1 Inledning

Detta dokument är Örebro universitets Identity Management Practice Statement (IMPS), för den svenska akademiska identitetsfederationen SWAMID. Detta dokument beskriver Örebro universitets rutiner för att hantera digitala identiteter enligt SWAMID:s tillitsprofiler 1, 2 och 3.

4 Organisational Requirement

4.1 Enterprise and Service Maturity

Örebro universitet, organisationsnummer 202100-2924, är en statlig utbildningsmyndighet vilket gör att lärosätets 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 innehåller uppgifter om organisationen samt personuppgifter om alla som är verksamma vid lärosätet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas. Dataskyddsförordningen och offentlighets- och sekretesslag (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok och därför gäller även förordning (SFS 1993:1153) om redovisning av studier med mera vid universitet och högskolor för hanteringen av studenters personuppgifter i Ladok.

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (Främst MSBFS 2020:6 och MSBFS 2020:7).

Data lagras, gallras och raderas i enlighet med fastställd informationshanteringsplan. Utrangerad lagringsmedia samlas i låst och larmat utrymme innan de förstörs fysiskt av universitetets upphandlade avfalls- och återvinningsföretag.

4.2 Notices and User Information

Örebro universitet har centrala policys och riktlinjer som beskriver hur information får hanteras och vilka regler användarna måste förhålla sig till. De består bland annat av informationssäkerhetspolicy, lösenordspolicy och riktlinjer för användning av IT-resurser vid Örebro universitet.

https://www.oru.se/globalassets/inforum-sv/centrala-dokument/styrdokument/kommunikation_it/it/informationssakerhetspolicy-for-orebro-universitet.pdf

För att få använda IT-resurserna måste användaren godkänna en ansvarsförbindelse där man förbinder sig att följa riktlinjer för användning av IT-resurser vid Örebro universitet.
https://www.oru.se/om-universitetet/mitt-konto/ansvarsforbindelse-for-anvandning-av-it-tjanster-och-it-utrustning-vid-orebro-universitet/anvandning-av-it-tjanster/

När användaren loggar in första gången så får de upp ansvarsförbindelsen och godkänner den genom att kryssa i en kryssruta. När de sedan trycker ok så får de göra en inloggning för att säkerställa att det är rätt person som godkänner den.

https://www.oru.se/om-universitetet/mitt-konto/ansvarsforbindelse-for-anvandning-av-it-tjanster-och-it-utrustning-vid-orebro-universitet/

Om det sker förändringar av ansvarsförbindelsen måste användarna godkänna den på nytt för att få fortsätta använda IT-resurserna. Information att detta är gjort och när det är gjort sparas sedan i katalog- och behörighetssystem.

Beskrivningen av identitetstjänsten finns på:
https://www.oru.se/om-universitetet/mitt-konto/swamid-tjanstebeskrivning/

4.3 Secure Communications

För att säkerställa att endast behörig personal har tillgång till gemensamma lösenord och privata nycklar lagras dessa skyddade på följande sätt.

Gemensamma lösenord, till exempel administratörskonton, lagras i ett lokalt lösenordshanteringssystem som endast nås från det interna nätet och efter två autentiseringar med olika konton, så kallad bruten SSO. Endast behörig driftspersonal har åtkomst.

Privata nycklar finns endast konfigurerade i de system som nyttjar dessa och finns då endast i applikationerna eller skyddade med behörigheter på filstruktur.

Samtlig kommunikation mellan ingående system är krypterad. Om ett system inte har stöd för kryptering så används stunnel för att säkerställa att informationen går krypterad över nätverket.

Minsta längd på IdP-nycklarna för servrar som hanterar autentisering är 2048 bitar.

4.4 Security-relevant Event (Audit) Records

Samtliga säkerhetshändelser från relevanta system loggas lokalt och i vissa fall även till central loggserver och lagras minst 6 månader. Detta inkluderar lyckade och misslyckade inloggningsförsök.
Samtliga servrar och nätverksutrustning synkroniserar sin tid mot en central NTP-källa.
Lokalt används ntp.oru.se som är fullt redundant och som i sin tur hämtar tid från ntp.se (www.ntp.se)

5 Operational Requirements

5.1 Credential Operating Environment

Örebro universitet har stöd för autentisering på samtliga AL nivåer. Vid AL1 och AL2 sker autentisering med en single-factor – lösenord. Lösenordskravet är konstruerad ett premiera långa lösenord/fraser som i sin tur minskar kravet på att använda tecken från alla 4 kategorier. Gällande regelverk ger en entropi på minst 19 bitar enligt universitetets lösenordspolicy vilket ger en entropi på motsvarande minst 24 bitar enligt NIST.

Vid AL3 sker autentisering med svensk e-legitimation på lägst nivå LoA3.

De protokoll som används vid autentisering bygger på sessioner enligt SWAMID SAML WebSSO Technology Profile.

