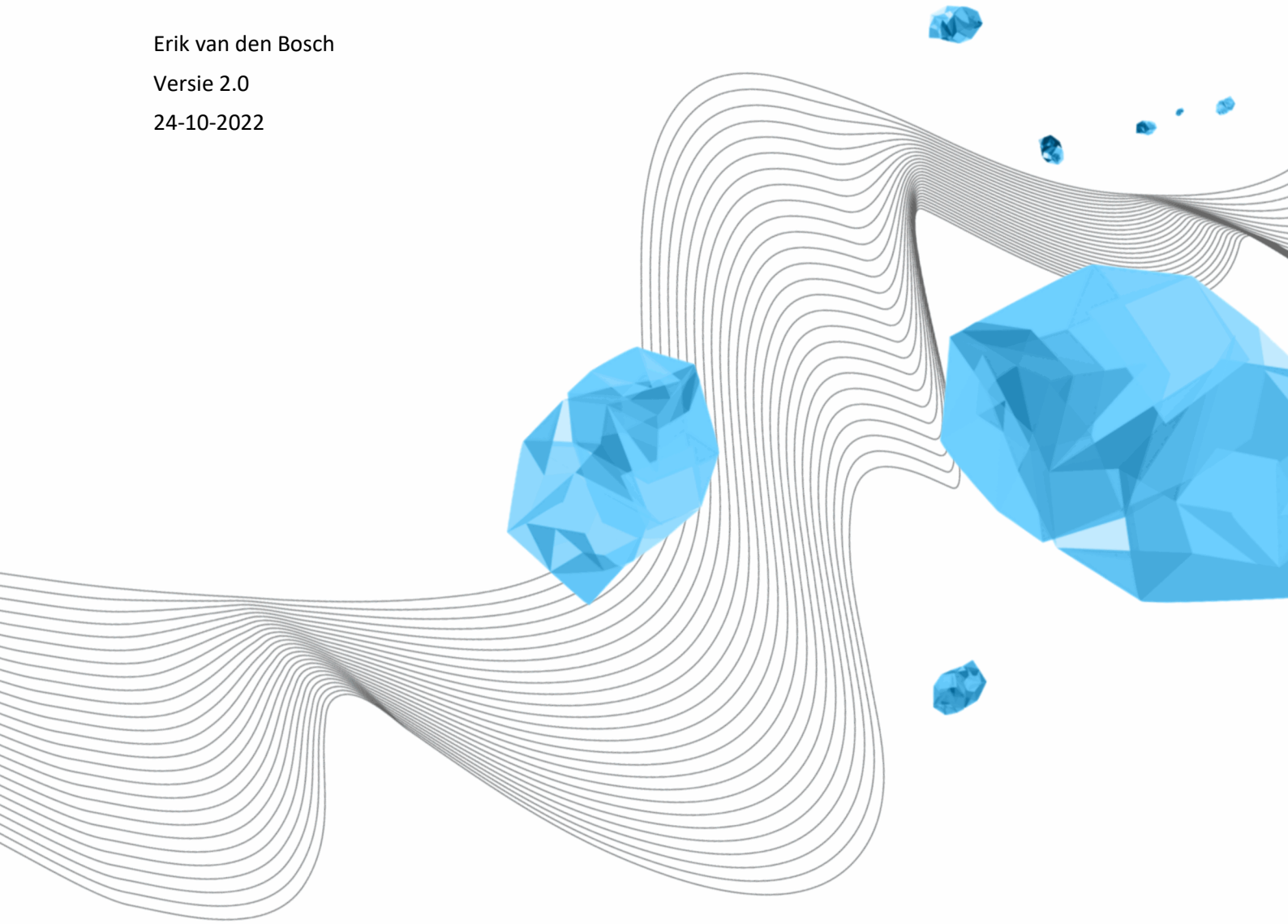
Vertaling van de door het College van Bestuur op 24 oktober 2022 goedgekeurde Engelse versie.

