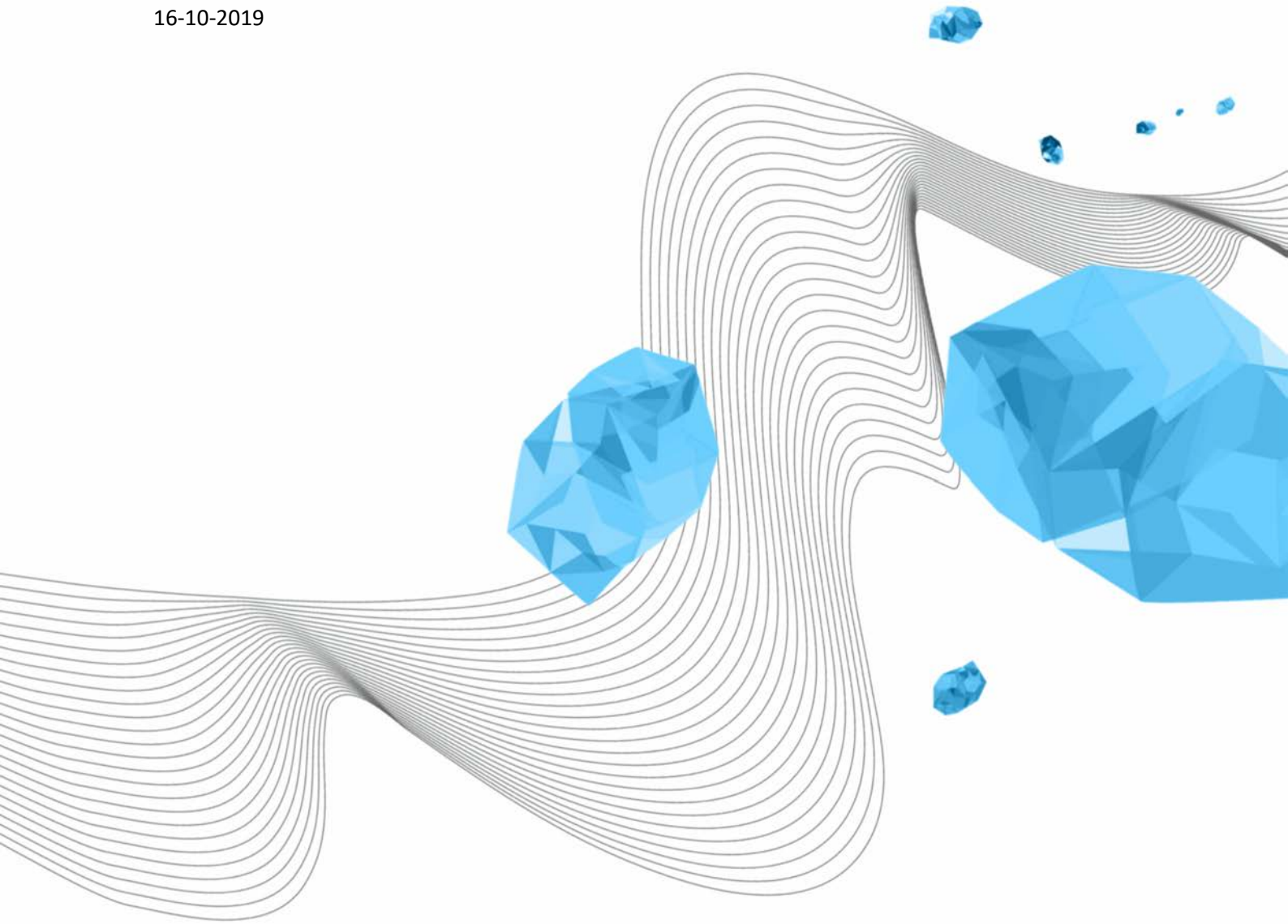
Status: Definitief
Datum vastgesteld in CvB: 11-11-2019
Auteur: Rianne te Brake/Jan Evers

DIGITALE GEDRAGSCODE VOOR MEDEWERKERS UNIVERSITEIT TWENTE

Brake - Loeve, A.A. te (LISA)

