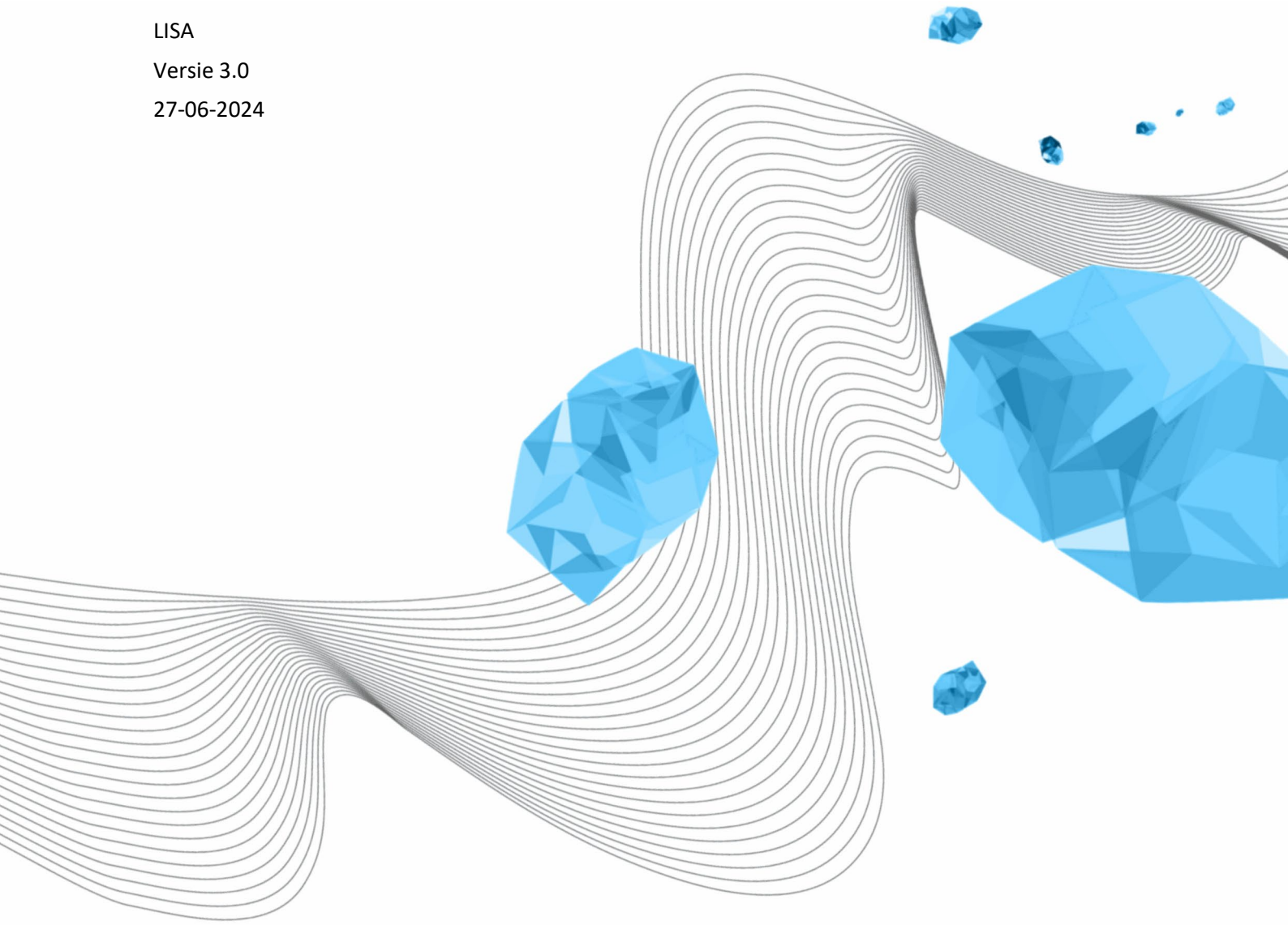
Status: Versie 3.0
Datum vastgesteld in MT-LISA: 08-07-2024
Datum vastgesteld in CvB: 03-09-2024
Herzien: 27-06-2024

AUTORISATIEBELEID UNIVERSITEIT TWENTE

LISA
Versie 3.0
27-06-2024



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Autorisatiebeleid Universiteit Twente

KENMERK
LISA-xxx

VERSIE (STATUS)
3.0

DATUM
27-06-2024

AUTEUR(S)
Henk Swaters

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.
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
3.0	27-06-2024	Henk Swaters	Bij de tijd gebracht

DISTRIBUTIELIJST

VERSIE	DATUM	GEDISTRIBUEERD AAN	OPMERKING
2.0	07-10-2019	Stuurgroep project Autorisatiebeheer	
2.1	31-10-2019	I-Beraad	
2.2	05-11-2019	Ter vaststelling naar CvB van 25-11-2019	
3.0	08-07-2024	Ter bespreking MT-LISA	Vastgesteld

INHOUDSOPGAVE

1 INLEIDING

De Universiteit Twente maakt gebruik van informatiesystemen voor het raadplegen en vastleggen van relevante gegevens. De integriteit van deze systemen is cruciaal; het is namelijk niet wenselijk dat iedereen gegevens zomaar kan wijzigen. Daarnaast speelt vertrouwelijkheid bij veel systemen een belangrijke rol, aangezien niet iedereen toegang mag hebben tot persoonsgegevens of andere vertrouwelijke informatie.

