Kenmerk: SB/UIM/13/0819/khv
Datum: 4 oktober 2013

Autorisatiebeleid Universiteit Twente

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 Wet Bescherming Persoonsgegevens 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 geeft algemene richtlijnen hoe bij informatiesystemen om te gaan met autorisaties. De meer complexe systemen zullen de behoefte hebben aan een eigen nadere uitwerking. De eenvoudiger systemen kunnen volstaan met het vastleggen wie welke rol vervult.

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.

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.

---

[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

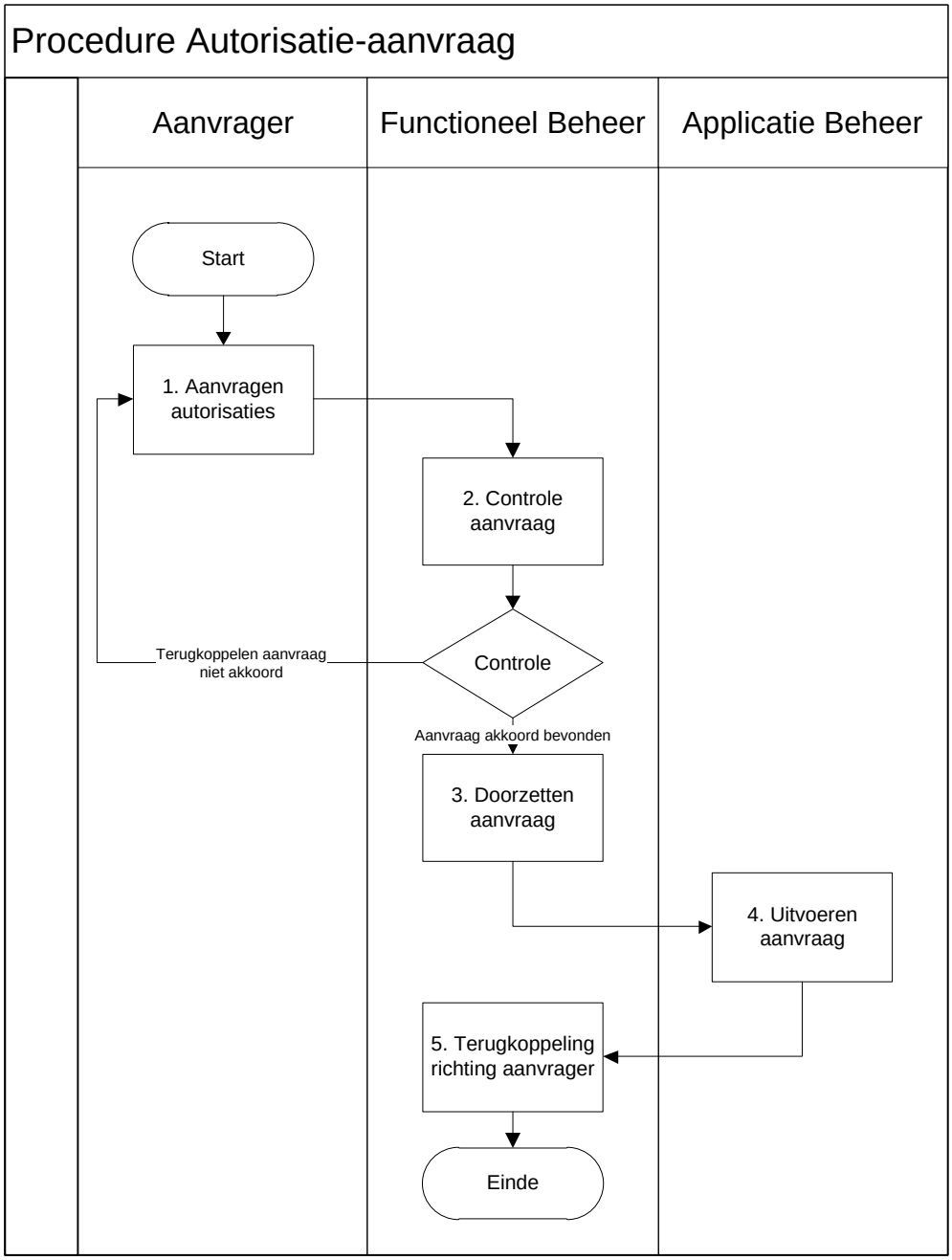
Procesverantwoordelijke: is verantwoordelijk voor de gegevens en controleert periodiek de autorisatiematrix. Doorgaans betreft dit een hoofd van een afdeling of portefeuillehouder ICT.

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.

Procedures[4]

Procedure Autorisatie-aanvraag



[4] Bij de beschrijving van deze procedures is dankbaar gebruik gemaakt van het Autorisatiebeleid Osiris.

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.

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.

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 jaar wordt voor iedere procesverantwoordelijke 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.

Procedure Logging en Periodieke audit

Om achteraf na te kunnen gaan welke acties er ondernomen zijn, is het van belang deze vast te leggen. Voor het vastleggen van de aanvragen is de eenvoudigste manier om dit te realiseren door alle formele communicatie per e-mail te laten plaatsvinden (dus niet alleen mondeling of telefonisch) en deze op een standaard manier te archiveren. Voor het vastleggen van de uitvoering is logging de oplossing.

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.

Implementatie en Evaluatie

Universitair Informatiemanagent publiceert deze richtlijn op haar website en brengt deze onder de aandacht van de houders. Daarna zal UIM periodiek bij de houders informeren naar de implementatie. Najaar 2014 wordt dit beleid en de implementatie voor de eerste keer in het I-Beraad geëvalueerd.