Versie 2.3

16-10-2019



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Digitale gedragscode voor medewerkers Universiteit Twente

KENMERK
UIM/181204/brk

VERSIE (STATUS)
2.3

DATUM
16-10-2019

AUTEUR(S)
Brake - Loeve, A.A. te (LISA)

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	2009	Wim Koolhoven	Definitieve versie
1.1	15-06-2018	Rianne te Brake	Herziene versie: - Structuur volgens actuele SURF model - Actualisatie voor wat betreft privacywetgeving (AVG) en stand techniek - Onderdelen geschrapt die in zelfstandige documenten zijn opgenomen
1.6	04-12-2018	Rianne te Brake	Sjabloon aangepast, reacties verwerkt
1.8	15-01-2019	Jan Evers	Opmerkingen MT LISA verwerkt
1.9	06-02-2019	Jan Evers	Opmerkingen MT LISA en Harma Evers verwerkt (o.a. WNRA-check)
2.0	26-02-2019	Jan Evers	Positief advies UCB (26-02-2019)
2.1	15-04-2019	Jan Evers	11-03-2019 voorgenomen vaststelling CvB 10-04-2019 CvB overleg met UR commissie FPB: ter instemming naar OPUT en ter informatie naar UR 15-04-2019 toezeggingen CvB aan UR cie FPB verwerkt 24-04-2019 UR: positief advies onder toevoeging van 1. analyse alleen op basis van UT-account, 2. beheer/ verwerking data op basis van wet- en regelgeving
2.2	28-08-2019	Jan Evers	Wijzigingen nav vragen OPUT
2.3	16-10-2019	Jan Evers	Gericht onderzoek en toegang tot mail bij leden van UR, OPUT, etc. extern. (5.5 en 5.6) – nav bespreking OPUT 16-10-2019 schriftelijke instemming OPUT (brief kenmerk 2019/10/001) 11-11-2019 vastgesteld in CvB

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
1.1	15-06-2018	Rianne te Brake	Jan Evers, Henk Swaters, Peter Peters, Marc Berenschot, Erna van der Zandt, Wim Olijslager (security & privacy overleg)
1.6	06-12-2018	Rianne te Brake	Jan Evers, Henk Swaters, Peter Peters, Marc Berenschot, Erna van der Zandt, Wim Olijslager
1.8	15-01-2019	Jan Evers	MT LISA, HR – Harma Evers
1.9	06-02-2019	Jan Evers	UCB
2.0	27-02-2019	Jan Evers	CvB
2.1	15-04-2019	Jan Evers	Ter instemming naar OPUT van 27-06-2019 Ter informatie naar UR van 24-04-2019
2.2	28-08-2019	Jan Evers	Ter instemming naar OPUT van 19-09-2019
2.3	16-10-2019	Jan Evers	Ter instemming naar OPUT voor schriftelijke afhandeling CvB, ter vaststelling

INHOUDSOPGAVE

1 Bronvermelding 4
2 Basis voor de gedragscode 4
3 Artikelen 4
Artikel 1. Uitgangspunten 4
Artikel 2. Vertrouwelijke informatie 5
Artikel 3. Gebruik van ICT-voorzieningen 5
Artikel 4. Gebruik van sociale media 6
Artikel 5. Monitoring en controle 6
Artikel 6. Gericht onderzoek 7
Artikel 7. Consequenties van overtreding 7
Artikel 8. Slotbepaling 8

1 BRONVERMELDING

De Digitale gedragscode voor medewerkers van Universiteit Twente, verder aangeduid als de Universiteit, is gebaseerd op het Model Acceptable Use Policy voor medewerkers voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo. Deze publicatie is beschikbaar onder de licentie Creative Commons Naamsvermelding 3.0 Nederland[1].

2 BASIS VOOR DE GEDRAGSCODE

Het gebruik van het interne computernetwerk en het openbare computernetwerk (internet) en ICT-middelen die door de Universiteit beschikbaar worden gesteld, is voor (veel van) de medewerkers van de Universiteit noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik van deze faciliteiten zijn risico's verbonden, om deze te verminderen zijn medewerkers gehouden aan gedragsregels van de Universiteit. Tegen de achtergrond hiervan mag van de medewerkers verantwoord gebruik van internet en ICT worden verwacht.