EIGENAARSCHAP VAN EEN INSTELLINGSSYSTEEM

Erik van den Bosch

Versie 2.0

24-10-2022



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Eigenaarschap van een instellingssysteem

ONDERWERP
Afspraken rond het eigenaarschap van een instellingssysteem

KENMERK
LISA-0361

VERSIE (STATUS)
2.0

DATUM
24-10-2022

AUTEUR(S)
Erik van den Bosch

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	24-06-2015	Jan Evers	
1.6	15-07-2022	Erik van den Bosch	Gereviseerde versie.
1.7	30-8-2022	"	Reviewcommentaar verwerkt.
1.8	23-9-2022	"	Reviewcommentaar verwerkt.
1.82	28-9-2022	"	Commentaren verwijderd. Tbv goedkeuring CDO en I-beraad.
1.9	3-10-2022	"	Commentaren CDO verwerkt.
2.0	24-10-2022	"	Vertaling van de goedgekeurde Engelse versie.

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
1.6	15-07-2022	Erik van den Bosch	Jan-Laurens Lasonder, Henk Swaters
1.7	30-8-2022	"	CDO
1.8	26-9-2022	"	LISA MT
1.82	27-9-2022	"	CDO & I-beraad
1.9	3-10-2022	"	CvB
2.0	24-10-2022	"	Publicatie Service Portal website

INHOUDSOPGAVE

INLEIDING

De UT heeft het eigenaarschap van instellingssystemen belegd bij de directeuren van de diensten. Deze notitie geeft duidelijkheid over wat deze rol inhoudt. Dat betreft in het bijzonder de zeggenschap over de functionaliteit van en de gegevens in de systemen en de verantwoordelijkheid voor security en privacy. Deze notitie is bestemd voor de eigenaren van instellingssystemen (dienstdirecteuren) en hun vertegenwoordigers in het I-Beraad. Dienstdirecteuren zijn beheerder volgens artikel 29, lid 3 van het BBR (bestuurs- en beheersreglement). Volgens artikel 30, lid 3 van het BBR kan het CvB voorschriften en aanwijzingen geven omtrent de bevoegdheden en taakinvulling van de beheerder. Deze notitie over eigenaarschap van instellingsystemen is te beschouwen als zo'n voorschrift.

Daarnaast zijn collega's die werkzaam zijn in de IT-keten de doelgroep: functioneel beheerders, applicatiebeheerders, projectmanagers en andere betrokkenen.

WIE IS DE EIGENAAR VAN EEN INSTELLINGSSYSTEEM?

Elk instellingssysteem heeft een eigenaar die verantwoordelijk is voor dat systeem. Een instellingsysteem is een systeem dat van belang is voor een groot deel van de UT community en door de gehele UT gebruikt kan worden. Juist omdat het systeem voor algemeen gebruik bestemd is, is het belangrijk om de verantwoordelijkheid hiervoor helder en op één plek te beleggen. De eigenaar van een instellingssysteem is altijd een *directeur van een dienst*. Meestal ligt het voor de hand welke dienstdirecteur eigenaar is. In zijn algemeenheid is de hoofdverantwoordelijke voor de bedrijfsprocessen die ondersteund worden door het systeem ook de eigenaar van het systeem. Zo is de directeur van HR eigenaar van het HR-systeem.

Meestal is de dagelijkse aansturing van gebruik en beheer van het instellingssysteem door de directeur gedelegeerd aan een team- of afdelingshoofd uit de dienst. Deze persoon zit in het I-Beraad (regulier overleg van eigenaren van Instellingssystemen, voorgezeten door het hoofd van universitair informatiemanagement). De directeur blijft echter eindverantwoordelijk.

De lijst van instellingssystemen wordt actueel gehouden door UIM en gepubliceerd op de website utwente.nl/uim. Voor de bekostiging van instellingssystemen: zie "*Instellingssystemen en hun bekostiging*" op dezelfde locatie.

SYSTEEMEIGENAAR IS VERANTWOORDELIJK VOOR SYSTEEM ÉN GEGEVENS

De eigenaar van een instellingssysteem is verantwoordelijk voor zowel de functionaliteit en het gebruik van het systeem als de gegevens opgeslagen in dat systeem. Dat betekent dat de eigenaar gaat over wijzigingen in functionaliteit en vernieuwing van het systeem.

De systeemeigenaar bepaalt in afstemming met het lijnmanagement van de gebruikersorganisatie wie toegang heeft tot (delen van) het systeem en wie toegang heeft tot de gegevens in het systeem en zorgt voor het verlenen van toegang en autorisaties. De systeemeigenaar past het autorisatiebeleid van de UT toe om toegangsrechten te beheren.

