gegevens die toegankelijk zijn met behulp van de ICT- faciliteiten en -voorzieningen . De Gebruiker is in dit geval verplicht ook gegevens die de Gebruiker niet op de harde schijf van de elektronische apparatuur bewaart, maar die wel via de ICT- faciliteiten en -voorzieningen toegankelijk zijn, ter inzage te geven en het maken van kopieën daarvan toe te staan.

7.9 Het Bevoegd Gezag zal na afronding van het onderzoek schriftelijk aan de Gebruiker berichten wat het Bevoegd Gezag aan onregelmatigheden heeft aangetroffen alsmede een korte omschrijving van de aanleiding van het onderzoek. Indien geen onregelmatigheden zijn aangetroffen, kan het Bevoegd Gezag volstaan met dit aan de Gebruiker mede te delen. Het Bevoegd Gezag is niet verplicht om aan Gebruiker mee te delen of het Bevoegd Gezag aangifte doet bij de politie of andere maatregelen zal treffen. Het bepaalde in artikel 11 en 12 is van overeenkomstige toepassing. Ingeval de gebruiker een Werknemer is, is het bepaalde in artikel 13 van overeenkomstige toepassing.

Artikel 8 Meldingen en te volgen procedure

8.1 Meldingen tegen een Gebruiker kunnen uitsluitend worden gedaan per brief of per e-mail. Iedere

Melding dient gemotiveerd te zijn en duidelijk te zijn omschreven.

8.2 Meldingen over studenten worden gedaan bij de CGC, waarvoor de CGC een e-mailadres heeft ingesteld zoals vermeld staat op de website van ESA. Meldingen die elders binnen de TU/e worden gedaan worden doorgestuurd naar het e- mailadres van de CGC. De Voorzitter CGC beoordeelt de Meldingen.

8.3 Op Meldingen over Studenten is de procedure zoals vermeld in artikel 9, 11 en 12 van toepassing.

8.4 Meldingen over Werknemers worden gedaan bij de desbetreffende beheerder.

8.5 Op de Werknemer is de procedure zoals genoemd in artikel 13 van toepassing.

8.6 Meldingen over Derden worden (voor zover van toepassing) ook gedaan bij het voor deze Derde Bevoegde Gezag .

Artikel 9 Procedure na een Melding over Studenten

9.1 Na Melding als genoemd in artikel 8.2 draagt de Voorzitter van de CGC zorg voor het terstond achterhalen van de identiteit van de Student over wie de Melding is gedaan.

9.2 Meldingen zijn onder te verdelen in:
- (Kennelijk) ongegrond
- Lichte vorm van Misbruik in de zin van bijlage 1.
- Zware vorm van Misbruik in de zin van bijlage 1.

9.3 De Voorzitter van de CGC kan LIS vragen de aard en de omvang van het gebruik waarover een Melding over een Student is ontvangen, te onderzoeken. LIS rapporteert zo spoedig mogelijk aan de voorzitter van de CGC over de uitkomst van het onderzoek.

9.4 De Voorzitter van de CGC bepaalt:
- Of de Melding (kennelijk) ongegrond is dan wel een vorm van Misbruik bevat.
- Of de Melding wordt voorgelegd aan de voltallige CGC conform het bepaalde in artikel 11.
- Of de Melding ziet op fraude door een of meerdere Studenten bij (onderdelen) van onderwijseenheden.

9.5 De Voorzitter van de CGC informeert het voor de Student Bevoegde Gezag ingeval de Melding Misbruik inhoudt. De Voorzitter van de CGC geleidt in geval van fraude bij onderwijseenheden de Melding door naar de examencommissie van de opleiding die de Student volgt.

9.6 Ingeval de Voorzitter van de CGC de Melding (kennelijk) ongegrond acht, handelt de Voorzitter de Melding zelfstandig af.