Met deze gedragscode stelt de Universiteit regels omtrent het gewenst gebruik van deze bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van de medewerker.
Het gebruik van social media zoals Facebook, LinkedIn en Twitter wordt steeds belangrijker maar kan ook zijn weerslag hebben op de Universiteit. Daarom stelt de Universiteit ook hier bepaalde regels aan.
De Universiteit is als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer, zo volgt uit de wet. Daarnaast zijn de "Verplichtingen werkgever en werknemer", zoals vermeld in de CAO Nederlandse Universiteiten, onverkort van kracht:

- De werkgever is verplicht al datgene te doen en na te laten, wat een goed werkgever in gelijke omstandigheden behoort te doen en na te laten.
- De werknemer is gehouden zijn functie naar zijn beste vermogen uit te oefenen, zich te gedragen als een goed werknemer en te handelen naar de aanwijzingen door of vanwege de werkgever gegeven.

Omdat de Gedragscode voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van medewerkers, heeft de OPUT instemmingsrecht.

3 ARTIKELEN

ARTIKEL 1. UITGANGSPUNTEN

1.1. Beperkt privégebruik van internet en ICT-middelen is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of het netwerk van de Universiteit. De Universiteit is echter niet verplicht van privé-bestanden reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen. Gebruik voor nevenwerkzaamheden is uitsluitend toegestaan als en voor zover de Universiteit hiervoor schriftelijk toestemming heeft verleend.
1.2. Deze gedragscode geldt voor iedereen die voor de Universiteit werkzaam is, dus ook voor uitzendkrachten en tijdelijke medewerkers. Daarnaast is deze gedragscode van toepassing op

[1] www.creativecommons.org/licenses/by/3.0/nl.

ex-medewerkers die vallen onder de Regeling ICT-faciliteiten ex-UT-ers. Voor gasten van medewerkers die gebruik maken van de ICT-voorzieningen van de Universiteit geldt deze gedragscode eveneens.

1.3. De gedragscode geldt niet voor (gast)studenten; hiervoor is een aparte gedragscode opgesteld. Deze code geldt wel onverkort voor studenten die tevens in dienst zijn bij de Universiteit.

1.4. De Universiteit streeft in het kader van handhaving van deze gedragscode naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

1.5. Elke medewerker draagt zoveel mogelijk zelf verantwoordelijkheid voor het verantwoord en veilig gebruiken van de ICT- en internetvoorzieningen van de Universiteit.

ARTIKEL 2. VERTROUWELIJKE INFORMATIE

2.1 De medewerker dient vertrouwelijke informatie en privacygevoelige informatie waaronder persoonsgegevens, waar hij in het kader van het werk toegang toe heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

2.2 De medewerker treft beveiligingsmaatregelen conform de adviezen en aanwijzingen van het cybersafety-team van de Universiteit[2]. Het cybersafety team heeft geen formele status en bevoegdheden. Het team bevordert awareness op het gebied van cybersafety. De leden zijn medewerkers van HR, M&C, LISA. Het team geeft adviezen en aanwijzingen op basis van vastgesteld beleid.

ARTIKEL 3. GEBRUIK VAN ICT-VOORZIENINGEN

3.1 ICT-voorzieningen waaronder begrepen computer- en netwerkfaciliteiten, (software-)licenties, e-mail en andere ICT-communicatiemiddelen en internet, worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

3.2 Privégebruik en gebruik voor nevenwerkzaamheden van deze middelen is alleen toegestaan zoals bepaald in artikel 1.1 en alleen als de licentievoorwaarden van de leverancier dit toestaan.

3.3 De medewerker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan het systeembeheer per direct het betrokken account ontoegankelijk maken.

3.4 De Universiteit kan voor onderwijs-, onderzoek- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een elektronische leeromgeving, een emailsysteem, (mobiele) applicaties (apps) of multimediadiensten. De medewerker zal voor de betreffende doeleinden alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.

