MALMÖ UNIVERSITET

Styr- och handledningsdokument

Dokumenttyp:	Policy
Beslutsdatum:	2023-05-17
Beslutande/Titel:	Malmö university identity management
Giltighetstid:	
Dokumentansvarig/Funktion:	robert.faling@mau.se
Diarienummer:	
Version:	1.2
Revisionsdatum:	

Malmö university identity management

Postadress
Malmö universitet
Gemensamt verksamhetsstöd

Besöksadress
Neptuniplan 7

Telefon

Fax

E-post
robert.faling@mau.se

Webb
www.mau.se

1. Inledning

Malmö universitet är som svenskt lärosäte beroende av att på ett säkert och enkelt sätt kunna ge sina betrodda användare tillgång till gemensamma nationella resurser. Detta ges genom medlemskap i SWAMID och de tjänster som följer med medlemskapet.
Malmö universitet ser ett fortsatt medlemskap i SWAMID som en förutsättning för sin verksamhet och tar efterlevnaden av de regler som följer på medlemskapet på största allvar.
Malmö universitet uppfyller kravet för SWAMID AL1 och SWAMID AL2.

2. Disposition

Detta dokument beskriver tjänsten “Malmö University identity management” även kallad “identitetshanterare”.
Dokumentet utgår från de punkter som återfinns i *Document SWAMID Identity Assurance Level 2 Profile [Identifier http://www.swamid.se/policy/assurance/al2 Version V2.0].*
Numrering i resterande rubriker samt hänvisningar följer numreringen i denna utgångspunkt.

3. Efterlevnad och revision *[Compliance and Audit]*

Identitetshanteraren och underliggande system hanteras och granskas i enlighet med universitetets ledningssystem för informationssäkerhet. Årlig revision sker i samband med risk och sårbarhetsanalys (3.2).

4. Organisationskrav *[Organisational Requirements]*

4.1 Organisationens och tjänstens mognad *[Enterprise and Service Maturity]*

Malmö universitet (MAU), organisationsnummer [202100-4920], är en statlig utbildningsmyndighet vars verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr universitetets arbete är regeringsformen (SFS 1974:152), tryckfrihetsförordning (SFS 1949:105), myndighetsförordningen (SFS 2007:515), högskolelagen (SFS 1992:1434) och högskoleförordningen (1993:100).

Regleringsbrevet utställs årligen av regeringen och styr universitetets uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.
Lärosätets katalog- och behörighetssystem Active Directory (AD) innehåller uppgifter om lärosätets organisation samt personuppgifter för alla som är verksamma vid lärosätet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas. Dataskyddsförordningen tillsammans med kompletterande lagstiftning och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.
Studenters personuppgifter hämtas ur studiedokumentationssystem Ladok och som omfattas av (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor för hanteringen av studenters personuppgifter i Active Directory (AD).
Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).
Process för hantering av utrangerad hårdvara regleras i IT-handboken avsnitt 3.11.5.

4.2 Upplysningar och information till användare *[Notices and User Information]*

Samtliga dokument som beskriver användares rättigheter och skyldigheter finns publicerade på universitetets webbplats.

Tjänsten beskrivs i universitetets tjänstekatalog. Här beskrivs begränsningar, rättigheter och förhållandet till svensk lag i de dokument som innefattar användarens rättigheter och skyldigheter. Tjänstekatalogen anger även kontaktinformation till Helpdesk.

- Datorregler student och personal (på engelska) (4.2.1)
- GDPR (på engelska)
- Tjänstedefinition (på engelska) (4.2.5)

Användaren måste acceptera användaravtalet (4.2.2) och förändringar i användaravtalet (4.2.3) innan tillträde till identitetshanteraren ges.

Serviceportalen kräver ett godkännande innan åtkomst och version och versionsdatum för godkännande av användaravtalet lagras (4.2.4).

4.3 Säker kommunikation *[Secure Communications]*

Användarkontot ges tillträde till resurser efter behov och tillträde ges endast efter inloggning via serviceportalen. Regler för administratörskonton finns i dokumentet ”*Ansvar, befogenheter och skyldigheter för systemadministratörer”* och lärosätets förvaltningsdokumentation. (4.3.1).

Lösenordsinformation hanteras och granskas i enlighet med universitetets ledningssystem för informationssäkerhet (4.3.2).

All kommunikation från servrar till servrar och servrar till användare är krypterad (4.3.3) och använder 2048 bit RSA nycklar (4.3.4).

4.4 Insamling (loggning) av säkerhetsrelaterade händelser *[Security-relevant Event (Audit) Records]*

Säkerhetsrelaterade händelser i Active Directory loggas (4.4.1). Loggboken backas upp och arkiveras. Varje arkiv sparas i ett år.

5. Driftskrav *[Operational Requirements]*

5.1 Behörighetskrav i driftmiljö *[Credential Operating Environment]*

Universitetets lösenordspolicy föreskriver minst 8 tecken med komplexitet (5.1.1) och man måste godkänna ”användarens rättigheter och skyldigheter” (5.1.3).

