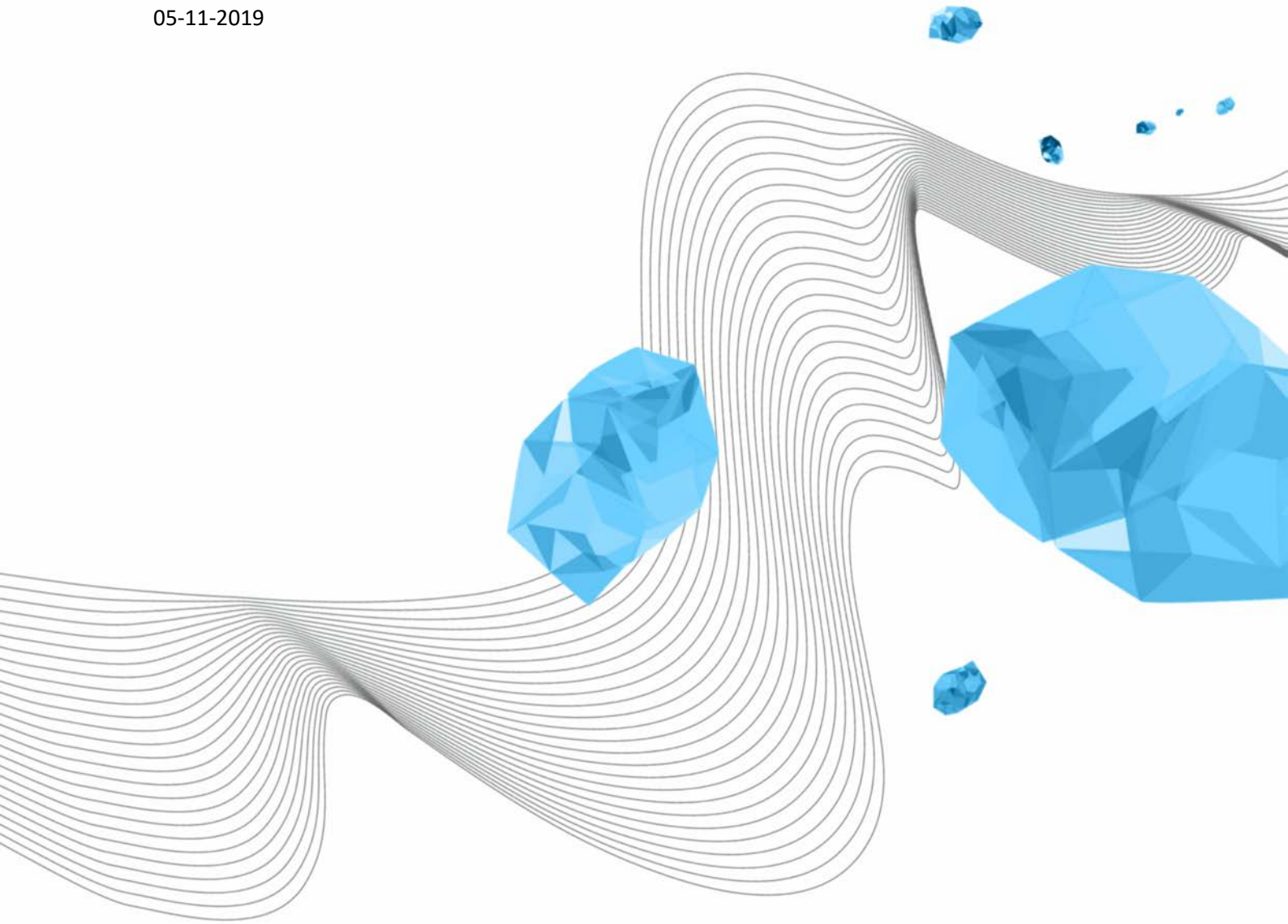
Status: Definitief
Datum vastgesteld in CvB: 25-11-2019
Auteur: Harry Renting

AUTORISATIEBELEID UNIVERSITEIT TWENTE

Renting H. (LISA)

