Universitair Informatiemanagement UNIVERSITEIT TWENTE.

Kenmerk: SB/UIM/13/0213/khv
Datum: 9 juni 2015

Beleidsregels Identitymanagement Universiteit Twente

Versiebeheer

Datum	Wijziging
2 december 2013	Originele versie
9 juni 2015	Aanpassing op grond van Wachtwoordbeleid en actualisatie: 9. randvoorwaarden voor functionele identiteiten toegevoegd 19. Aanvulling op verplichte jaarlijkse wijziging vervangen

Inleiding

ICTS is als houder verantwoordelijk voor het Identitymanagement (IDM) systeem. Het IDM-systeem zorgt voor de authenticatie van gebruikers voor de informatiesystemen. Authenticatie is het proces waarmee een persoon zijn identiteit aantoont. Autorisatie is het proces van het verlenen van toegang aan personen of systemen tot functionaliteit van ICT-diensten.

Er is vanuit de organisatie behoefte aan een korte bondige set beleidsuitgangspunten welke vervolgens als randvoorwaarden bij de verdere ontwikkelingen van het IDM-systeem gelden. Dit document beschrijft het kortetermijnbeleid, hiernaast is er autorisatiebeleid[1] ontwikkeld.

De eisen die aan het IDM-systeem worden gesteld, worden vanuit drie gezichtspunten belicht: gebruikers, security en architectuur. Voor het beleid ten aanzien van e-mailadressen wordt verwezen naar het Namenbeleid voor websites en e-mailadressen UT[2].

Gebruikers

1. Voor toegang tot alle systemen van de UT gebruiken medewerkers en studenten één unieke gebruikersnaam. Het m-nr c.q. s-nr is hier prima voor geschikt. Indien een individu meerdere soorten relaties (bijvoorbeeld student en docent) met de UT heeft dan worden deze niet gecombineerd.
2. Tenzij hier om securityredenen van moet worden afgeweken kunnen medewerkers en studenten op alle UT-systemen na invoering van hun gebruikersnaam inloggen met hetzelfde wachtwoord.
3. Idealiter wordt voor alle systemen Single Sign-On gebruikt, dat wil zeggen dat één keer inloggen genoeg is. Tenzij hier om securityredenen van moet worden afgeweken wordt bij nieuwe systemen de toegang geregeld via het IDM-systeem van de UT. Bestaande systemen die binnenkort uitgefaseerd worden, hoeven hier niet geschikt voor gemaakt te worden.

[1] Autorisatiebeleid Universiteit Twente, kenmerk SB/UIM/13/0819/khv, zie http://www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf
[2] zie http://www.utwente.nl/uim/voor-eindgebruikers/namenbeleid_ict_domeinen_ut.pdf

4. De authenticatie wordt zoveel mogelijk zo ingericht dat docenten in onderwijssituaties hun wachtwoord niet hoeven in te voeren.
5. De systemen worden zo ingericht dat delegatie van werkzaamheden, bijvoorbeeld aan een secretaresse, mogelijk is zonder afgifte van het wachtwoord. Via handleidingen op de website van ICTS wordt dit aan gebruikers kenbaar gemaakt.
6. Gebruikers kunnen via een self-service webapplicatie hun wachtwoord wijzigen.
7. Er bestaat een procedure volgens welke gebruikers die hun wachtwoord vergeten zijn deze via de helpdesk kunnen laten resetten.
8. Medewerkers kunnen via een self-service webapplicatie gegevens welke in de adressenlijst en telefoongids worden getoond beheren.
9. Medewerkers kunnen via een self-service webapplicatie functionele identiteiten en tijdelijke identiteiten voor externen aanvragen. Het gebruik van functionele identiteiten wordt zo ingericht dat altijd is na te gaan welke medewerker welke handeling heeft verricht. Bij overdracht van verantwoordelijkheid wordt het wachtwoord gewijzigd.
10. Gebruikers wensen een IDM-systeem wat instellingsoverstijgende samenwerking faciliteert. SURFconext kan hierin voorzien.
11. Voor noodgevallen bestaat er een spoedprocedure waarmee een identiteit (tijdelijk) buiten werking gesteld kan worden.

Security

De Wet Bescherming Persoonsgegevens en de Code voor informatiebeveiliging ISO 27002 stellen eisen met betrekking tot het IDM-beleid.

12. De Beschikbaarheid van het IDM-systeem is noodzakelijk voor het gebruik van enig ander systeem en daardoor hoogst kritiek. Er wordt dan ook voldoende redundantie toegepast om continue beschikbaarheid te kunnen garanderen.
13. In die gevallen waarbij hoge eisen worden gesteld aan de integriteit of vertrouwelijkheid van gegevens kan de houder (in overleg met de proceseigenaar) er voor kiezen om hogere eisen aan de authenticatie te stellen. In die gevallen is alleen het ingeven van een wachtwoord niet genoeg, maar zijn aanvullende maatregelen nodig (tweefactorauthenticatie).
14. Voor zover mogelijk wordt de gebruiker bij verdachte logins geïnformeerd en aangeraden zijn wachtwoord aan te passen.
15. De procedures voor de aanmaak van identiteiten en het wijzigen van wachtwoorden worden gedocumenteerd. De verschillende rollen worden zo verdeeld dat functiescheiding wordt toegepast.
16. De betrouwbaarheid van het IDM-systeem alsmede de genomen beveiligingsmaatregelen worden periodiek geaudit.
17. In het Security Overleg tussen UIM en ICTS wordt periodiek besproken in hoeverre het IDM-systeem aan het geformuleerde beleid voldoet.