Identitetshanteraren är konfigurerad enligt SWAMID’s rekommendationer för att motverka omsändning (5.1.2).

Ansvar för löpande administration finns och systemet omfattas av LIS (5.1.4).

5.2 Utfärdande av behörighet *[Credential Issuing]*

Identitetshanterarens (5.2.2) scope är ”mah.se” och ”mau.se” (5.2.1).

Ett (AL-klassat) användarkonto är unikt (5.2.3) per person och kategoriseras som personal, student eller både och (5.2.4). Personuppgifter kan ändras i Ladok för student och i Primula för personal. Informationen i Primula har prioritet över den i Ladok.

Tilläggsinformation (mobilnummer och alt. epost-adress) kan ändras i serviceportalen (5.2.7). Vid ändring av epost-adress skickas information om ändringen till befintlig adress och ett verifieringsmail skickas till den ändrade adressen. Ändringen sker först när

användaren har verifierat ändringen via länken i mailet. Vid ändring av mobilnummer skickas information om ändringen till epost-adressen och en engångskod via sms till det nya mobilnummer som måste verifieras innan ändringen sparas.

Alla verifikationsmail och sms koder är tidsbegränsade till 24 timmar och av engångskaraktär.

Servicedesk, helpdesk, it-administrativ personal och personalhandläggare med AL2 har rättighet att ändra information på användarens konto. Även i detta fall måste användaren själv verifiera sina nya uppgifter med samma rutin som om användaren ändrat själv.

Beställning av användarkonto görs i serviceportalen för konton klassade som student eller personal. Här gäller följande:

Student (AL1)

För att beställa ett studentkonto måste man vara antagen eller registrerad i Ladok på en kurs, ett program eller forskningsämne på Malmö universitet under innevarande termin. Verifieringslänk skickas bara till e-postadresser som är registrerade i Ladok eller NyA.

Det finns tre rutiner för att få den verifieringslänk (kontroll av e-post för AL1) som gör det möjligt att skapa ett konto:

- Vid onlineregistreringen används e-postadressen i Ladok som identifikation tillsammans med en captcha för kontroll.
- Vid felaktig e-postadress krävs det ett personligt besök vid helpdesk för kontroll av legitimation innan e-posten uppdateras.

Vid båda rutinerna skickas länk med tidsbegränsad kod till e-postadressen.

Denna länk går till serviceportalen där man ska verifiera och komplettera personuppgifter, välja lösenord samt godkänna användaravtalet innan kontot blir skapat.

När kontot är färdigt, skickas kontonamnet till e-postadressen. I detta utskick bifogas “information för ny student till lärosätet” och information om hur man skapar konton till eduroam.

Personal (AL1)

Vid personligt besök med personalhandläggare kontrolleras personuppgifter som läggs in i personal- och lönesystemet Primula.

Kontot beställs av personalhandläggaren och kontoinformationen skickas till den nyanställdes alt. e-postadress tillsammans med en länk till lösenordsåterställning (kontroll av e-post för AL1). Bifogat i detta utskick finns även informationsmaterial för nyanställd. Datorregler godkänds vid lösenordsåterställningen.

Personal eller student (AL2)

Förutsättningarna för att få en AL2 nivå är att innehavaren av ett AL1-klassat konto vid personligt besök uppvisar en giltig identifikationshandling vars information stämmer överens med informationen på kontot. Giltiga identifikationshandlingar är:

- Identitetshandlingar som är godkända för ansökan till svenskt pass eller svenskt nationellt id-kort (enligt krav på punkten 4 i 5.2.5)
- Internationella pass (enligt krav på punkten 5 i 5.2.5)
- EU/EES nationellt id-kort (enligt krav på punkten 5 i 5.2.5)

Endast personal vid servicedesk och särskilt utsedda administratörer med AL2 har rättigheter (administratörskonto) att uppgradera ett användarkonto till AL2. Alla ändringar av AL-nivåer loggas i serviceportalen (5.2.6) och verifieras med engångskod via sms (5.2.8).

För att få tillitsnivå AL2 på digital väg, så verifieras din inloggning mot tjänsten eduId eller svensk e-legitimation LoA3. Fördefinierade identifierare för att knyta person till svensk e-legitimation är:

- Svenskt personnummer (personalIdentityNumber)

eduId-kontot måste uppfylla tillitsnivå AL2 eller AL3. Fördefinierade identifierare för att knyta person till konto från eduId är en av följande:

- Svenskt personnummer (personalIdentityNumber)
- Samordningsnummer (personalIdentityNumber)
- Interim personnummer (norEduPersonNIN)

Personal eller student (eduID AL2 utan svenskt personnummer)

För att få tillitsnivå AL2 på digital väg, så verifieras din inloggning mot tjänsten eduId. eduId-kontot måste uppfylla tillitsnivå AL2. Fördefinierade identifierare som krävs för att knyta person till konto från eduId är:

