



**Linnéuniversitetet**

Kalmar Växjö

# SWAMID Identity Management Practice Statement (IMPS) - Linnaeus University (level 2)

**Version:** V 2.0

**Approved:** 2024-??-??

**Dnr-Lnu:** LNU-2023/2481





# Innehållsförteckning

<b>1. Inledning</b> .....	<b>1</b>
<b>4. Organisational Requirement</b> .....	<b>1</b>
4.1 Enterprise and Service Maturity .....	1
4.2 Notices and User Information .....	1
4.3 Secure Communications.....	2
4.3.1 och 4.3.2.....	2
4.3.3.....	2
4.3.4.....	2
4.4 Security-relevant Event (Audit) Records .....	3
<b>5. Operational Requirement</b> .....	<b>3</b>
5.1 Credential Operating Environment .....	3
5.1.1.....	3
5.1.2.....	3
5.1.3.....	3
5.1.4.....	4
5.2 Credential Issuing.....	4
5.2.1 <i>Identitetsutfärdarens administrative domän I SWAMID</i> .....	4
5.2.2 <i>Identitetsutfärdarens globalt unika identifierare</i> .....	4
5.2.3 <i>Varje användare ska ha ett eller flera användarnamn som inte får återanvändas för andra användare.</i> .....	4
5.2.4 <i>Om användare har fler än ett användarkonto ska de kunna välja vilken de använder vid inloggning, ex. personalkonto eller studentkonto.</i> .....	4
5.2.5 Utlämning av inloggningsidentiteter .....	5
5.2.6.....	8
5.2.7.....	8
5.2.8.....	8
5.3 Credential Renewal and Re-issuing .....	9
5.3.1.....	9
5.3.2.....	9
5.3.3.....	9
5.4 Credential Revocation.....	9
5.4.1.....	9
5.4.2.....	9
5.4.3.....	9
5.5 Credential Status Management.....	10
5.5.1.....	10
5.5.2.....	10
5.6 Credential Validation/Authentication .....	10
5.6.1.....	10
5.6.2.....	10
5.6.3.....	10
5.6.4.....	10



## 1. Inledning

Linnéuniversitetet är som svenskt lärosäte beroende av att på ett och enkelt sätt kunna ge sina anställda och studenter tillgång till nationella och internationella IT-resurser. Detta ges genom medlemskap i SWAMID. Universitetet ser därför ett fortsatt medlemskap som en förutsättning för sin verksamhet.

Linnéuniversitetet avser att fortsatt uppfylla kraven för AL1 och AL2.

## 4. Organisational Requirement

*The purpose of this section is to define conditions and guidance regarding participating organizations responsibilities.*

### 4.1 Enterprise and Service Maturity

Linnéuniversitetet, organisationsnummer 202100-6271, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr universitetets/högskolans 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 och integrationsplattform innehåller uppgifter om lärosätets organisation samt personuppgifter om alla som är verksamma vid lärosätet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas. GDPR (Förordning (EU) 2016/679), Dataskyddslagen (SFS 2018:218) och offentlighets- och sekretesslagen (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 och integrationsplattform.

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

Fysisk lagringsmedia som använts inom identitetshanteringen förstörs enligt rutiner för destruering av lagringsmedia. Lagringsmedia som ska återanvändas formateras innan återanvändning.

### 4.2 Notices and User Information

*The member organization provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organization Subjects. These policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the General Data Protection Regulation (EU) 679/2016.*



Linnéuniversitetet kräver att samtliga användare godkänner ett användaravtal i kontohanteringsportalen innan de får åtkomst till universitetets IT-tjänster. När ny version av användaravtalet publiceras krävs ett förnyat av godkännande.

Länk till kontoportal: <https://account.lnu.se/>.

Linnéuniversitetets användaravtal finns publicerat under universitetets interna styrdokument: <https://lnu.app.box.com/file/1638290502928>.

Linnéuniversitetet loggar all historik över användarens godkännanden. Loggen innehåller information om datum och tid samt avtalsversion kopplat till varje enskild användare.

Kontroll av godkännande sker vid varje inloggning genom användning av Entra IDs Terms of Use funktion. Saknas godkännande kommer systemet tvinga användaren att godkänna användaravtalet.

Linnéuniversitetets Tjänstebeskrivning för federerad inloggning (eduid definition + Privacy Policy) finns publicerat under universitetets interna styrdokument:

<https://lnu.se/medarbetare/organisation/it/styrdokument-it/#policy-personuppgifter-idp>

(Policy för hantering av personuppgifter inom ramen för identitetsutgivaren (Identity Provider, IdP) som fastställs av Linnéuniversitetet) samt

<https://lnu.se/medarbetare/organisation/it/styrdokument-it/#federal-inloggning>

(Tjänstebeskrivning för federal inloggning).