Versie 2.2

05-11-2019



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Autorisatiebeleid Universiteit Twente

KENMERK
[xx/xx/xx]

VERSIE (STATUS)
2.2

DATUM
05-11-2019

AUTEUR(S)
Renting H. (LISA)

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	2013	Wim Koolhoven	Definitieve versie
2.0	07-10-2019	Harry Renting	Aangepast om het nieuwe autorisatie werkwijze. Besproken met de stuurgroep project Autorisatiebeleid Kleine tekstuele aanpassingen
2.1	31-10-2019	Harry Renting	Besproken in het I-Beraad
2.2	05-11-2019	Harry Renting	Opmerkingen I- beraad verwerkt. 25-11-2019 Vastgesteld in CvB

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
2.0	07-10-2019	Harry Renting	Stuurgroep project Autorisatiebeheer
2.1	31-10-2019	Harry Renting	Leden van het I-Beraad ter bespreking in het overleg van 31-10-2019
2.2	05-11-2019	Harry Renting	Ter vaststelling naar CvB van 25-11-2019

INHOUDSOPGAVE

1 INLEIDING

De Universiteit Twente gebruikt informatiesystemen om relevante gegevens te raadplegen en vast te leggen. Bij alle systemen is de integriteit van belang, we willen immers niet dat iedereen zomaar gegevens kan veranderen. Bij veel systemen speelt de vertrouwelijkheid een rol, niet iedereen mag zomaar persoonsgegevens of anderszins vertrouwelijke informatie[1] raadplegen. Voor het naleven van de AVG is het noodzakelijk dat het autorisatiebeleid van de systemen welke de gegevens over personen bevatten goed is geregeld.

Het toekennen van rechten wie wat mag, noemen we autorisatie. Het controleren of iemand is wie hij zegt te zijn is authenticatie en wordt verder uitgewerkt in de Beleidsregels Identitymanagement[2].

Het Autorisatiebeleid is een voorschrift hoe bij informatiesystemen om te gaan met autorisaties.

2 AUTORISATIE VOLGENS HET ROLL BASED ACCESS CONTROL PRINCIPE

Autorisaties voor bepaalde toegangsrechten tot een applicatie worden aangevraagd op basis van een of meerdere rollen die de persoon vervult bij die applicatie. Elke applicatie heeft hiervoor een aantal voor-gedefinieerde rollen, aan elk van de rollen zijn één of meerdere rechten in de applicatie gekoppeld (RBAC: Role Based Access Control). Het verband tussen rollen en rechten wordt per applicatie vastgelegd in een autorisatiematrix. Voor een applicatie zijn de rollen niet van belang. Het gaat uiteindelijk om het vastleggen van de rechten in de applicatie. Een persoon kan per applicatie één of meer rollen hebben.

3 VERANTWOORDELIJKHEID

De houder of eigenaar van het informatiesysteem is ook verantwoordelijk voor de goede inrichting van de autorisatieprocedure. In het Informatiebeveiligingsbeleid[3] noemen we deze functionaris de Systeemhouder.

Bij de meer complexe systemen is de verantwoordelijke voor de gegevens niet dezelfde als de houder van het systeem. Doorgaans ligt de verantwoordelijkheid voor het systeem bij een centrale eenheid en ligt de verantwoordelijkheid voor de gegevens bij een opleiding of faculteit. De procesverantwoordelijke is verantwoordelijk voor de gegevens in het systeem. De Systeemhouder is verantwoordelijk voor het autorisatiebeleid van het betreffende systeem en voor de afstemming met de diverse procesverantwoordelijken.

