Mälardalens universitet

Ärendenummer 2022/2594
Datum 2023-09-22

Handläggare
Peter Falck

IT-sektionen

Innehåll

1 Inledning

Detta är Mälardalens universitets (MDU) Identity Management Practice Statement (IMPS), för den svenska akademiska identitetsfederationen SWAMID.

Detta dokument beskriver hur vi uppfyller kraven i SWAMID AL1 och SWAMID AL2

En gång per år ska lärosätet bekräfta för SWAMID att denna IMPS fortfarande är giltig samt delge förändringar till SWAMID.

I resten av detta dokument kommer begreppet *användare* att genomgående användas för att representera medarbetare och studenter.

4 Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1 Svenskt organisationsnummer

Lärosätet har organisationsnummer 202100-2916.

4.1.2 Tillämpbara lagrum

Lärosätet är en statlig utbildningsmyndighet vars verksamhet regleras i lagar, förordningar och regleringsbrev. Verksamhetens arbete har sin grund i regeringsformen (1974:152), tryckfrihetsförordning (949:105), myndighetsförordning (2007:515), högskolelag (1992:1434) och högskoleförordning (1993:100). Regeringen utfärdar årligen regleringsbrev som styr lärosätets uppdrag under ett kalenderår. Som statlig myndighet arbetar lärosätet med ett ledningssystem för informationssäkerhet i enlighet med föreskrifter utfärdade av Myndigheten för samhällsskydd och beredskap. I övrigt följer lärosätet svensk lag och förordning.

Lärosätet har identitets- och behörighetssystem som innehåller personuppgifter om medarbetare och studenter som är verksamma vid lärosätet. Lärosätets behandling av personuppgifter sker i enlighet med gällande dataskyddslagstiftning, såsom den allmänna dataskyddsförordningen (GDPR) och nationell kompletterande lagstiftning, t.ex. Studieregisterförordningen (1993:1153). Lärosätet har även en rutin för att hantera behov av skyddade personuppgifter i enlighet med Offentlighets- och sekretesslagen (2009:400).

4.1.3 Rutiner för destruering av lagringsmedia

När ett system tas ur drift och hårdvara inte ska återanvändas sker fysisk destruering av enheten alternativt att data destrueras genom säker radering med en programvara. Enheter samlas i ett låst utrymme dit endast behörig medarbetare har tillträde. Destruktion/återtag av enheter sker löpande via lärosätets upphandlade avfalls- och återvinningsleverantörer.

Hantering av uppgifter i informationssystem framgår av lärosätets informationshanteringsplan. Uppgifter i informationssystem bevaras eller gallras i

enlighet med lärosätets instruktion för bevarande av elektroniska handlingar samt gällande gallringsbeslut.

4.2 Notices and User Information

4.2.1 Publicering av AUP

Samtliga versioner av AUP finns tillgängliga via https://portal.mdu.se/aup/

4.2.2 Godkännande av AUP

För att få använda IT-resurser på lärosätet och för att få inloggningsuppgifter måste användaren godkänna en AUP. Godkännandet sker i samband med att användaren får sina inloggningsuppgifter.

4.2.3 Kräva nytt godkännande när AUP modifieras

Om det sker förändringar av en AUP måste samtliga befintliga användare godkänna den nya AUP:n för att få fortsätta använda IT-resurserna. Det görs i en webbapplikation där användarna själva loggar in och godkänner den nya AUP:n.

Efter publicering av ny AUP och information om det har gått ut till användaren har användaren en viss tid på sig att godkänna den nya AUP:n. Om den inte godkänns inom denna tid kommer inloggningsuppgifterna att återkallas.

4.2.4 Lagra godkännande av AUP

Godkännande av AUP, samt information om när den har godkänts, lagras per användare i en databas.

4.2.5 Publicera IDP Service Definition

Service definition/tjänstebeskrivningen finns publicerad på lärosätets IDP och därmed tillgänglig för alla vid inloggning. Tjänstebeskrivningen nås även via följande länk: https://idp.mdh.se/idp.html

4.3 Secure Communications

4.3.1 Skydda hemligheter

Lärosätet använder Microsofts Active Directory för att lagra inloggningsuppgifter.

All kommunikation till och från servrar som ingår i identitets- och behörighetssystemet är krypterad enligt standardprotokoll.

Administratörsrättigheter tilldelas enbart de medarbetare på MDU som har ett behov av detta i sin roll som systemadministratör. Om arbetsuppgifterna ändras tas administratörsrättigheterna bort.