9.7 In geval de Voorzitter van de CGC de Melding gegrond acht als een lichte vorm van Misbruik doet de Voorzitter de Melding als volgt af:
- Indien de Melding de eerste Melding over een Student is, ontvangt de Student een schriftelijke waarschuwing van de Voorzitter.
- Indien binnen één jaar na de eerste Melding inhoudende een lichte vorm van Misbruik, wederom over dezelfde Student een Melding wordt gedaan die een lichte vorm van Misbruik bevat, ontvangt de student een schriftelijke aanzegging van afsluiting van alle ICT-faciliteiten en -voorzieningen. De mogelijkheid bestaat om die afsluiting te voorkomen.

9.8 Ingeval de Student na een geannuleerde of tijdelijke afsluiting binnen een jaar weer Misbruik maakt wordt de Student door de Voorzitter van de CGC opgeroepen voor een gesprek teneinde over de Melding te worden gehoord. Wanneer er sprake is van een zware vorm van misbruik, leidt de voorzitter de melding door aan de voltallige CGC.

9.9 Indien de Voorzitter van de CGC de Melding van een zware vorm van Misbruik gegrond acht, wordt de Melding door door naar de voltallige CGC afgehandeld. Hierover wordt de Student over wie de Melding is gedaan, schriftelijk bericht.

9.10 De Voorzitter van de CGC heeft indien de Melding daartoe aanleiding geeft, waaronder in de gevallen van zwaar Misbruik of veel voorkomend of herhaald licht Misbruik van de ICT-faciliteiten en -voorzieningen, de bevoegdheid om met onmiddellijke ingang voorlopige maatregelen te treffen tegen de Student mits de Voorzitter van de CGC de beslissing hieromtrent gelijktijdig schriftelijk of per email en gemotiveerd aan de Student doet toekomen. De maatregel kan onder meer inhouden een waarschuwing, tijdelijke afsluiting van de ICT-faciliteiten en -voorzieningen. De voorlopige maatregel van de Voorzitter van de CGC blijft van kracht tot dat het Bevoegd Gezag de voorlopige beslissing op advies van de CGC conform het bepaalde in artikel 11 en 12 de beslissing bevestigt, ongedaan maakt of wijzigt. De Voorzitter CGC treft geen voorlopige maatregel dan na overleg met het voor de Student Bevoegd Gezag.

9.11 De Student kan binnen zes weken na ontvangst van de beslissing ex artikel 9.10 bezwaar maken bij het Bevoegd Gezag tegen de beslissing als genoemde in artikel 9.10. Het bepaalde in artikel 11, 12 en 14 is van overeenkomstige toepassing. Tegen een feitelijke maatregel zonder rechts relevante gevolgen staat geen bezwaar open.

9.12 De besluiten van het Bevoegd Gezag ex artikel 9 kunnen nimmer aanleiding zijn voor aansprakelijkheid jegens de Student, degene die heeft gemeld of welke andere dan ook, behoudens indien aan het Bevoegd Gezag opzet of grove schuld kan worden verweten.

Artikel 10 Bijzondere Personen

Elektronische berichten en gegevens van de Universiteitsraad en IGOleden, leden van de Faculteitsraden en Dienstraden, bedrijfsartsen en andere personen die van het Bevoegd Gezag een formele vertrouwensfunctie hebben gekregen, zijn uitgesloten van onderzoek of monitoring tenzij het bepaalde in artikel 6 of 7 van dit Reglement toepassing vindt. De onderhavige bepaling betreft enkel elektronische berichten en -gegevens en gecreëerd, ontvangen en/of verzonden en/of opgeslagen door voornoemde personen in de uitoefening van hun functie waarbij tevens een directe relatie bestaat met de uitoefening van deze functie.

Artikel 11 De Commissie gedragscode computergebruik

11.1 Er is een CGC die belast is met het onderzoek van een ingediende Melding over een Student of een Melding over een Student en het daaromtrent uitbrengen van advies aan het Bevoegd Gezag omtrent een eventueel te nemen maatregel tegen deze Student.