De systeemeigenaar bepaalt in redelijkheid of een ander systeem toegang heeft tot gegevens in zijn systeem. Voor gebruikersvriendelijkheid en het voorkomen van het dubbel moeten invoeren van gegevens zijn koppelingen van belang. Aspecten van privacywetgeving en security moeten hierbij in ogenschouw worden genomen. Zie ook de volgende paragraaf over brongegevens.

Om te bepalen welke beveiligingsmaatregelen nodig zijn voor het systeem volgt de eigenaar de Classificatierichtlijn van de UT, te vinden op utwente.nl/cyber-safety.

De eigenaar is verantwoordelijk voor de inrichting van de bedrijfsprocessen waarbinnen gebruik gemaakt wordt van het systeem, een op het proces passende inrichting van het systeem en het aanbieden van passende voorlichting, training en trainingsmateriaal.

De eigenaar is ook verantwoordelijk voor het beheren van de gegevens in het systeem tijdens hun hele levenscyslus. De eigenaar is daarmee ook verantwoordelijk voor de verplichte periodieke schoning van verouderde gegevens, in afstemming met het lijnmanagement.

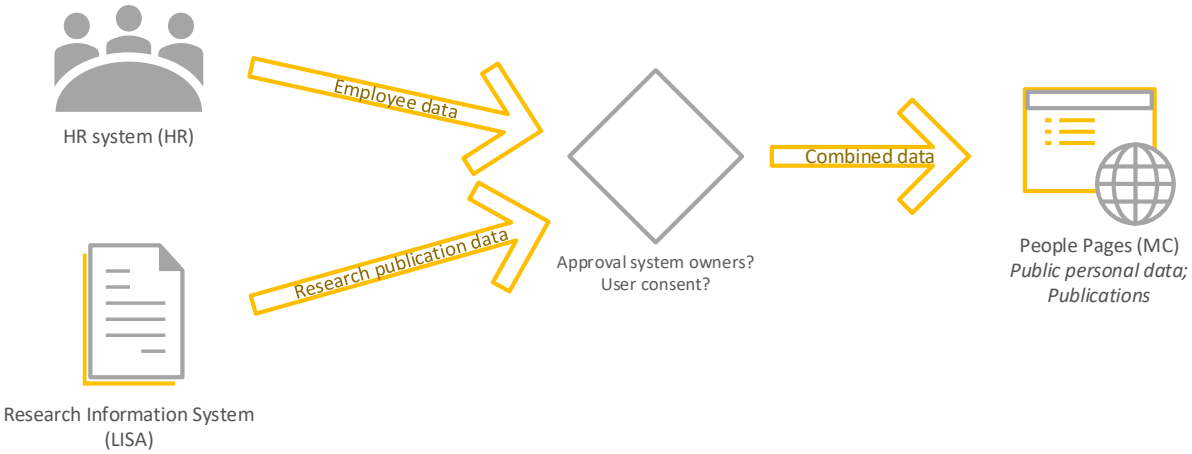
Een belangrijk onderdeel van de verantwoordelijkheid van eigenaren is het opstellen van continuïteitsplannen: wat moet er gedaan worden als het systeem niet beschikbaar is, misschien ook gedurende een langere periode? Deze plannen moeten goed aansluiten op de meer op de infrastructuur gerichte continuïteitsplannen van LISA.

BRONGEGEVENS EN EIGENAARSCHAP

Volgens de UT architectuurprincipes leggen we alle gegevens slechts eenmaal vast, op de plek waar de gegevens ontstaan. Op deze manier wordt gewaarborgd dat er maar één versie van “de waarheid” is en wordt verwarring en onnodige discussie voorkomen. Het systeem waarin we de gegevens initieel opslaan, noemen we het bronsysteem. Als deze gegevens op andere plekken nodig zijn, moet de eigenaar van het bronsysteem toestemming geven op basis van vastgelegde afspraken. De eigenaar van het systeem met brongegevens blijft ook de eigenaar van eventueel gekopieerde gegevens en behoudt zeggenschap over de data.

Een systeemeigenaar is wel verantwoordelijk voor classificatie van alle gegevens in het systeem en voor het (laten) treffen van passende beveiligingsmaatregelen.