4.3.2 Skydda privata nycklar

Nycklar och lösenordsfiler skyddas med behörighetskontroll i filsystem.

4.3.3 Säker och krypterad kommunikation

All kommunikation till och från servrar som ingår i identitets- och behörighetssystemet är krypterad med TLS.

4.3.4 Entitetnycklar

Alla nycklar som används av IDP är minst 2048 bitar.

4.4 Security-relevant Event (Audit) Records

4.4.1 Loggning av säkerhetsrelaterade händelser

Säkerhetsrelaterade händelser i lärosätets identitets- och behörighetssystem loggas och enbart behörig systemadministratör kan vid behov komma åt loggarna.

5 Operational Requirements

5.1 Credential Operating Environment

5.1.1 Autentisering

Inloggning sker med enfaktorsinloggning mot Active Directory. Lösenordet måste följa lärosätets gällande lösenordspolicy:

- Minst 8 tecken långt
- Max 20 tecken långt
- Minst en liten bokstav (a-z)
- Minst en stor bokstav (A-Z)
- Minst en siffra (0-9)
- Lösenordet får inte vara ditt användar-id, eget förnamn eller eget efternamn

5.1.2 Skydd av protokoll

All kommunikation mellan de olika delar som används för hantering av användare och lösenord sker krypterat som beskrivs under rubriken 4.3.3. TLS har inbyggt skydd mot message replay.

5.1.3 Skydd mot missbruk av inloggningsuppgifter

Vår AUP för användare förbjuder återanvändning av lösenord i andra system samt delning av inloggningsuppgifter.

5.1.4 Hantering av systemhot

Omvärldsbevakning av systemhot sker dagligen och patchning av system sker när säkerhetsuppdateringar släpps.

5.2 Credential Issuing

5.2.1 Identitetshanterarens DNS-domän

Lärosätet använder sig av domänerna mdu.se och mdh.se

5.2.2 Unik IDP enhetsidentifierare

Vår IDP har entitetsid https://idp.mdh.se/idp/shibboleth

5.2.3 Unik användaridentitet

Användaridentiteter är unika, personliga och återanvänds ej.

5.2.4 Val av användaridentitet vid inloggning

Om användaren har flera användaridentiteter så väljer den själv vilken användaridentitet den loggar in med.

5.2.5 Säkerställ identitet vid utlämnande av inloggningsuppgifter

Följande metoder från SWAMID:s Identity Assurance Profiles får användas för identifiering:

- AL2 metod 1 enligt 5.2.5. Online med SWAMID Identity Assurance Level 2 eller högre
- AL2 metod 2 enligt 5.2.5. Online med svensk e-legitimation Level of Assurance 3 eller högre
- AL2 metod 4 enligt 5.2.5. På plats med svensk identitetshandling. Vi accepterar identitetshandlingar som finns på polisens godkända lista för uthämtning av svenskt pass.
- AL2 metod 5 enligt 5.2.5. På plats med utländsk identitetshandling. Vi accepterar utländskt pass som uppfyller ICAO Doc 9303 samt EU/EES nationellt ID-kort som uppfyller European Commission Regulation 562/2006
- AL1 metod 4 enligt 5.2.5. Online med engångslösenord som skickas till förregistrerad e-postadress i kombination med CAPTCHA
- AL1 metod 7 enligt 5.2.5. Digitalt möte på distans med svensk eller utländsk identitetshandling, enligt AL2 metod 4, respektive AL2 metod 5

Assurance Level sätts baserat på den identifieringsmetod som används.

Studenter

AL2 metod 1 och 2. Onlineidentifiering

Inloggningsuppgifter hämtas ut i en självbetjäningstjänst online. Användaren anger själv sitt önskade lösenord. Förregistrerad identifierare är personnummer eller interimspersonnummer från LADOK.

AL2 metod 4. Svensk identitetshandling

Överlämning av ett engångslösenord från kontoadministratör vid lärosätet, efter identitetskontroll. Engångslösenordet används tillsammans med personnummer för att hämta ut inloggningsuppgifter i en självbetjäningstjänst online. Förregistrerad identifierare är personnummer från LADOK.

AL2 metod 5. Utländsk identitetshandling

Samma rutin som för användare med svensk identitetshandling. Förregistrerad identifierare är interimspersonnummer, kombinerat med namn från LADOK.