- Födelsedata (schacDateOfBirth)
- Förnamn (givenName)

- Efternamn (sn)
- E-post (mail)

Kriterierna för att automatiskt godkännas är att:

- födelsedata måste stämma överens (matchning mot samordningsnummer)
- förnamn måste stämma överens (kontrolleras med metoden levenshteinavståndet att max en bokstav är fel)
- efternamnet måste stämma överens (kontrolleras med metoden levenshteinavståndet att max en bokstav är fel)
- e-posten måste stämma överens

Uppfylls inte kraven så blir personen ombedd att lägga ett ärende. Personal vid servicedesk med AL2 rättigheter (administratörskonto) kontrollerar manuellt uppgifterna från den automatiska verifieringen och gör en bedömning att det är samma person och därefter uppgraderar användarkontot till AL2. Fördefinierade identifierare som krävs för att knyta person till konto från eduId är:

- Födelsedata (schacDateOfBirth)
- Förnamn (givenName)
- Efternamn (sn)
- E-post (mail)

Kriterierna för att manuellt godkännas är att:

- födelsedata måste stämma överens (matchning mot samordningsnummer)
- ett av förnamnet stämmer överens när man har flera förnamn (där olika stavningar som ger identiskt eller näst intill identiskt uttal av förnamnet är godkänt)
- efternamnet måste stämma överens (där olika stavningar som ger identiskt eller näst intill identiskt uttal av efternamnet är godkänt)
- e-posten måste stämma överens

Övriga personliga konton

Utöver AL-klassade användarkonton förkommer även personunika gäst- respektive besöks-konton. Dessa konton saknar AL-klassning och har endast begränsad åtkomst på "library-walk-in”-nivå till publika datorer samt mau wi-fi.
Gästkonto skapas av personal eller servicedesk i serviceportalen.

Besökskonto skapas av helpdesk vid uppvisande av ID-handling i serviceportalen.

5.3 Förnyande och åter utfärdande av behörighet *[Credential Renewal and Re-issuing]*

Alla konton kan byta lösenord i serviceportalen (5.3.1). I formuläret där lösenordsändringen sker måste användaren verifiera sitt befintliga lösenord (5.3.2).

Lösenordsåterställning kan begäras från serviceportalen. Nedan följer rutiner för AL1- respektive AL2-konton (5.3.3).

- För konton med AL1 skickas ett e-postmeddelande till användaren med information om att en ändring pågår samt en tidsbegränsad (24h) engångslänk som leder till en sida i serviceportalen där användaren kan ange ett nytt lösenord.

- För konton med AL2 skickas ett e-postmeddelande till användaren med information om att en ändring pågår samt en tidsbegränsad (24h) engångslänk som leder till en sida i serviceportalen där användaren kan ange ett nytt lösenord. I samband med detta skickas även en tidsbegränsad engångskod via sms till användarens mobilnummer som, även den, måste anges i serviceportalen innan ändringen sparas. Användarens konto bibehåller härigenom sin AL2-nivå. Den användare som av olika orsaker inte kan verifiera sitt konto med tidsbegränsad engångskod via sms, men verifierat sin e-post, erbjuds att ändra sitt lösenord med konsekvensen att kontot ändras till AL1-nivå.

Lösenordspolicyn föreskriver minst 8 tecken med komplexitet (5.3.1).

5.4 Återkallande av behörighet *[Credential Revocation]*

Administrativ personal kan inaktivera (5.4.1) alla kontotyper i serviceportalen på förfrågan från användaren själv eller från organisationen. I de fall där åtgärden beror på en säkerhetsincident så informeras användaren om orsaken via telefon eller privat epost-adress. Säkerhetsincidenter följs alltid upp, rapporteras och åtgärdas så att de inte upprepas (5.4.3).

Vid återaktivering (5.4.2) sätts ett för användaren okänt lösenord och användaren tvingas därigenom att använda någon av återställningsmetoderna med e-post och sms (vid AL2) enligt 5.3 för att sätta ett nytt lösenord. Servicedesk och helpdesk kan i särskilda fall vara behjälplig, men i sådana fall sker legitimationskontroll.

5.5 Hantering av behörighetsstatus *[Credential Status Management]*
Alla tilldelade användaridentiteter är registrerade genom sin förekomst i universitetets katalogtjänst (5.5.1).
Alla identiteter sparas i en databas för spårbarhet och återskapning med regeln en identitet per användare (punkt 5.2.4).
Universitetet tillgodoser redundans och beredskap på identitetshanteraren och underliggande system så att kraven på tillgänglighet är uppfyllda (5.5.2).

5.6 Godkännande/validering/autentisering av behörighet
[Credential Validation/Authentication]

Identitetshanteraren är konfigurerad efter SWAMID's rekommendationer (5.6.1) och validerar med lösenordsverifikation (5.6.3) endast aktiva personal-, student- och gäst/besökare konton (5.6.2). Valideringen är giltig i 12 timmar för en tjänst med en *.mau.se/*.mah.se adress (5.6.4).