11.2 De CGC bestaat uit:
- De Voorzitter CGC (directeur ESA of door hem/haar gemandateerde)
- De Secretaris (directeur LIS of een door hem/haar gemandateerde)
- Een Opleidingsdirecteur
- Een jurist
- Een Student

De benoeming van de leden van de CGC geschiedt door het bevoegd gezag voor vier jaar, met uitzondering van de benoeming van de Student. Deze wordt steeds voor een periode van één jaar benoemd.

11.3 De CGC is bevoegd om, indien het dit voor de uitoefening van haar werkzaamheden nodig acht, al datgene te doen wat nodig is om het onderzoek tot een goed einde te brengen.

11.4 De CGC bepaalt haar eigen werkwijze met inachtneming van het onderstaande:
a. De CGC neemt uitsluitend Meldingen in behandeling die schriftelijk bij de CGC zijn ingediend;
b. Van het horen van de Student wordt een verslag gemaakt;
c. De Student kan zich tijdens de hoorzitting door een raadsman laten bijstaan;

d. De CGC kan naar eigen goeddunken anderen horen, van dit horen wordt een verslag gemaakt, dat indien mogelijk ook naar de Student wordt gezonden. De Student kan het horen van de anderen bijwonen, tenzij de CGC unaniem anders beslist;
e. Ieder die door de CGC wordt opgeroepen teneinde te worden gehoord heeft een verschijnings- en informatieplicht;
f. De zitting van de CGC, waarin een melding wordt behandeld, is niet openbaar;
g. De CGC brengt schriftelijk advies uit aan het Bevoegd Gezag; de student krijgt afschrift van het advies. Het advies kan door het Bevoegd Gezag te nemen maatregelen bevatten;
h. De CGC kan het advies van deskundigen inwinnen;
i. Uiterlijk binnen zes weken na de hoorzitting over een Melding brengt de CGC schriftelijk rapport uit aan het Bevoegd Gezag en voegt bij haar rapport ook een advies over een eventueel te nemen maatregel.

11.5 De CGC stelt jaarlijks een verslag op van haar werkzaamheden, welk verslag openbaar is.

Artikel 12 Maatregelen tegen Studenten

12.1 Het Bevoegd Gezag kan, gelet op het advies en het rapport van de CGC, tegen de Student die in strijd heeft gehandeld met het bepaalde in artikel 2 en/of 4 alsmede tegen degene met wiens gebruikersnaam, password en/of e-mailadres in strijd wordt gehandeld met artikel 2 of 4 een of meer van de navolgende maatregelen en/of sanctie nemen:
a. Een schriftelijke waarschuwing waaronder een schriftelijke waarschuwing voorzien van voorwaarden.
b. Het onverwijld verwijderen of blokkeren van informatie. Daarbij kan ook andere informatie van Gebruiker worden verwijderd of geblokkeerd. De Student is aansprakelijk voor alle schade die voortvloeit uit het verwijderen of blokkeren van informatie als bedoeld in dit artikel, ook wanneer hierbij andere informatie dan de informatie van Student wordt verwijderd of geblokkeerd;
c. Het voorwaardelijk of onvoorwaardelijk ontzeggen van de toegang tot en/of het gebruik van de ICT-faciliteiten en -voorzieningen en/of het gebruik van de gebruikersnaam, password en/of e- mailadres en/of voorwaardelijk of onvoorwaardelijk ontzeggen van de toegang tot de TU/e- gebouwen;
d. Het doen van aangifte van een strafbaar feit;
e. Indien een ander aannemelijk maakt dat zijn rechten zijn geschonden, kan de identiteit van de Student aan deze andere kenbaar worden gemaakt mits dit geen ontoelaatbaar verwerking van persoonsgegevens oplevert zoals bedoeld in de Algemene Verordening Gegevensbescherming.