Dessutom sparar kontoadministratören namn, födelsedatum, utfärdandeland och identitetshandlingsnummer i en förteckning. Denna information används för att säkerställa senare identifiering enligt avsnitt 5.3.3 och 5.4.2.

AL1 metod 4. Engångslösenord som skickas till en förregistrerad e-postadress i kombination med CAPTCHA

Utlämning av inloggningsuppgifter kan ske med hjälp av ett engångslösenord som skickas till den förregistrerade e-postadressen (identifierare), som angavs i samband med anmälan till utbildningen, t.ex. på universityadmissions.se eller i mobilitetssystemet MoveOn. Engångslösenordet beställs från en kontoadministratör och används sedan i en självbetjäningstjänst online.

AL1 metod 7. Digitalt möte på distans i kombination med identitetshandling

Användare som av någon anledning inte kan infinna sig på lärosätet fysiskt, eller inte kan använda någon av ovanstående metoder, kan boka ett Zoom-möte med en kontoadministratör vid lärosätet.

Samma rutin för identitetshandlingar och förregistrerade identifierare som används i AL2 metod 4 och 5, men kontoadministratören lämnar ut ett engångslösenord till användaren. Engångslösenordet delas via Zoom. Engångslösenordet används sedan av användaren i en självbetjäningstjänst online.

Medarbetare

AL2 metod 4. Svensk identitetshandling

Användaren går till en kontoadministratör för att hämta sina inloggningsuppgifter. Användaren visar upp identitetshandling och vi delar ut inloggningsuppgifter via en intern webbapplikation. Det tillfälliga lösenordet måste bytas första gången användaren loggar in. Förregistrerad identifierare är personnummer från MDU HR-system.

AL2 metod 5. Utländsk identitetshandling

Samma rutin som för användare med svensk identitetshandling. Förregistrerad identifierare är personnummer, samordningsnummer eller interimspersonnummer samt namn från MDU HR-system.

Dessutom sparar kontoadministratören namn, födelsedata, utfärdandeland och passnummer. Denna information används för att säkerställa senare identifiering enligt avsnitt 5.3.3 och 5.4.2.

AL1 metod 7. Digitalt möte på distans i kombination med identitetshandling

Användare som av någon anledning inte kan infinna sig på lärosätet fysiskt, eller inte kan använda någon av ovanstående metoder, kan boka ett Zoom-möte med en kontoadministratör vid lärosätet.

Samma rutin för identifiering och förregistrerade identifierare som för AL2 metod 4 och 5, men kontoadministratören lämnar ut ett engångslösenord till användaren. Engångslösenordet delas via Zoom. Engångslösenordet används sedan av användaren i en självbetjäningstjänst online.

5.2.6 Register över ändrad AL-nivå för användare

Alla händelser som rör förändring av AL-nivåer loggas. Sådana loggar gallras enligt gällande gallringsbeslut.

5.2.7 Uppdatera angiven information

En användare kan ändra alla uppgifter som den angivit om sig själv.

5.2.8 Krav på kontoadministratör som lämnar ut inloggningsuppgifter

Alla kontoadministratörer som genomför identitetskontroll och lämnar ut inloggningsuppgifter är verifierade för samma eller högre AL-nivå som inloggningsuppgifterna som lämnas ut.

5.3 Credential Renewal and Re-issuing

5.3.1 Tillåt byte av lösenord (renew)

Alla användare kan och har rätt att byta sitt lösenord, förutom när inloggningsuppgifterna är inaktiverade eller återkallade.

5.3.2 Kräv gammalt lösenord vid byte av lösenord (renew)

När en användare byter sitt lösenord måste användaren först ange det gamla lösenordet. Det nya lösenordet måste uppfylla kraven i avsnitt 5.1.1 ovan.

5.3.3 Utlämning av inloggningsuppgifter vid glömt lösenord (re-issuing)

Assurance Level sätts baserat på den identifieringsmetod som används.

Studenter

AL2 metod 1 och 2. Onlineidentifiering
Samma rutin som i 5.2.5.

AL2 metod 4. Svensk identitetshandling
Samma rutin som i 5.2.5.

AL2 metod 5. Utländsk identitetshandling
Samma rutin som i 5.2.5.

Dessutom måste användaren visa upp samma identitetshandling, som visades upp vid första utlämnandet av inloggningsuppgifter, eller en identitetshandling med samma namn, födelsedatum och utfärdandeland.