Wachtwoorden

Er is een apart wachtwoordbeleid[3] opgesteld, daarin zijn onderstaande aspecten afgewogen en verder uitgewerkt.

18. Wachtwoorden zijn vertrouwelijk.
19. Wanneer er aanwijzingen zijn dat hun wachtwoord is gecompromitteerd dan dienen gebruikers het dwingende advies te krijgen dit te wijzigen. Wachtwoorden worden ten minste jaarlijks gewijzigd.

[3] Wachtwoordbeleid Universiteit Twente, kenmerk SB/UIM/14/0131/khv, zie http://www.utwente.nl/uim/informatiebeveiliging/wachtwoordbeleid-universiteit-twente.pdf

20. Een zekere complexiteit van wachtwoorden wordt afgedwongen, waarbij de onthoudbaarheid niet in het gedrang komt. Hiervoor is een wachtwoord policy van kracht.
21. Gebruikers gebruiken hun wachtwoord niet als wachtwoord voor andere systemen, dat wil zeggen niet voor systemen waarbij de toegangscontrole niet door het UT IDM-systeem wordt verzorgd. Zij worden hier actief op gewezen.
22. Gebruikers schrijven hun wachtwoord niet op en verstrekken dit niet aan anderen. Zij worden hier actief op gewezen.
23. Wachtwoorden worden middels een beveiligde verbinding verstuurd.
24. Wachtwoorden zijn door ICTS-medewerkers niet oproepbaar of te ontsleutelen.
25. Wachtwoorden worden via langzame eenwegsleutels opgeslagen. Dit betekent dat er geen ontsleutelalgoritme bestaat en dat een brute-force aanval lang duurt.

Auditbaarheid

26. Alle wijzigingen in het IDM-systeem worden gelogd. Deze logfiles worden periodiek handmatig gecontroleerd.
27. Alle wijzigingen in bronsystemen welke leiden tot wijzigingen in het IDM-systeem worden gelogd. Deze logfiles worden periodiek handmatig gecontroleerd.

Privacy

28. Er wordt in en door het IDM-systeem niet meer informatie opgeslagen dan noodzakelijk.
29. Bij het verlenen van toegang tot een (externe) applicatie wordt aan de betreffende applicatie niet meer informatie doorgegeven dan noodzakelijk.

Architectuur

30. Het IDM-systeem wordt zo eenvoudig als mogelijk ingericht om de beheersbaarheid en auditbaarheid te garanderen. Het ideaal van een enkelvoudig systeem voor toegangscontrole is helaas niet haalbaar, maar kan wel benaderd worden.
31. Alleen met toestemming van ICTS mag gebruik worden gemaakt van de UT-identiteit.
32. Applicaties welke niet door ICTS worden beheerd mogen in geen geval zelf om een wachtwoord vragen, maar moeten dit overlaten aan een systeem wat door ICTS wordt beheerd.
33. Webapplicaties regelen niet zelf de toegang, maar gebruiken een centrale UT-accessmanager. Bij externe webapplicaties wordt dit geregeld via SURFfederatie / SURFconext in combinatie met de centrale UT-accessmanager.

Bronsystemen

34. Identiteiten worden niet rechtstreeks ingevoerd in of verwijderd uit het IDM-systeem. Dat gebeurt altijd in één van de bronsystemen. Het IDM-systeem is geen bronsysteem.
35. Het IDM-systeem volgt de informatie uit de bronsystemen met betrekking tot aanmaak, buitengebruikstelling en verwijdering van identiteiten.
36. Als een gebruiker in meerdere bronsystemen voorkomt, dan zal deze meerdere identiteiten hebben.
37. Er worden door ICTS sluitende afspraken gemaakt met de houders van de bronsystemen over het gebruik van informatie en de verdeling van verantwoordelijkheden, onder andere ten aanzien van de aanmaak, buitengebruikstelling en verwijdering van identiteiten.
38. Voor medewerkers en PNUT-ers[4] is het personeelsinformatiesysteem[5] het bronsysteem.

[4] PNUT = personeel niet-UT
[5] onder verantwoordelijkheid van HR

39. Voor studenten is het studenteninformatiesysteem[6] het bronsysteem.
40. Voor alumni is het alumniinformatiesysteem[7] het bronsysteem.
41. Voor andere groepen[8] van identiteiten wordt met de betreffende procesverantwoordelijke afgesproken welk systeem als bronsysteem gebruikt wordt.
42. Voor tijdelijke identiteiten (tot enkele dagen) wordt een apart bronsysteem gebruikt.
43. Voor functionele identiteiten wordt een apart bronsysteem[9] gebruikt.

[6] onder verantwoordelijkheid van CES
[7] onder verantwoordelijkheid van S&B
[8] Voor ex-UT-ers geldt de Regeling ICT-faciliteiten ex-UT-ers, zie http://www.utwente.nl/uim/voor-eindgebruikers/regeling_ict_faciliteiten_ex_uters.pdf
[9] onder verantwoordelijkheid van M&C