Mälardalens universitet

Ärendenummer 2022/2594
Datum 2022-11-08

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 universitetets rutiner för att hantera digitala identiteter. Universitetet har som mål att, beroende på användarkategori, uppfylla kraven för Identity Assurance Level 1 och Identity Assurance Level 2.

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

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

4 Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1 Svenskt organisationsnummer

Mälardalens universitet har organisationsnummer 202100-2916.

4.1.2 Tillämpbara lagrum

Mälardalens universitet (MDU) 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 universitetets 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. Universitetets behandling av personuppgifter sker i enlighet med gällande dataskyddslagstiftning, såsom den allmänna dataskyddsförordningen (GDPR) och nationell kompletterande lagstiftning, t.ex. Studieregisterförordningen (1993:1153). Universitetet 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 universitetets upphandlade avfalls- och återvinningsleverantörer.

Hantering av uppgifter i informationssystem framgår av universitetets informationshanteringsplan. Uppgifter i informationssystem bevaras eller gallras i enlighet med universitetets 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 MDU och för att få inloggningsuppgifter måste personen godkänna en AUP. Godkännandet sker i samband med att personen 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 https://portal.mdu.se/aup/

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 MDU:s IDP och därmed tillgänglig för alla vid inloggning. Tjänstebeskrivningen nås även via följande länk: https://idp.mdh.se/idp.html

4.3 Secure Communications

This subsection defines how clear text passwords, private keys and shared secrets must be protected to obtain operational security.

4.3.1 Skydda hemligheter

Mälardalens universitet 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 universitetets 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 universitetets 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 medarbetare förbjuder återanvändning av lösenord i andra system samt delning av inloggningsuppgifter. Vår AUP för studenter förbjuder delning av inloggningsuppgifter. Studenter får AL1.

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

Mälardalens universitet 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

Vid granskning av id-handling accepteras följande typer:

- Godkänd svensk ID-handling (SIS-märkt ID-kort, körkort)
- Svenskt nationellt ID-kort eller pass
- Utländskt pass som uppfyller ICAO Doc 9303
- EU/EES nationellt ID-kort som uppfyller European Commission Regulation 562/2006

För studenter skapas inloggningsuppgifter med AL1

Inloggningsuppgifter hämtas ut av studenter på följande sätt:
1 Via autentisering mot antagning.se (självbetjäningstjänst via webbgränssnitt)

2 Via beställning av ett temporärt lösenord som skickas till folkbokföringsadress, (självbetjäningstjänst via webbgränssnitt) som sedan används tillsammans med personnummer för att hämta ut inloggningsuppgifter.

3 Via överlämning av ett temporärt lösenord från medarbetare vid universitetet, efter identitetskontroll. Det temporära lösenordet används tillsammans med personnummer för att hämta ut inloggningsuppgifter.

Efter autentisering, med hjälp av federerad inloggning eller temporärt lösenord tillsammans med personnummer, kan studenten, via självbetjäningstjänst i ett webbgränssnitt, skapa inloggningsuppgifter.

För medarbetare

Medarbetare som blir identifierade enligt metod 4och 5 nedan får AL2.

Medarbetare som blir identifierade enligt metod 8 nedan får AL1.

Metod 4. Medarbetare med svensk id-handling
Medarbetaren går till studenttorget för att hämta sina inloggningsuppgifter. Medarbetaren visar upp id-handling och vi delar ut inloggningsuppgifter via en intern webbapplikation. Medarbetaren får läsa igenom och godkänna universitetets AUP

genom att bocka i en ruta direkt på webbsidan. Godkännandet lagras digitalt. Vi skriver därefter ut en sida som innehåller AUP och inloggningsuppgifter och ger till medarbetaren. Det nya tillfälliga lösenordet måste bytas till något personligt första gången medarbetaren loggar in.

Metod 5. Medarbetare med utländsk id-handling
Samma rutin gäller som för medarbetare med svensk id-handling. Utöver det sparar Studenttorget namn, födelsedata, utfärdandeland och passnummer. Denna information används för att säkerställa senare identifiering enligt avsnitt 5.3.3.

Metod 8. Distans
Medarbetare som av någon anledning inte kan infinna sig på universitetet fysiskt kan boka ett Zoom-möte med Studenttorget. Samma rutin som ovan används men medarbetare på Studenttorget bockar i rutan för godkännande av AUP på uppdrag av medarbetaren. Inloggningsuppgifterna delas via Zoom.

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 person kan ändra alla uppgifter som den angivit om sig själv.

5.2.8 Krav på medarbetare som lämnar ut inloggningsuppgifter

Alla medarbetare 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 person byter sitt lösenord måste personen 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)

För studenter

Utlämning av inloggningsuppgifter vid glömt lösenord sker med hjälp av ett temporärt lösenord som skickas via SMS eller e-post till ett av studenten angivet telefonnummer eller e-postadress, som angavs i samband med utlämnandet av inloggningsuppgifterna. Vid återställning av lösenordet sätts AL1.

För medarbetare

Utlämning av inloggningsuppgifter vid glömt lösenord sker enligt någon av följande metoder. För medarbetare sätts AL2 vid metod 4 och 5, eller AL1 vid metod 8.

Metod 4. Medarbetare med svensk id-handling
För medarbetare med svensk id-handling sker utlämning av inloggningsuppgifter på samma sätt som beskrivs under avsnitt 5.2.5 ovan.

Metod 5. Medarbetare med utländsk id-handling
För medarbetare med utländsk id-handling sker utlämning av inloggningsuppgifter på samma sätt som beskrivs under avsnitt 5.2.5. Dessutom måste medarbetaren visa upp samma id-handling, som visades upp vid första utlämnandet av inloggningsuppgifter, eller en id-handling med samma namn, födelsedatum och utfärdandeland. För att kunna kontrollera detta underhåller Studenttorget en förteckning över namn, födelsedatum, utfärdandeland och id-handlingsnummer för medarbetare som saknar svenskt personnummer.

Metod 8. Distans
Medarbetare som av någon anledning inte kan befinna sig på universitetet fysiskt kan boka ett Zoom-möte med studenttorget för att visa upp sin id-handling. Samma rutiner som beskrivs ovan i detta avsnitt tillämpas. Inloggningsuppgifterna delas via Zoom.

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 när tidsgräns om fyra terminer, utan aktiv registrering på program eller kurs i LADOK, passerats.

Inloggningsuppgifter kan återkallas på begäran av innehavaren av inloggningsuppgifterna.

5.4.2 Utlämning av inloggningsuppgifter efter återkallning

IT-sektionen vid Mälardalens universitet ansvarar för kontakt med personer efter att inloggningsuppgifter har återkallats. Vid denna kontakt får personen information gällande anledningen till att inloggningsuppgifterna har återkallats.

För studenter

Student som fått återkallade inloggningsuppgifter måste sätta om sitt lösenord med ett temporärt lösenord som skickas per SMS eller e-post.

AL-nivå som sätts är AL1.

För medarbetare

För medarbetare används samma metoder som i avsnitt 5.3.3. AL-nivå som sätts är AL2 för metod 4 och 5 eller AL1 för metod 8.

5.4.3 Återkalla inloggningsuppgifter pga säkerhetsrelaterad incident

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

IT-sektionen samtalar med den drabbade personen 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 MDU 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 universitetets krav.

5.6 Credential Validation/Authentication

5.6.1 Validering av inloggningsuppgifter

MDU använder Shibboleth Identity Provider som har inbyggt stöd för protokollen som det ställs krav på i avsnitt 5.6.1. MDU 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.