Policy för personlig integritet görs tillgänglig för samtliga i samband med inloggning via en länk på inloggningsidan i Entra ID: <https://lnu.se/mot-linneuniversitetet/kontakta-och-besoka/personuppgifter/>.

## 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 och 4.3.2

Enbart systemadministratörer av identitetssystemen och underliggande system har tillgång till serverna som står i datorhallar. Känslig information skyddas genom rättigheter. Nycklar och hemligheter lagras i klartext, bedöms godtagbart då ingen utan behörighet har tillgång till systemen. I de fall de finns delade lösenord eller motsvarande lagras dessa i lösenordshanteringssystem, där åtkomst loggas och begränsas till behöriga systemadministratörer.

### 4.3.3

All kommunikation mellan vår Identity Provider och underliggande system (AD) är krypterad via TLS. Krypteringsnycklar byts ut vart 3:e år eller vid större uppgraderingar.

### 4.3.4

Gränssnittet för inloggning via vår Identity Provider är SSL-krypterad med 2048bit RSA nyckel.



## 4.4 Security-relevant Event (Audit) Records

*This section defines the need to keep an audit trail of relevant systems.*

Identitetsutgivartjänsterna med underliggande katalogtjänst loggar händelser i central loggserver. System för att administrera identiteter loggar händelser i databas.

## 5. Operational Requirement

*The purpose of this section is to ensure safe and secure operations of the service.*

### 5.1 Credential Operating Environment

*The purpose of this subsection is to ensure adequate strength of Subject credentials, such as passwords, and protection against common attack vectors.*

#### 5.1.1

Lösenordspolicyn bygger på Sunets krav samt Microsoft Best Practise.

Lösenordets komplexitet regleras i följande lösenordspolicydokument och uppfyller kravet på minst 24 bitars komplexitet.

<https://lnu.app.box.com/file/1641004502207> (Lösenordsregler för Linnéuniversitetet).

#### 5.1.2

Genom användning av TLS samt SAML-protokoll för samtliga transaktioner skyddas systemen mot replay-attacker, avlyssning och förvanskning.

#### 5.1.3

Användarna tvingas ta del av reglerna för hanteringen av lösenord i användaravtalet, som godkänds elektroniskt i samband med att kontot skapas eller används första gången samt i samband med ny version av användaravtalet.

Linnéuniversitetets användaravtal finns publicerat under universitetets interna styrdokument: <https://lnu.app.box.com/file/1638290502928>.

I användaravtalet står bl.a. att ”lösenordet som tillhör behörigheten ska behandlas som en värdehandling och är personlig”.

Inom ramen för Linnéuniversitetets IT- och informationssäkerhetsarbete utbildas och påminns personal om att kontinuerligt skydda information, genom att exempelvis aldrig lämna ut lösenord.

I samband med att personaldator lämnas ut, betonar IT-support vikten av att lösenord är personligt och inte få delas eller lämnas ut.

Studenter får i samband registrering information om att aldrig lämna ut kontouppgifter, inkl. lösenord, samt uppmanas att byta lösenord om det hamnat i orätta händer.



## 5.1.4

Systemen som används för identitetshantering skyddas bakom brandväggar och endast de portar som är nödvändiga för inloggning är öppna. Patchning sker kontrollerat och regelbundet.

Systemen används aldrig mer än till deras syfte. Access till identitetshandlingen är endast är åtkomlig av behörig personal och aktiviteterna loggas.

Risk och hot hanteras av universitetets Incident Response Team (IRT) samt inom informationssäkerhetsarbetet som drivs av universitetets kansli (UK).

I informationssäkerhetsarbetet ingår att regelbundet genomföra riskanalys på inkomna incidenter samt sårbarhetsanalys på samtliga it-komponenter i förvaltningsobjekten. Universitetet använder sig av en förvaltningsmodell som bygger på PM3.

Linnéuniversitetet stänger av konton vid brott mot avtal och regler.

## 5.2 Credential Issuing

*The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process. All relying parties have a need to uniquely identify the Identity Provider and the Identities provided by that Identity Provider.*

### 5.2.1 Identitetsutfärdarens administrativa domän I SWAMID

Linnéuniversitetet har domänen lnu.se, som används på alla användaridentiteter för att göra dem globala.