Regelverket för lösenord finns beskrivet i lösenordspolicyn som finns publicerad tillsammans med övriga styrdokument. Det finns även regler i riktlinjer för användning av IT-resurser som beskriver att det inte är tillåtet att lämna ut sina inloggningsuppgifter.

Vid införande av nya och vid större förändring av befintliga system genomförs en riskanalys. Den ligger sedan till grund för åtgärder som behöver genomföras för att hantera eventuella säkerhetshot. För befintliga system sker både proaktiva och reaktiva åtgärder:

- Sårbarhetsscanning av externa gränssnitt
- Säkerhetsuppdatering av befintliga system sker enligt en fastställd process
- Verktyg för skadlig kod finns installerat både på klienter och servrar men även på delade lagringsplatser. Mitigering är automatiserad enligt leverantörernas Best Practice och som eskalering sker larm till övervakningsverktyg.

5.2 Credential Issuing

ORU-kontos användarnamn genereras och kombineras med vårt domännamn. Denna kombination används som eduPersonPrincipalName och är unikt och återanvänds aldrig till en ny identitet. Örebro universitets identity provider har globalt unik identifierare (entityID) som finns under DNS-domänen oru.se.

Alla konton är unika och består av användarnamn följt av oru.se i federerade tjänster.

Om ett användarnamn har använts så får det inte återanvändas, detta för att spårbarheten ska vara god samt för att kontot ska kunna återaktiveras vid ett senare tillfälle.

Om användaren har flera roller i ett system, kan användaren välja vilken roll som hen ska logga in med i samband med autentiseringen.

Vid granskning av legitimation för både anställda och studenter, 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

Det finns intern dokumentation som utbildade medarbetare använder för verifiering av legitimationen. Den beskriver processen för att verifiera en ID-handling, vilka ID-handlingar som accepteras och länkar till externa sajter för hjälp med verifiering (till exempel PRADO).

Användare uppfyller olika tillitsnivåer, inloggningstjänsten kan via attributrelease signalera till aktuell tjänst vilken tillitsnivå som användaren har.

Ändringar av tillitsnivån på ett ORU-konto loggas i katalog- och behörighetssystemet samt i den applikation som utfört ändringen. I loggen sparas vilken typ av legitimation som använts.

Alla som har ett ORU-konto har möjlighet att uppdatera sina egenuppgivna uppgifter. För studenter sker detta via Ladok. För personal och samarbetspartner sker det via olika gränssnitt, via Avdelningen för digitalisering och IT eller via HR-avdelningen. All personal vid Örebro universitet som har rätt att administrera ORU-konto använder själv ett ORU-konto på minst samma nivå som ORU-kontot som ska administreras. Detta säkerställs av de administrativa verktyg som används för kontohantering.

ORU-konto Anställd

En anställds ORU-konto skapas utifrån en beställning från en behörig beställare. Behörig beställare anger personuppgifter i ett beställningsformulär. Konto skapas av IT-support utifrån beställningen. Vilken AL-nivå som sätts för ett nytt ORU-konto beror på vilken metod för utlämning av användaruppgifter som används:

1. Inloggningsuppgifter skickas i förslutet kuvert till beställaren via internpost. Beställaren förmedlar uppgifterna via de etablerade kontaktuppgifter som upparbetats. CAPTCHA finns då användaren accepterar ansvarsförbindelsen. Denna metod ger AL1.
2. Inloggningsuppgifter skickas i förslutet kuvert till användarens folkbokföringsadress. Inloggningsuppgifterna är tidsbegränsade. Denna metod ger AL2.
3. Inloggningsuppgifterna överlämnas personligen till användaren efter legitimering enligt fastställd rutin. För de som har svenskt personnummer är detta identifieraren. För de som inte har svenskt personnummer används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare. Denna metod ger AL2.

Användaren aktiverar sedan sitt ORU-konto genom sin första inloggning. I samband med inloggningen sker godkännande av ansvarsförbindelse och ett tvingande lösenordsbyte.

En anställd kan höja sin AL-nivå på befintligt ORU-konto från AL1 till AL2 genom legitimering enligt fastställd rutin. För de som har svenskt personnummer är detta identifieraren. För de som inte har svenskt personnummer används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare.

En anställd kan höja sin AL-nivå på befintligt ORU-konto från AL1 eller AL2 till AL3 genom att koppla ihop sitt ORU-konto med en svensk e-legitimation på lägst nivå LoA3 på sidan https://www.oru.se/om-universitetet/mitt-konto/

Systemet kontrollerar personnumret från den lokala identity providern mot personnumret från e-legitimationens inloggning. Under förutsättning att dessa matchar, så tillåts användaren koppla ihop sitt ORU-konto med sin e-legitimation. För AL3 är personnumret identifieraren. En anställd kan därefter autentisera sig på AL2-nivå med endast lösenord eller på AL3-nivå med e-legitimation på lägst LoA3.