12.2 Het besluit de toegang te ontzeggen kan het geheel of een gedeelte van de universitaire gebouwen, terreinen, ICT-faciliteiten en -voorzieningen betreffen. De Regelgeving en richtlijnen Beheer en Gebruik Gebouwen TU/e is van overeenkomstige toepassing.

12.3 Het besluit tot het nemen van maatregelen bedoeld in lid 1 wordt schriftelijk genomen door het Bevoegd Gezag en wordt aan Student aangetekend toegezonden.

12.4 Het Bevoegd Gezag behoudt zich te allen tijde het recht voor om af te wijken van het advies van de CGC; het Bevoegd Gezag kan ook andere dan de hier genoemde maatregelen treffen.

12.5 Het Bevoegd Gezag besluit binnen drie weken na ontvangst van het advies van de CGC.

12.6 Het Bevoegd Gezag kan in spoedeisende gevallen in afwijking van het bepaalde in dit artikel met onmiddellijke ingang maatregelen treffen als bedoeld in lid 1 sub a t/m d; deze maatregelen zullen aan de Student schriftelijk en aangetekend worden medegedeeld.

12.7 Het bepaalde in artikel 11, lid 4, is van overeenkomstige toepassing op Gebruiker niet zijnde Werknemers of Studenten.

12.8 Het CERT heeft het mandaat om in noodgevallen of wanneer dat nodig is om ervoor te zorgen dat een risico van schade zich niet (verder) voordoet de nodige maatregelen te nemen zoals beschreven in artikel 7.5.

Artikel 13 Procedure en maatregelen betreffende Werknemers

13.1 Voor werknemers van de TU/e geldt dat niet-naleving van dit reglement leidt tot een arbeidsrechtelijke maatregel.

13.2 Het CERT heeft het mandaat om in noodgevallen of wanneer dat nodig is om ervoor te zorgen dat een risico van schade zich niet (verder) voordoet de nodige maatregelen te nemen zoals beschreven in artikel 7.5.

Artikel 14 Gebruik van social media

14.1 Sociale media zijn met in achtneming van artikel 4.1 van dit Reglement toegestaan voor zaken die de functie of het functioneren van de Gebruiker betreffen. De Gebruiker moet er echter voor waken de goede naam van de TU/e en de Gebruiker te schaden. Met andere woorden, sociale media moeten op verantwoorde wijze worden gebruikt.

14.2 De TU/e ondersteunt een open dialoog, het uitwisselen van ideeën en het delen van de kennis van de Gebruiker met anderen via sociale media. Voor gerelateerde onderwerpen moet de Gebruiker ervoor zorgen dat het profiel en de inhoud overeenkomen met hoe hij zich in tekst, beeld en geluid zou presenteren aan anderen.

14.3 Directeuren, managers, leidinggevenden en anderen die namens de TU/e beleid of strategie uitdragen, hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, zelfs als de inhoud niet rechtstreeks verband houdt met hun werk. Op basis van hun positie moeten zij overwegen of indien dit van toepassing is zij op persoonlijke titel kunnen publiceren. Zij moeten zich ervan bewust zijn dat anderen lezen wat zij schrijven.

14.4 Het delen of verspreiden van andermans persoonsgegevens via sociale media in een professionele hoedanigheid is alleen toegestaan als dit past in het reguliere werk van de werknemer en is getoetst op naleving van de AVG. Extra aandacht moet worden besteed aan de verspreiding van beeldmateriaal (foto's en video's) waarin anderen kunnen worden geïdentificeerd; hiervoor is meestal de uitdrukkelijke toestemming van de betreffende personen vereist.

Artikel 15 Intellectueel eigendom en confidentiële informatie

15.1 Dit artikel is met name van toepassing op systeembeheerders, voor wie een inbreuk op deze bepalingen gezien hun bijzondere positie als een ernstig plichtsverzuim zal worden beschouwd.