### 5.2.2 Identitetsutfärdarens globalt unika identifierare

Linnéuniversitetet identitetsutgivare har globalt unika identifierare och är utgivare för samma identiteter.

### 5.2.3 Varje användare ska ha ett eller flera användarnamn som inte får återanvändas för andra användare.

Användarnamn som varit i bruk av person återanvänds aldrig när denne slutar, detta för att kunna säkerställa historik. Linnéuniversitetets kontohanteringssystem kontrollerar att användarnamn inte återanvänds.

### 5.2.4 Om användare har fler än ett användarkonto ska de kunna välja vilken de använder vid inloggning, ex. personalkonto eller studentkonto.

Alla användare har en unik identitet utifrån den roll som användaren har i organisationen och kan identifieras vid denna. Skilda identiteter för studenter och personal. Användaren väljer vilket konto som ska användas vid inloggningstillfället.

För att säkerställa historiken för ett konto återanvänds inte användarnamn när personens konto arkiveras.



## 5.2.5 Utlämning av inloggningsidentiteter

- Länk till kontoregler: <https://lnu.se/medarbetare/organisation/it/styrdokument-it/> (kontoregler på Linnéuniversitetet)
- Länk till kontoportalen: <https://account.lnu.se/>

### Utlämning av inloggningsidentiteter till studenter

#### *Skapa studentkonto*

Studentkonto kan endast skapas om studenten är antagen till Linnéuniversitetets innevarande eller nästkommande termin. Kontroll görs att inget annat aktivt studentkonto finns på denna person.

Studenter hämtar ut (skapar) konto i Kontoportalen (account.lnu.se), genom att använda antagning.se, eduID, e-legitimation eller beställa en engångskod för att logga in på tjänsten.

Internationella studenter (studenter som saknar svenskt personnummer), får automatiskt utskickad engångskod. När en internationell student blivit antagen och överförd till Ladok skickas automatiskt ett mail till studentens e-postadress (från NyA/Ladok) med ett interimspersonnummer\* och en automatiskt genererad engångskod.

\* En internationell student behöver ett tillfälligt personnummer eller ett svenskt personnummer för att kunna hämta ut sitt studentkonto. Tillfälligt personnumret får studenten i samband med antagning, kan hittas i NyA.

Länk till NyA: <https://expert.antagning.se/dw/index.dw>.

Studenter som använder sig av engångskod, som de begärt ut via IT-support eller via kontoportalen får AL1.

Engångskoder som skickas via sms, e-post, till folkbokföringsadress eller till hushållningsadress (adressuppgift i NyA/Ladok) är tidsbegränsade till 90 dagar. Vid användning av engångskod används CAPTCHA för att verifiera att användaren inte är en robot.

Som förregistrerad identifierare används:

- E-post registrerad i Nya/Ladok.

#### **Metoder som resulterar i ett AL2 konto för student:**

- Mot uppvisande av giltig\* legitimationshandling på plats hos IT-supporten kan studenter manuellt tilldelas AL2. Personal på IT-supporten som hanterar AL-nivåer har AL2 på sina personalkonton.

\* Följande typer av legitimationer accepteras:

- a) Godkänd svensk ID-handling (SIS-märkt ID-kort, SIS-märkt tjänstekort, SIS-märkt företagskort, körkort).
- b) Svenskt nationellt ID-kort eller pass.
- c) Nationellt ID-kort eller pass utgivet av medlem i EU/EES.
- d) Annat utländskt pass där ICAO doc 9303 är uppfyllt.



- Antagning.se – efter inloggning kontrolleras att kontot är AL2 från antagning.se (eduPersonAssurance). Dessutom kontrolleras att antagning.se är giltig utfärdare för denna tillitsnivå. Studentkontot sätts till AL2.
- eduID - efter inloggning kontrolleras att kontot är AL2 från eduID (eduPersonAssurance). Dessutom kontrolleras att eduID är giltig utfärdare för denna tillitsnivå. Studentkontot sätts till AL2.
- Svensk e-legitimation – efter legitimering kontrolleras att legitimeringen görs med minst LoA3. Studentkontot sätts till AL2.

Som förregistrerad identifierare används:

- Personnummer, om det finns tillgängligt.
- Namn och födelsedata vid riskbaserad bedömning.

## Utlämning av inloggningsidentiteter till personal

Personal som använder engångslösenord i kontoportalen får AL1.

Beställare för personalkonton är chef eller av chef utsedd kontaktperson. Personal kan inte själva beställa ett konto. Det åligger beställaren att identifiera individen och inhämta en e-postadress dit kontoaktivering kan skickas.