In onderstaand voorbeeld bepaalt directeur HR als eigenaar van de medewerkergegevens en directeur LISA als eigenaar van Pure of medewerkergegevens respectievelijk publicaties overgenomen mogen worden in People Pages (van M&C). De gebruiker kan in dit specifieke geval vervolgens zelf nog aangeven wat er publiek getoond mag worden. M&C hoort wel alle gegevens in People Pages te classificeren, omdat combinaties van gegevens en een andere context kunnen leiden tot een andere classificatie.



FUNCTIONEEL BEHEER

De eigenaar van het instellingssysteem organiseert de inrichting van functioneel beheer voor het instellingssysteem. Functioneel Beheer (FB) vertegenwoordigt de stem van de gebruiker. FB zorgt ervoor dat de functies van het instellingssysteem en de bedrijfsprocessen die ondersteund moeten worden, goed op elkaar aansluiten. Daartoe organiseert FB goede afstemming met de gebruikers (vraagsturing). Dat omvat onder meer het maken van afspraken over communicatie over onderhoud en storingen en waar eindgebruikers incidenten kunnen melden.

Functioneel beheer voert het autorisatiebeleid van de UT uit. Lijnmanagement geeft aan wie toegang mag hebben tot de gegevens/het systeem en met welke rechten, functioneel beheer bewaakt de uitvoering van het autorisatiebeleid. Verder ondersteunt functioneel beheer gebruikers, communiceert met hen, zorgt voor handleidingen of andere instructiematerialen en zorgt voor een goede inbedding van het systeem binnen de UT. Universitair informatiemanagement bevordert en ondersteunt een samenhangende uniforme wijze van werken van de verschillende functioneel beheerteams.

Functioneel beheer is verantwoordelijk voor de datakwaliteit van gegevens die binnen het eigen systeem ontstaan of worden gewijzigd, en maakt daartoe afspraken met eindgebruikers. Gegevens worden aangeleverd aan afnemende systemen en aan het datawarehouse van de UT en de kwaliteit van gegevens werkt door in deze informatieketen.

CHANGE MANAGEMENT

Wijzigingen in systemen kunnen vanwege de integratie van systemen verstrekkende gevolgen hebben voor beschikbaarheid van andere systemen en voor kwaliteit van rapportages. Om daarover goed af te stemmen wordt op de UT gewerkt volgens het *change management*-proces, waarvan LISA de proceseigenaar is. Alle functioneel beheerafdelingen moeten de centrale afspraken in dit proces volgen, de systeemeigenaar is daarvoor verantwoordelijk. Het I-beraad is het gremium waar afspraken en werkwijzen worden besproken en vastgelegd.

FUNCTIONEEL BEHEER, APPLICATIEBEHEER EN TECHNISCH BEHEER

Functioneel beheer, zoals hiervoor beschreven, is belegd bij de eigenaar van het systeem. Bij systemen waarbij licenties en hosting niet tot eenzelfde contract behoren is de hosting, applicatie- en technisch beheer belegd bij LISA en/of een externe leverancier. Functioneel beheer betreft het beheren van de informatievoorziening ten behoeve van een gebruikersorganisatie. Hosting betreft het beschikbaar stellen van de hardware en infrastructuur om een applicatie te kunnen ‘draaien’ en benaderen. Applicatiebeheer betreft het beheren, inrichten, updaten en installeren van de applicatie, op aanwijzen van functioneel beheer. Technisch beheer betreft het beheren van de onderliggende infrastructuur (bijv. servers, databases, operating systemen).

Bij SaaS-contracten, waar een groot deel van de UT-systemen inmiddels op zijn gebaseerd, wordt de software, hosting, applicatiebeheer en technisch beheer geleverd door een externe partij. Hierbij heeft functioneel beheer vaak direct contact met de leverancier om wijzigingen te bespreken.

Systemen kunnen vaak uitgebreid geconfigureerd worden via functionaliteit waar functioneel beheer over kan beschikken. Dit kan bestaan uit het wijzigen van een veldnaam, het configureren van een workflow, tot en met het configureren van complete gegevensintegraties met andere systemen. Met deze directe contacten en functionaliteiten heeft functioneel beheer mogelijkheden die in het verleden vaak voorbehouden waren aan de IT-organisatie, en kan veranderingen aanbrengen die verstrekkende gevolgen kunnen hebben voor afnemende systemen, de samenhang in het applicatielandschap en kwaliteit van rapportages.