Voor de naleving van de Algemene Verordening Gegevensbescherming (AVG) is het essentieel dat het autorisatiebeleid voor systemen die persoonsgegevens bevatten goed is geregeld. Autorisatie betreft het toekennen van rechten aan gebruikers om bepaalde acties uit te voeren. Authenticatie, het proces om te verifiëren of iemand is wie hij zegt te zijn, wordt verder uitgewerkt in de Guidelines on Identity & Access Management.

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

2 AUTORISATIE MET RBAC

Autorisaties voor specifieke toegangsrechten tot een applicatie worden aangevraagd op basis van een of meerdere rollen die een persoon vervult binnen die applicatie. Elke applicatie beschikt over een aantal voor gedefinieerde rollen, waaraan één of meerdere rechten zijn gekoppeld volgens het Role Based Access Control (RBAC) principe.

Het verband tussen rollen en rechten wordt per applicatie gedocumenteerd in een autorisatiematrix. Hoewel rollen belangrijk zijn voor het toekennen van rechten, ligt de focus uiteindelijk op het vastleggen van de toegangsrechten in de applicatie. Een persoon kan binnen een applicatie meerdere rollen hebben, en daarmee de bijbehorende rechten verkrijgen.

3 VERANTWOORDELIJKHEDEN VOOR DE AUTORISATIEPROCEDURE

De houder of eigenaar van het informatiesysteem is verantwoordelijk voor de juiste inrichting van de autorisatieprocedure. In het Informatiebeveiligingsbeleid wordt deze functionaris aangeduid als de Systeemhouder.

Bij meer complexe systemen is de verantwoordelijke voor de gegevens niet altijd dezelfde persoon als de houder van het systeem. Over het algemeen berust de verantwoordelijkheid voor het systeem bij een centrale eenheid, terwijl de verantwoordelijkheid voor de gegevens bij een opleiding of faculteit ligt. De procesverantwoordelijke is verantwoordelijk voor de gegevens binnen het systeem.

De Systeemhouder draagt de verantwoordelijkheid voor het autorisatiebeleid van het betreffende systeem en zorgt voor de afstemming met de diverse procesverantwoordelijken.

4 FUNCTIESCHEIDING BIJ AUTORISATIE

Binnen de Universiteit Twente wordt voor autorisatie functiescheiding toegepast. In het algemeen worden hierbij de volgende rollen onderscheiden:

- **Aanvrager**: Deze persoon vraagt namens de procesverantwoordelijke autorisaties en wijzigingen in autorisaties aan. Doorgaans is dit een hoofd van een afdeling of een teamleider.
- **Eigenaar Autorisatiematrix**: Deze rol is verantwoordelijk voor de autorisatiegegevens en controleert periodiek de autorisatiematrix. Voor elke applicatie dient er een specifieke eigenaar te zijn, meestal dezelfde persoon als de Systeemhouder.
- **Functioneel Beheer**: Namens de Systeemhouder controleert deze persoon de aanvragen en voert de regie over de autorisatieprocedures.
- **Applicatiebeheer**: Deze rol zorgt voor de uitvoering van de autorisatiewijzigingen.

5 WIJZIGINGSBELEID VOOR AUTORISATIEMATRICES

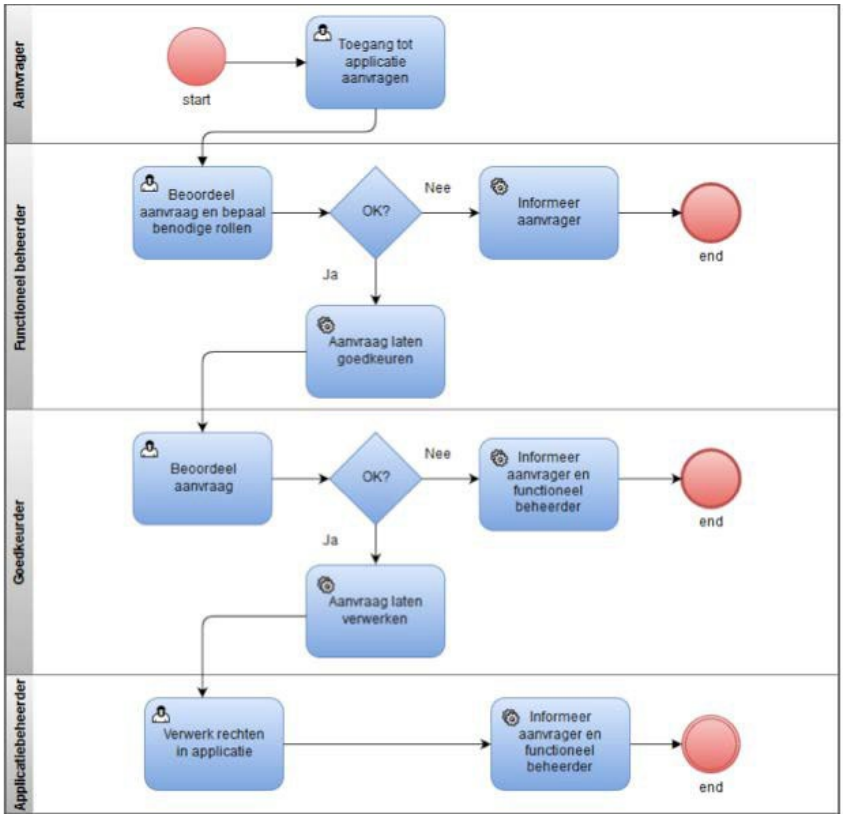
De autorisatiematrices zijn zo ontworpen dat er niet vaak behoefte zal zijn aan aanpassingen of wijzigingen per applicatie. Indien, vanwege een gewijzigde situatie, toch een wijziging noodzakelijk is, wordt geadviseerd dit maximaal 1-2 keer per jaar te doen.