IT-support skickar en engångskod till den e-postadress som beställaren angivit. Vid användning av engångskod används CAPTCHA för att verifiera att användaren inte är en robot.

Kontoinnehavaren kan inte själv beställa engångskod eller engångslösenord i Kontoportalen.

Kontoinnehavaren loggar in med engångslösenordet i Kontoportalen där byte av lösenord krävs innan kontot kan användas.

Som förregistrerad identifierare används:

- E-post angiven av beställaren.

## Metoder som resulterar i ett AL2 konto för personal:

- Mot uppvisande av giltig\* legitimationshandling på plats hos IT-supporten kan personal manuellt tilldelas AL2. Personal på IT-supporten som hanterar AL-nivåer har AL2 på sina personalkonton.

\* Följande typer av legitimationer accepteras:

- a) Godkänd svensk ID-handling (SIS-märkt ID-kort, SIS-märkt tjänstekort, SIS-märkt företagskort, körkort).
  - b) Svenskt nationellt ID-kort eller pass.
  - c) Nationellt ID-kort eller pass utgivet av medlem i EU/EES.
  - d) Annat utländskt pass där ICAO doc 9303 är uppfyllt.
- eduID - efter inloggning kontrolleras att kontot är AL2 från eduID (eduPersonAssurance). Dessutom kontrolleras att eduID är giltig utfärdare för denna tillitsnivå. Personalkontot sätts till AL2.





- Svensk e-legitimation – efter legitimering kontrolleras att legitimeringen görs med minst LoA3. Studentkontot sätts till AL2.
- Videosamtal

Rutin för **verifiering av betrodd part** vid videosamtal:  
Betrodd part är kontoinnehavarens chef organisatoriskt.  
Kontoadministratör säkerställer att betrodd part har tillitsnivå AL2.

Betrodd part verifieras antingen på plats tillsammans med kontohandläggaren alternativt via BankID under videosamtalet.

Kontoadministratör och betrodd part genomför ett videosamtal där betrodd part delar skärm.

Under videosamtalet:

Betrodd part öppnar sitt digitala ID-kort via BankID mobilapp och visar QR-kod för kontoadministratör. Kontoadministratör skannar uppvisad QR-kod och får tillbaka bild på personen för att kunna verifiera att det är samma person. Kontoadministratör dokumenterar ärendenummer samt verifieringsmetod på kontot.

Rutin för **verifiering av kontoinnehavare** vid videosamtal:  
Kontoinnehavaren skickar en kopia av giltig identitetshandling till IT via ärendehanteringssystemet.

Kontoadministratör verifierar att namn och födelsedata stämmer överens med uppgifterna på kontoinnehavarens konto.

Ett videosamtal med kontoinnehavare, kontoadministratör och betrodd part genomförs.

En riskbaserad bedömning av identitet sker genom att kontoadministratör ser kontoinnehavare framför sig som visar upp samma identitetshandling som tidigare har verifierats av kontoadministratör. Som del av riskbedömningen intygar betrodd part att det är rätt person.

Kontroll görs av kontoadministratör under videosamtalet att identitetshandling är giltig.

Kontoadministratör ändrar kontoinnehavarens tillitsnivå från AL1 till AL2 och dokumenterar ärendenummer samt verifieringsmetod på kontot.

Som förregistrerad identifierare används:

- Namn och födelsedata vid riskbaserad bedömning.
- Personnummer.

## **Utlämning av inloggningsidentiteter till externa personer**

Anställd vid Lnu beställer externkonto till externa personer hos IT-support. Det åligger kontobeställaren att identifiera individen.



Externa personer får, till verifierad e-post (förregistrerad identifierare), tillskickat kontouppgifter med engångslösenord, som måste bytas vid första inlogg. AL-nivån sätts till AL1.

## Metoder som resulterar i ett AL2 konto för externa personer:

- Mot uppvisande av giltig\* legitimationshandling på plats hos IT-supporten kan personal manuellt tilldelas AL2. Personal på IT-supporten som hanterar AL-nivåer har AL2 på sina personalkonton.

\* Följande typer av legitimationer accepteras:

- a) Godkänd svensk ID-handling (SIS-märkt ID-kort, SIS-märkt tjänstekort, SIS-märkt företagskort, körkort).
  - b) Svenskt nationellt ID-kort eller pass.
  - c) Nationellt ID-kort eller pass utgivet av medlem i EU/EES.
  - d) Annat utländskt pass där ICAO doc 9303 är uppfyllt.
- eduID - efter inloggning kontrolleras att kontot är AL2 från eduID (eduPersonAssurance). Dessutom kontrolleras att eduID är giltig utfärdare för denna tillitsnivå. Externkontot sätts till AL2.
  - Svensk e-legitimation – efter legitimering kontrolleras att legitimeringen görs med minst LoA3. Externkontot sätts till AL2.