3.5 Gebruik van de faciliteiten (privé of niet) mag niet storend zijn voor de goede orde op de Universiteit en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de Universiteit of derden of de integriteit en de veiligheid van het netwerk aantasten.
Tenminste verboden bij elk gebruik (privé of niet) van ICT-voorzieningen is:

- het bezoeken van sites of verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud, tenzij dit noodzakelijk is voor de vrije informatievergaring in het kader van de functie-uitoefening en hiervoor toestemming is verkregen van de beheerder;
- het verzenden van berichten met een (seksueel) intimiderende inhoud;
- het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;

[2] Bijvoorbeeld het Cybersafety 10-stappenplan.

- het versturen van kettingbrieven, spam of kwaadaardige software zoals virussen, Trojaanse paarden of spyware
- het gebruik van filesharing- of streamingdiensten, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen.

3.6 De medewerker gebruikt voor privémail bij voorkeur een ander dan het door de Universiteit verstrekte e-mailadres, binnen de grenzen van artikel 1.1. De Universiteit zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.

3.7 De medewerker verstrekt bij voorkeur een privé e-mailadres aan de Universiteit, onder andere ten behoeve van het beheer van zijn account. Zo wordt voor wijzigen wachtwoord (wanneer vergeten) het geresette wachtwoord naar het privé e-mailadres gestuurd. Wanneer dat niet beschikbaar is, moet de medewerker met zijn identiteitsbewijs naar de service desk. Het privé e-mailadres wordt door HR ook gebruikt in de aanstellingsprocedure.

3.8 De medewerker is bij beëindiging van het dienstverband verplicht de apparatuur van de Universiteit in te leveren, inclusief de bijbehorende toegangscodes.

3.9 Het aansluiten van actieve netwerkcomponenten (zoals access-points en routers) is niet toegestaan zonder schriftelijke toestemming van LISA netwerkbeheer.

ARTIKEL 4. GEBRUIK VAN SOCIALE MEDIA

4.1 De Universiteit ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de medewerker met vakgenoten en derden via sociale media. Indien dit werk gerelateerde onderwerpen betreft, dient de medewerker ervoor te zorgen dat het profiel en de inhoud in overeenstemming zijn met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's en studenten.

4.2 Bestuurders, managers, leidinggevenden en anderen die namens de Universiteit beleid of strategie uitdragen of een representatieve functie vervullen hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, ook als de inhoud niet direct verband houdt met hun werk. Op grond van hun positie moeten zij afwegen of zij op persoonlijke titel kunnen publiceren.

4.3 Dit artikel geldt ook indien medewerkers vanaf privécomputers of -internetaansluitingen deelnemen aan sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

4.4 De medewerker draagt bij beëindiging van het dienstverband werkgerelateerde sociale-media-accounts over aan de Universiteit.

ARTIKEL 5. MONITORING EN CONTROLE

5.1 Controle van gebruik van de ICT-voorzieningen vindt slechts plaats in het kader van handhaving van de regels uit deze gedragscode.

5.2 Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). De data van medewerkers wordt uitsluitend verzameld en geanalyseerd op basis van een geregistreerd account van de medewerker op de ICT-systemen van de Universiteit. Bij beheer en verwerking van deze data wordt de nationale wet- en regelgeving aangehouden. Deze gegevens zijn alleen toegankelijk voor de verwerkingsverantwoordelijke of medewerkers met een toezichthoudende en/of uitvoerende taak in het kader van een gericht onderzoek.

5.3 Bij vermoedens van overtreding van de regels uit deze gedragscode kan het CvB opdracht geven tot het uitvoeren van een gericht onderzoek (zie artikel 6.1). Op basis van een gericht onderzoek mag e-mail van een medewerker gecontroleerd worden zonder toestemming te vragen aan de betreffende medewerker. Niet alle bij wet verboden activiteiten staan expliciet in deze gedragscode vermeld. Op deze bij wet verboden activiteiten kan echter wel gecontroleerd worden. Een voorbeeld hiervan is het downloaden van illegaal materiaal.

5.4 De Universiteit houdt zich bij het uitvoeren van een gericht onderzoek onverkort aan de Algemene Verordening Gegevensbescherming en andere relevante wet- en regelgeving. In het

bijzonder beveiligt de Universiteit de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang.