De eigenaar van de autorisatiematrix stelt de wijziging vast na advies van een door hem samengestelde adviesraad. Deze adviesraad bestaat uit gebruikers van de betreffende applicatie, een functioneel beheerder, en de functioneel beheerder van de autorisatiebeheerapplicatie.

Door deze procedure te volgen, wordt gewaarborgd dat wijzigingen zorgvuldig en weloverwogen plaatsvinden, met input van relevante stakeholders en experts.

6 PROCEDURES

6.1 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. Het doel is dan ook om dit vóór aanvang van het dienstverband al geregeld te hebben.

De eindgebruiker speelt zelf geen actieve rol in het autorisatieproces.

Door deze aanpak wordt gewaarborgd dat autorisaties op een gestructureerde en gecontroleerde manier worden toegekend en gewijzigd, in lijn met de beveiligings- en beleidsrichtlijnen van de Universiteit Twente..

6.2 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.

6.3 PROCEDURE PERIODIEKE CONTROLE AUTORISATIES

Om ervoor te zorgen dat toegekende autorisaties altijd accuraat zijn, is periodieke controle essentieel. Het is gebruikelijk dat het ontbreken van voldoende rechten voor een gebruiker snel wordt opgemerkt, vanwege het onvermogen om taken correct uit te voeren. Echter, te veel rechten kunnen het principe van functiescheiding ondermijnen en onnodige risico's introduceren.

Om deze reden wordt tweemaal per maand een rapport gegenereerd voor de functioneel beheerder van het desbetreffende systeem. Dit rapport biedt een overzicht van de verleende autorisaties aan individuele medewerkers. Na controle door de functioneel beheerder worden de bevindingen ter validatie voorgelegd aan de betreffende procesverantwoordelijken. Eventuele geconstateerde fouten worden direct gecorrigeerd.

6.4 PROCEDURE LOGGING EN PERIODIEKE AUDIT

Om te kunnen verifiëren welke stappen zijn genomen tijdens het autorisatieproces, is het essentieel om deze nauwkeurig vast te leggen. Vanaf 1 november 2019 is de applicatie TACS (Twente Autorisatie Controle Systeem) beschikbaar gesteld voor het registreren van aanvragen en goedkeuringen.

Voor systemen die zijn geclassificeerd als kritiek op basis van integriteit of vertrouwelijkheid, is het noodzakelijk om zowel de aanvragen als de uitvoering van autorisaties te documenteren. Periodiek zal een audit worden uitgevoerd om de correctheid en naleving te waarborgen.

7 BIJLAGE 1

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

7.1 OVERZICHT EIGENAREN VAN AUTORISATIEMATRICES

Systemen die persoonsgegevensbevatten of systemen die op vertrouwelijkheid en integriteit hoog geclassificeerd zijn moeten aan het autorisatiebeleid voloen. Hieronder een korte lijst van systemen die hier altijd aan moeten voldoen:

APPLICATIE	FUNCTIE	EIGENAAR
UNIT4	Hoofd Financial Services	R.P. Ree
AFAS	Hoofd HR services	A.G.M.J. Holterman
Osiris	Hoofd Informatiemanagement	J. Pasman
BO	Afdelingshoofd BI-Studio	Kees Posch
JOIN	Afdelingshoofd OILS	O. Steen
TIM/TACS	Afdelingshoofd DSM	H.W.Swaters

8 REVIEW VAN DIT BELEID

Dit beleid wordt minimaal iedere drie jaar herzien. De volgende herziening vindt plaats medio 2027. Er kunnen reden zijn voor een tussentijdse evaluatie. Als die evaluatie er aanleiding toe geeft zal het beleid eerder worden aangepast.

De CISO van de Universiteit Twente is verantwoordelijk voor dit beleid.

Dit beleid wordt vastgesteld door het CvB.