AL1 metod 4. Engångslösenord som skickas till en förregistrerad e-postadress i kombination med CAPTCHA
Utlämning av inloggningsuppgifter kan ske med hjälp av ett engångslösenord som skickas till den e-postadress, som angavs i samband med utlämnandet av inloggningsuppgifterna. Självbetjäningstjänst online.

AL1 metod 7. Digitalt möte på distans i kombination med identitetshandling
Samma rutin som i 5.2.5.

Medarbetare

AL2 metod 4. Svensk identitetshandling
Samma rutin som i 5.2.5.

AL2 metod 5. Utländsk identitetshandling
Samma rutin som i 5.2.5.

Dessutom måste användaren visa upp samma identitetshandling, som visades upp vid första utlämnandet av inloggningsuppgifter, eller en identitetshandling med samma namn, födelsedatum och utfärdandeland.

AL1 metod 7. Digitalt möte på distans i kombination med identitetshandling
Samma rutin som i 5.2.5.

5.4 Credential Revocation

5.4.1 Återkalla inloggningsuppgifter (revoke credentials)

Vid behov kan inloggningsuppgifter återkallas. Detta kan göras omedelbart om ärendet är brådskande.

När en medarbetares sista kvarvarande anställning eller uppdrag avslutas så återkallas inloggningsuppgifterna automatiskt.

Inloggningsuppgifter för studenter gallras med automatik fyra terminer efter senaste registrering på utbildning i LADOK.

Inloggningsuppgifter kan återkallas på begäran av innehavaren av inloggningsuppgifterna.

5.4.2 Utlämning av inloggningsuppgifter efter återkallning

IT-sektionen ansvarar för kontakt med användare efter att deras inloggningsuppgifter har återkallats. Vid denna kontakt får användaren veta anledningen till att inloggningsuppgifterna har återkallats.

Processen för att återfå sina inloggningsuppgifter efter att de har återkallats genomförs utan systemstöd. Nedanstående identifieringsmetoder används. Assurance Level sätts baserat på den identifieringsmetod som används.

AL2 metod 4. Svensk identitetshandling
Samma rutin som i 5.3.3.

AL2 metod 5. Utländsk identitetshandling
Samma rutin som i 5.3.3.

AL1 metod 7. Digitalt möte på distans i kombination med identitetshandling
Samma rutin som i 5.3.3.

5.4.3 Återkalla inloggningsuppgifter pga säkerhetsrelaterad incident

Lärosätet hanterar säkerhetsincidenter, baserat på MSB/CERT-SE:s incidenthanteringsprocess (CIHSP). Denna process innehåller erfarenhetsåterföring och används vid allvarliga incidenter samt säkerställer att lärosätet i framtiden förebygger motsvarande typer av incidenter.

IT-sektionen samtalar med den drabbade användaren efter att en incident har skett i syfte att minimera risken för att liknande incidenter inträffar igen. Gällande medarbetare kan kontakt också tas med ansvarig chef och HR-sektionen.

CSIRT på lärosätet ansvarar för att utredning av möjliga incidenter genomförs samt att eventuella åtgärder vidtas.

5.5 Credential Status Management

5.5.1 Ha ett register över alla utlämnade inloggningsuppgifter

Loggning av alla händelser som rör utlämnade av inloggningsuppgifter sker i respektive applikation. Lösenordsförändringar loggas till syslog. Loggarna gallras enligt gällande gallringsbeslut.
Vi sparar användarid för samtliga utdelade inloggningsuppgifter för att säkerställa att de inte återanvänds.

5.5.2 Tillgänglighet för IDP

Tillgängligheten på IDP och underliggande system bedöms tillräcklig för att uppfylla lärosätets krav.

5.6 Credential Validation/Authentication

5.6.1 Validering av inloggningsuppgifter

Lärosätet använder Shibboleth Identity Provider som har inbyggt stöd för protokollen som det ställs krav på i avsnitt 5.6.1. Lärosätet har implementerat samtliga tekniska protokoll enligt SWAMIDs rekommenderade best practice.

5.6.2 Tillåt inte inloggning med återkallade inloggningsuppgifter (inaktiverade inloggningsuppgifter)

Inloggning kan ej ske om inloggningsuppgifterna är återkallade.

5.6.3 Kräv lösenord vid inloggning

Aktuella inloggningsuppgifter måste fyllas i vid inloggning.

5.6.4 Kräv inloggning minst var 12:e timme

Inloggning krävs 1 gång i timmen.