[1] zie verder de Classificatierichtlijn Informatie en Informatiesystemen
http://www.utwente.nl/sb/uim/informatiebeveiliging/classificatierichtlijn_ut.pdf
[2] Beleidsregels Identitymanagement Universiteit Twente, kenmerk SB/UIM/13/0213/khv
[3] http://www.utwente.nl/sb/uim/informatiebeveiliging/informatiebeveilingsbeleid_ut.pdf § 4.6.5, pagina 12

4 FUNCTIESCHEIDING

Binnen de UT wordt voor autorisatie functiescheiding toegepast. In het algemeen zijn hierbij de volgende rollen te onderscheiden:

Aanvrager: namens de procesverantwoordelijke vraagt deze autorisaties en autorisatie-wijzigingen aan. Doorgaans betreft dit een hoofd van een afdeling of een teamleider.

Eigenaar Autorisatiematrix: is verantwoordelijk voor de autorisatiegegevens en controleert periodiek de autorisatiematrix. Deze dient per applicatie benoemd te zijn. Doorgaans betreft dit dezelfde persoon als de systeemhouder [4]

Functioneel beheer: namens de systeemhouder controleert deze de aanvragen en voert de regie over de autorisatieprocedures.

Applicatie beheer: zorgt voor de uitvoering van de autorisatiewijzigingen.

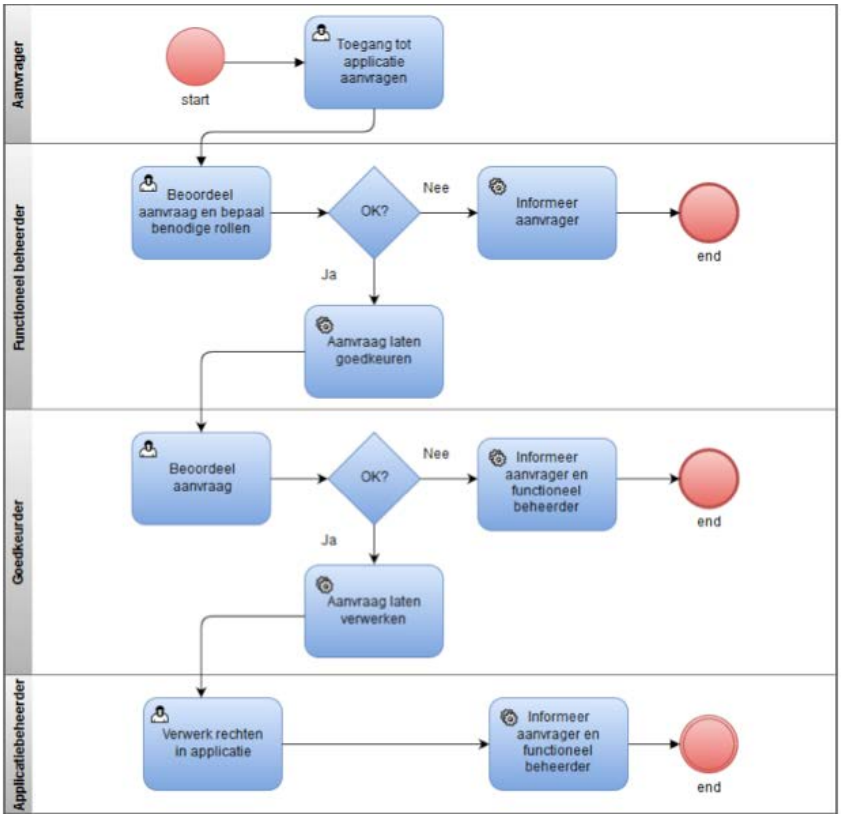
5 WIJZIGINGSPROCES AUTORISATIEMATRIX

De autorisatiematrices zijn zo ontworpen dat niet snel behoefte zal zijn aan het aanpassen of wijzigen van de autorisatiematrix per applicatie. Indien, vanwege een gewijzigde situatie, toch een wijziging gewenst is wordt geadviseerd dat maximaal 1-2 keer per jaar te doen. De eigenaar van de autorisatiematrix stelt de wijziging vast na advies van een door hem samengesteld adviesraad samengesteld uit gebruikers van de betreffende applicatie aangevuld met een functioneel beheerder en de functioneel beheerder van de autorisatie beheer applicatie TACS.