15.2 De Gebruiker moet vertrouwelijke informatie en privacygevoelige informatie - waaronder persoonsgegevens - waartoe hij in het kader van zijn werkzaamheden of studie toegang heeft, als strikt vertrouwelijk behandelen en voldoende maatregelen nemen om de vertrouwelijkheid te waarborgen.

15.3 De Gebruiker mag geen inbreuk maken op de intellectuele eigendomsrechten van de TU/e en van derden en moet de binnen de TU/e geldende licentieovereenkomsten respecteren, zoals ook vermeld in art. 3.5 en 4.

15.4 De zeggenschap over de informatie van de instelling berust bij de TU/e. De Gebruiker heeft geen zelfstandige zeggenschap over de informatie, tenzij de TU/e deze toestemming uitdrukkelijk heeft verleend.

15.5 De Gebruiker dient bijzondere aandacht te besteden aan het treffen van maatregelen, zoals bedoeld in dit reglement, indien de uitvoering van zijn werkzaamheden de verwerking van vertrouwelijke informatie buiten de instelling noodzakelijk maakt, zoals per e-mail, in niet-institutionele cloudapplicaties of op externe opslagmedia of persoonlijke apparatuur (USB-sticks, tablets, etc.). De Gebruiker moet zich strikt houden aan alle door de TU/e opgestelde voorschriften met betrekking tot vertrouwelijkheid, naleving van de AVG en bescherming van intellectuele eigendom.

Artikel 16 Algemene Wet Bestuursrecht

Op de procedures zoals vermeld in dit Reglement staan uitsluitend voor studenten de bezwaarschriften en beroepsprocedures uit hoofde van de Algemene Wet Bestuursrecht open, nadat en voor zover

a) De procedure als genoemd in artikel 11 van dit Reglement is doorlopen.
b) Er sprake is van een besluit in de zin van de Algemene Wet Bestuursrecht.

Artikel 17 Toepasselijk recht

Indien er geschillen ontstaan uit hoofde van dit reglement of uit hoofde van andere regelingen c.q. overeenkomsten is Nederlands recht van toepassing. De Nederlandse bevoegde rechter is met uitsluiting van andere rechters bevoegd om van geschillen kennis te nemen.

Artikel 18 Bijlagen

Bij het Reglement behoort één Bijlage. De Bijlage kan door de voltallige CGC worden aangepast. De aangepaste Bijlage wordt op de website van de TU/e gepubliceerd alvorens deze werking heeft.

Artikel 19 Inwerkingtreding

19.1 Dit reglement kan worden aangehaald als Reglement Computer- en Netwerkgebruik.

19.2 Dit reglement treedt in werking per 1 januari 2023 en vervangt de regeling zoals die is vastgesteld op 01-01-2020

Aldus vastgesteld door het College van Bestuur in zijn vergadering van 01 december 2022, na verkregen advies van de Universiteitsraad.

Bijlage 1: Voorbeelden indeling van verschillende vormen van misbruik m.b.t. computerfaciliteiten

Deze indeling is een voorbeeld van toepassing van de Regeling. De voorbeelden zijn indicatief, niet limitatief.

Lichte vormen van misbruik (afhandeling door voorzitter CGC resp. Beheerder)

Overlast door o.a.:

- Spelletjes
- Geluid
- Chatten
- Screensavers, achtergrondschermen
- Overbodig bezet houden van hardware en randapparatuur
- Overmatige netwerkbelasting

Zware vormen van misbruik (afhandeling door CGC resp. Beheerder) zijn o.a.

- Racistische uitingen
- Seksistische uitingen
- Schelden
- Pornografie
- Illegaal kopiëren
- Hacken
- Gegevensmanipulatie
- Verspreiding van virussen en illegale software
- E-mailbommen/junkmail
- Opzettelijk beschadigen van hardware en randapparatuur
- Het door middel van bijv. een robot of script uitlezen van bestanden die door de bibliotheek worden aangeboden, terwijl deze alleen volgens de licentievoorwaarden gebruikt mogen worden