5.5 Gericht onderzoek in geval van leden van een medezeggenschapsorgaan, van OPUT-leden en hun adviseurs, van bedrijfsartsen, van HR-functionarissen en van eenieder die zich op grond van de wet op vertrouwelijkheid mag beroepen, wordt altijd uitgevoerd door een extern (forensisch) onderzoeksbureau.

5.6 In geval van langdurige ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de medewerker, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is de Universiteit gerechtigd een vervanger / leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen. Dit is uitsluitend toegestaan indien aangetoond kan worden dat toestemming van de medewerker verkrijgen onmogelijk is of het bedrijfsbelang zodanig zwaar is dat toestemming niet gevraagd kan worden en na toestemming van het College van Bestuur. De vervanger / leidinggevende mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar dan wel afkomstig van leden van een medezeggenschapsorgaan, van OPUT-leden en hun adviseurs, van bedrijfsartsen, van HR-functionarissen en van eenieder die zich op grond van de wet op vertrouwelijkheid mag beroepen – als die mails betrekking hebben op hun hier genoemde rol. Alvorens de vervanger of leidinggevende toegang krijgt, schakelt de Universiteit een medewerker van CERT-UT, een vertrouwenspersoon en / of een HR-adviseur in om de betreffende informatie van de medewerker te controleren om zo privéinformatie te herkennen en af te schermen. In geval van mails verzonden naar dan wel afkomstig van leden van een medezeggenschapsorgaan, van OPUT-leden en hun adviseurs, van bedrijfsartsen, van HR-functionarissen en van eenieder die zich op grond van de wet op vertrouwelijkheid mag beroepen, worden deze mails door een extern forensisch onderzoeksbureau onderzocht en afgeschermd als die mails betrekking hebben op hun hier genoemde rol. Ook het afschermen van privéinformatie wordt dan gedaan door het forensisch onderzoeksbureau.

ARTIKEL 6. GERICHT ONDERZOEK

6.1 Bij zwaarwegende vermoedens van overtreding van deze, of andere, gedragscode door een medewerker heeft de Universiteit het recht om een gericht onderzoek uit te voeren. Onder gericht onderzoek wordt verstaan het onderzoeken van bestaande, reeds beschikbare informatie om vast te stellen of er, en in welke mate, sprake is geweest van overtreding van de gedragscode. Voor het uitvoeren van een gericht onderzoek is altijd een opdracht vanuit het CvB nodig. De Universiteit garandeert dat een gericht onderzoek op een zorgvuldige manier wordt uitgevoerd.

ARTIKEL 7. CONSEQUENTIES VAN OVERTREDING

7.1 Bij handelen in strijd met deze gedragscode kan het College van Bestuur, afhankelijk van de aard en de ernst van de overtreding (proportionaliteit), een of meer van de volgende sancties opleggen:
   a. tijdelijke of definitieve beperking in de toegang tot bepaalde ICT-faciliteiten;
   b. tijdelijk of definitief verbod tot het gebruik van bepaalde ICT-faciliteiten;
   c. betalen van kosten voortvloeiend uit het geconstateerde misbruik;
   d. waarschuwing of berisping of ontslag.

7.2 Sancties (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een geautomatiseerd uitgevoerde verwerking van persoonsgegevens, zoals een automatisch filter of blokkade.

7.3 In afwijking van het voorgaande is het mogelijk dat de Universiteit bij (geautomatiseerde) constatering van overlast of een beveiligingsrisico een (tijdelijke) blokkade van de betreffende faciliteit invoert.

7.4 Sancties worden nooit getroffen zonder dat er sprake is geweest van hoor en wederhoor. Hiervan wordt een schriftelijk verslag gemaakt en verstrekt aan de medewerker.

ARTIKEL 8. SLOTBEPALING

8.1 Deze gedragscode wordt tweejaarlijks geëvalueerd.
8.2 In gevallen waarin deze gedragscode niet voorziet, beslist het College van Bestuur.
8.3 Deze gedragscode vervangt de Gedragscode ICT- en Internetgebruik Universiteit Twente 2009.