[4] In de bijlage staan de functienamen per applicatie opgesomd.

6 PROCEDURES

Procedure Autorisatie-aanvraag



Deze procedure wordt zowel gevolgd voor het aanvragen van nieuwe autorisaties voor medewerkers als voor wijzigingen in bestaande autorisaties van medewerkers. Alle relevante details worden in de aanvraag vermeld. Wat de relevante details zijn verschilt per systeem. Bij de controle van de aanvraag wordt niet alleen gecontroleerd of de aanvraag compleet en duidelijk is, maar ook of de aanvrager gemachtigd is om de aanvraag te doen.

De aanvraag om toegangsrechten wordt niet direct gedaan door de eindgebruiker, maar door de leidinggevende (of diens vervanger) via de functioneel beheerder van de applicatie. Meestal is bij een nieuwe medewerker al van tevoren duidelijk welke rollen hij of zij nodig heeft in de te gebruiken applicaties. Doel is dan ook om dit vóór aanvang dienstverband al geregeld te hebben.

De eindgebruiker speelt zelf geen actieve rol in het autorisatieproces.

6.1 PROCEDURE AUTORISATIE INTREKKEN

Wanneer een medewerker vertrekt bij de UT of een andere functie krijgt dan moeten autorisaties ingetrokken worden. Primair is de aanvrager verantwoordelijk om dit tijdig aan functioneel beheer door te geven.

6.2 PROCEDURE PERIODIEKE CONTROLE AUTORISATIES

Aangezien er in de praktijk altijd fouten gemaakt worden is het van belang om periodiek te controleren of de toegekende autorisaties nog wel juist zijn. Het toekennen van te weinig rechten aan een gebruiker wordt doorgaans snel onderkend omdat het werk niet goed uitgevoerd kan worden. Te veel rechten kan echter leiden tot ondermijning van het principe van functiescheiding en tot grotere risico's dan noodzakelijk.

Twee keer per maand wordt voor de functioneel beheerder van het betreffende systeem een rapport uitgedraaid dat een overzicht geeft van de toegekende rechten per medewerker. Na controle door functioneel beheer worden deze ter validatie aan de betreffende procesverantwoordelijken gestuurd. Geconstateerde fouten worden zo snel mogelijk hersteld.

6.3 PROCEDURE LOGGING EN PERIODIEKE AUDIT

Om achteraf na te kunnen gaan welke acties er in het autorisatieproces ondernomen zijn, is het van belang deze vast te leggen. Voor het vastleggen van de aanvragen en goedkeuring is per 1 november 2019 een applicatie (TACS, *Twente Autorisatie Controle Systeem)* beschikbaar gekomen waarmee de aanvraag wordt vastgelegd

Voor systemen welke qua Integriteit of Vertrouwelijkheid als kritiek zijn geclassificeerd is het noodzakelijk dat zowel de aanvragen als de uitvoering worden vastgelegd en dat periodiek een audit plaatsvindt.

7 IMPLEMENTATIE EN EVALUATIE

Universitair Informatiemanagement publiceert deze richtlijn en brengt deze onder de aandacht van de systeemhouders. Daarna zal UIM periodiek bij de houders informeren naar de implementatie. Over een jaar (2020) wordt dit beleid en de implementatie in het I-Beraad geëvalueerd.

8 BIJLAGE 1

Deze bijlage is een ‘levend’ document. Wanneer applicaties worden toegevoegd aan TACS zullen deze applicaties in deze bijlage worden opgevoerd.

8.1 OVERZICHT EIGENAREN AUTORISATIEMATRICES

Applicatie	Functie	eigenaar
Oracle Finance	Hoofd Financial Services	R.P. Ree
Oracle HR	Hoofd HR services	A.G.M.J. Holterman
Osiris	Hoofd Informatiemanagement	J. Pasman
BO	Afdelingshoofd Projects & Development	E.A. van den Bosch N.J.C. Letteboer (SP)
JOIN*	Hoofd Universitair Informatiemanagement	J.L. Evers

* Ad interim situatie.