ORU-konto Student

En antagen students ORU-konto skapas på något av följande sätt:

1. För studenter med svenskt personnummer är personnumret identifieraren.
   Konton skapas i förväg utifrån Ladokhändelse antagningsomgång 2. Studenten kan sedan aktivera sitt konto via autentisering hos antagning.se, eduID, e-legitimation på lägst LoA3 eller tidsbegränsad engångskod som skickas till folkbokföringsadress. Denna metod ger AL2.

   Om aktivering sker via antagning.se eller eduID kontrolleras att studenten (via assurance-attributet) och IdP:n (i metadata) uppfyller SWAMID AL2.
   Denna metod ger AL2 under förutsättning att kontrollen stämmer. Annars ger metoden AL1.

2. För studenter utan svenskt personnummer används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare.
   Konton skapas i förväg utifrån Ladokhändelse antagningsomgång 2. Studenten kan sedan aktivera sitt konto med aktiveringsnyckel som överlämnas vid registreringstillfället mot

uppvisande av godkänd identitetshandling. Denna metod ger den AL-nivå som förmedlas av antagning.se (AL2 eller AL1).

3. Samtliga studenter.
   Tidsbegränsad engångskod skickas via post till postadress som finns i Ladok. Denna metod ger AL1.
4. Samtliga studenter.
   Tidsbegränsad engångskod skickas via e-post till e-postadressen som finns i Ladok.
   CAPTCHA finns då användaren accepterar ansvarsförbindelsen. Denna metod ger AL1.

En student kan höja sin AL-nivå på befintligt ORU-konto från AL1 till AL2 genom legitimering enligt fastställd rutin. För de som har svenskt personnummer är detta identifieraren. För de som inte har svenskt personnummer används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare.

En student kan höja sin AL-nivå på befintligt ORU-konto från AL2 till AL3 genom att koppla ihop sitt ORU-konto med en svensk e-legitimation på lägst nivå LoA3 på sidan https://www.oru.se/om-universitetet/mitt-konto/

Systemet kontrollerar personnumret från den lokala identity providern mot personnumret från e-legitimationens inloggning. Under förutsättning att dessa matchar, så tillåts användaren koppla ihop sitt ORU-konto med sin e-legitimation. För AL3 är personnumret identifieraren. En student kan därefter autentisera sig på AL2-nivå med endast lösenord eller på AL3-nivå med e-legitimation.

ORU-externkonto
En samarbetspartner följer samma regelverk som anställda men har initialt inga behörigheter. De får enbart tillgång till de specifika system som de behöver.

ORU-externkonto kan beställas av anställd personal. Kontouppgift till användaren skickas med epost. Lösenord skickas med SMS. Denna metod ger AL1.

En extern användare kan själv skapa ett behörighetslöst ORU-externkonto på https://www.oru.se/om-universitetet/mitt-konto/ med hjälp av e-legitimation på lägst nivå LoA3. Inloggningsuppgifter kommuniceras inte. Denna metod ger AL3.

CAPTCHA finns då användaren accepterar ansvarsförbindelsen.

5.3 Credential Renewal and Re-issuing

Alla användare kan byta sitt lösenord i Microsoftportalen efter autentisering. Användare kan dessutom byta lösenord via en intern tjänst.

Vid lösenordsbyte måste det gamla lösenordet anges.

För att påtvinga lösenordsbyte, byts lösenordet till ett för användaren okänt värde och därmed tvingas användaren att igenom återställningsprocessen.

ORU-konto Anställd och ORU-externkonto

Om användaren har glömt bort sitt lösenord eller om kontot har blivit spärrat av någon anledning kommer kontot att nedgraderas till AL1 och användaren måste använda en av följande metoder för att återaktivera sitt ORU-konto.

1. Via videomöte med kontroll av personnummer eller kombination av passnummer, namn, nationalitet och födelsedata mot registrerade uppgifter för att säkerställa att det är samma individ. Denna metod ger AL1.
2. Legitimering sig hos IT-support med kontroll av personnummer eller kombination av passnummer, namn, nationalitet och födelsedata mot registrerade uppgifter för att säkerställa att det är samma individ. Denna metod ger AL2 eller AL3 (om användaren tidigare var på nivån AL3).
3. Om användaren inte kan ta sig till Campus Örebro kommer en tidsbegränsad engångskod skickas ut via vanligt brev till folkbokföringsadress. Denna metod ger AL2. För att eventuellt återfå AL3 igen måste användaren antingen besöka IT-support eller något av de dedikerade ombuden för en identitetskontroll eller återkoppla kontot med sin e-legitimation.
4. Via förregistrerade alternativa kontaktuppgifter. Användaren går till sin personliga återställningssida och initierar lösenordsåterställning. Då skickas en tidsbegränsad engångskod en av de förregistrerade uppgifterna. Ingen legitimering sker. Denna metod ger AL1.