Om te voorkomen dat elders in de keten problemen ontstaan, moeten alle wijzigingen beoordeeld worden op impact. Functioneel beheer heeft de verantwoordelijkheid om het change managementproces en de centrale afspraken te volgen. De LISA change manager is beheerder van dit proces. Wijzigingen in het change management worden besproken in het I-beraad.

Regie over applicatie- en technisch beheer ligt altijd bij LISA, ook als externe leveranciers dit uitvoeren.

CONTRACT- EN LEVERANCIERSMANAGEMENT

Het inkopen en het maken van de juiste inhoudelijke afspraken met leveranciers is een zeer gespecialiseerd proces dat veel inhoudelijke kennis vergt. Het gaat bijvoorbeeld om het sluitend vastleggen van afspraken in het kader van de AVG, security-afspraken, technische afspraken over de uitwisseling van gegevens, exit-strategieën, intellectueel eigendom, etc. Het risico voor de UT van onjuiste of onvolledige contractafspraken is groot.

Om deze redenen geldt voor alle instellingssystemen (dus ook SaaS) en alle daaraan gekoppelde systemen dat de inkoop en het afsluiten van contracten loopt via LISA contract- en leveranciersmanagement. LISA werkt hierin nauw samen met Inkoop als gaat om aanbestedingsprocedures en compliance van de inkoop.

AUDITVERKLARINGEN

Indien het systeem een SaaS-dienst betreft, dan vraagt LISA Contractmanagement – indien dit onderdeel is van het contract – jaarlijks de auditverklaringen op en zorgt dat de systeemeigenaar hier een afschrift van ontvangt. De eigenaar stemt indien nodig af met afdeling Operational Audit, deze afdeling geeft een advies op de auditverklaring. Indien er bevindingen zijn kan de eigenaar deze samen met LISA-contractmanagement en de leverancier bespreken. De systeemeigenaar neemt het definitieve besluit over het rapport.

SECURITY

De eigenaar van het instellingssysteem is eindverantwoordelijk voor de naleving van de maatregelen die nodig zijn om een voldoende niveau van beveiliging te garanderen. De basis voor het bepalen van welke maatregelen nodig zijn is de *classificatie van de data in het instellingssysteem* volgens de UT-richtlijn (te vinden op de cyber-security website). Met de classificatie van de data op de aspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) wordt bepaald welk niveau van security nodig is. Welke maatregelen nodig zijn bij een bepaald classificatieniveau wordt bepaald door de Information Security Officer van LISA.

De eigenaar dient geconstateerde of vermoedelijke security-incidenten te melden bij CERT-UT. Dit om zo snel mogelijk de juiste (technische) maatregelen te kunnen nemen, en op UT-niveau zicht te houden op deze incidenten. Het Computer Emergency Response Team (CERT-UT) van LISA speelt daarbij een belangrijke rol. CERT-UT werkt samen in een landelijk netwerk van CERT's. Security incidenten kunnen ook door security managers ontdekt worden of via de responsible disclosure procedure gemeld worden. De security managers beoordelen de ernst van een security incident en kunnen zelfstandig besluiten om een informatie systeem (tijdelijk) uit te schakelen indien de ernst van het incident dit nodig maakt. Dit vindt uiteraard zoveel mogelijk in afstemming plaats met de verantwoordelijke functioneel beheer afdeling.

PRIVACY

De eigenaar van een systeem is verantwoordelijk voor het respecteren van de privacywetgeving. Voor de verwerking van persoonsgegevens moeten doel en middel van de verwerking goed vastgelegd worden. Als persoonsgegevens door derden verwerkt worden is een verwerkersovereenkomst nodig. In de verwerkersovereenkomst moet onder andere een afspraak over de levenscyclus van de data gemaakt worden (bewaartermijn en het borgen dat data fysiek verwijderd wordt en niet meer via internet gevonden kan worden). LISA contract management zorgt voor het opstellen van verwerkingsovereenkomsten die aan alle eisen voldoen en stemt dit af met de Privacy ContactPersoon van de dienst en de Functionaris Gegevensbescherming (FG) van de UT. De eigenaar tekent de overeenkomst en is verantwoordelijk voor naleving.

Datalekken dienen direct gemeld te worden bij de FG. De FG heeft daarin een wettelijk vastgelegde rol en bekijkt samen met het CvB of een datalek gemeld moet worden bij de AP (Autoriteit persoonsgevens).