ORU-konto Student

Studenter som behöver ett nytt lösenord gör en återställning via inloggning mot antagning.se, eduID eller via tidsbegränsad engångskod som antingen skickas till folkbokföringsadressen eller överlämnas fysiskt i Studentcentrum efter legitimationskontroll. Det sker en kontroll av gällande AL-nivå och att personnummer matchar. Denna metod ger AL2.

För studenter utan svenskt personnummer gäller i första hand metoden engångskod som överlämnas i studentcentrum mot uppvisande av godkänd identitetshandling som matchas mot registrerad identifierare. Denna metod ger AL2.

Samtliga studenter kan också få en tidsbegränsad engångskod skickad till den e-postadressen som finns registrerad i Ladok enligt samma tillvägagångssätt som beskrivs i avsnitt 5.2. Denna metod ger AL1.

5.4 Credential Revocation

Konton kan vid behov spärras i Örebro universitets centrala identitetskatalog.

- Om kontot behöver spärras på användarens initiativ vänder sig denne till IT-support.
- Om kontot spärras med anledning av en incident kommer IT-support att söka användaren för att informera om situationen.

För återaktivering av konto gäller följande:

- Användaren måste besöka IT-support och uppvisa godkänd id-handling för matchning av förregistrerad identifierare.
- Vid återaktivering kommer användaren att erhålla nytt lösenord.

Om revokering av användaruppgifter har skett efter en säkerhetsincident kommer en orsaksanalys utförd av ORU CERT att besluta om vilka åtgärder som ska vidtas för att minska risken för att motsvarande händelse sker igen.

ORU-konto Anställd

ORU-konto Anställd övervakas dagligen av en automatiserad underhållsprocess. Underhållsprocessen undersöker tillståndet på två parametrar, synkroniseringsdatum med HR-systemet samt kontots

slutdatum. För personal med tillsvidare- eller tidsbegränsad anställning uppdateras synkroniseringsdatum på kontot varje dag under anställningsperioden.

För timanställd eller annan typ av förhållande, till exempel gästlärare mm, saknas synkroniseringsdatum.

Underhållsprocessen tittar i första hand på synkroniseringsdatum. Om synkroniseringsdatum är dagens datum betraktas kontot som fortsatt aktivt. Om inte, eller om synkroniseringsdatum saknas, kontrolleras kontots slutdatum. Om även detta datum passerats skapas ett ärende i ärendehanteringssystemet samt att en förfrågan skickas ut till berörd avdelning/institution. Utifrån avdelning/institutions bedömning kommer kontot att avslutas eller giltighetstiden att förlängas. Vid uteblivet svar inaktiveras kontot.

ORU-konto Student

Ett ORU-konto Student är aktivt i 24 månader efter senaste avslutat kurstillfälle och efter det avaktiveras kontot i Örebro universitets identitetskatalog och AD-kontot raderas. ORU-konto Student avaktiveras tillfälligt om en student blir avstängd. När avstängningen löper ut blir ORU-konto Student automatiskt återaktiverat.

ORU-externkonto

Ett ORU-externkonto inaktiveras när det den sista behörighetens giltighet har löpt ut. Efter sex månader rensas AD kontot helt. En chef kan dock besluta om förlängd tillgång vid behov.

Vid missbruk kan ett ORU-externkonto spärras enligt samma rutin som ovan. Det kan också göras genom att supportpersonal tillfälligt sätter om lösenordet.

5.5 Credential Status Management

Alla utgivna användaruppgifter lagras i ORU:s identitetskatalog.

Revokerade användaruppgifter kan återaktiveras för samma användare inom 24 månader. Om återaktivering inte skett inom 24 månader så raderas samtliga användaruppgifter förutom EPPN som sparas för att förhindra återanvändning. Vid Örebro universitet används EPPN som unik identifierare. Se punkt 5.4.1.

Samtliga system är placerade i en datorhall med redundans av el och nätverk. Vidare så är miljön till stora delar **virtualiserad** vilket gör det enkelt att flytta funktionen till en virtuell miljö i en annan datahall. Tillgängligheten motsvarar samma nivå som de interna system som använder identitetstjänsten.

5.6 Credential Validation/Authentication

Vi följer SWAMID:s rekommendationer för konfiguration av ingående system.

Det är inte möjligt att autentisera ett konto som är avaktiverat eller spärrat.

Samtliga system kräver att lösenord anges.

För system som hanterar information med högsta informationsklassen eller som tillhör kritisk infrastruktur sker alltid MFA med interaktiv autentisering.

Samtliga sessioner har en maxtid på 8 timmar. Sedan måste en ny inloggning ske för att skapa en ny session.