Som förregistrerad identifierare används:

- Namn och födelsedata vid riskbaserad bedömning.
- Personnummer.

Vid skapande av användarkonto för **gäster**:

- Tillfälliga gäster som får ett gästkonto med tidsbegränsat giltighetstid (2 veckor) får alltid AL1. Det åligger kontobeställaren att identifiera individen och validera

e-post (förregistrerad identifierare) innan uppgifter om konto och lösenord ges till mottagaren, skickas via e-post eller fysisk överlämning. Gäster kan inte logga in i SWAMIDs tjänster.

## 5.2.6

Alla AL-nivå ändringar sparas på användaren och kan kontrolleras i databasen vid behov.

## 5.2.7

Uppgifter som lagts in av användaren själv kan ändras av användaren. Studenter kan ändra vissa förutbestämda kontaktuppgifter som co-adress och telefonuppgifter med hjälp av Ladok på Webb (LPW). Rättningar av övriga uppgifter görs i källsystem av behöriga användare.

## 5.2.8

Endast användare som är identifierade på AL2 nivå, som är systemadministratör i identitetssystemen eller kontoadministratör kan hantera konton som de är behöriga att hantera.



## 5.3 Credential Renewal and Re-issuing

*Renewal of credentials occur when the Subject changes its credential using normal password reset. Re-issuing occurs when credentials have been invalidated.*

### 5.3.1

I kontoportalen kan användare byta lösenord, återställa lösenord samt höja AL-nivån, om kontotyp och verifiering tillåter.

### 5.3.2

Samtliga användare har möjlighet att byta lösenord via kontoportalen eller direkt på Lnu-dator (ej SAML/SSO). Först anges nuvarande lösenord och därefter det nya, som måste följa Linnéuniversitetets lösenordspolicy.

### 5.3.3

Användare som behöver återställa sitt lösenord tvingas till lösenordsåterställning och därefter genomgå utlämningsprocessen i 5.2.5. Kontroll görs mot sedan tidigare förregistrerade identifierare.

## 5.4 Credential Revocation

*The purpose of this subsection is to ensure that credentials can be revoked.*

### 5.4.1

Vid misstänkt säkerhetsincident kan specifika konton stängas av. En användare kan också begära att få sitt konto avstängt.

Avstängning av konton sker enligt kontoregler på Lnu:

<https://lnu.app.box.com/file/1634359965119?s=oj4kc8yad6a5inpnxb6j3m2xi91kpf2y>

(Kontoregler på Linnéuniversitetet).

### 5.4.2

På uppmaning från Incident Response Team (IRT) stänger IT-support av konto på grund av säkerhetsincident. Användaren informeras om anledning, samt vad den bör tänka på för att det inte ska hända igen.

Efter att användaren genomfört rekommenderade säkerhetsåtgärder, behöver lösenordet återställas innan kontot åter kan användas, enligt samma rutiner som vid tilldelning/återställning av konto enligt 5.2.5 eller 5.3.3.

### 5.4.3

IT-säkerhetsarbetet sker i nära samverkan med universitetets informations-säkerhetsarbete. Vi arbetar proaktivt för att stödja användaren i sin arbetsutövning. Det handlar om allt från att förmedla och utbilda i sunt säkerhetstänkande till god säkerhetsnivå på IT-system.

Beroende på incidentens karaktär kan även Linnéuniversitetets krisorganisation informeras/aktiveras. Bedömning om incidenten ska eskaleras dit görs av IT-arkitekt



säkerhet i samråd med driftschef. Bedömning om krisorganisation ska aktiveras görs av krisledningen.

## 5.5 Credential Status Management

*The purpose of this subsection is to ensure that credentials are stored accordingly and that Identity Management systems have a high degree of availability.*

### 5.5.1

Historiken över utfärdade identiteter/användarnamn finns sparade i universitetets kontohanteringssystem. Användarnamn återanvänds aldrig. I de fall en användare vill ha sina personuppgifter raderade enligt GDPR raderas all data utom användarnamn.

Kontohändelser som rör inloggningsinformation loggas.

### 5.5.2

System som används för kontohantering bedöms enligt risk- och sårbarhetsanalyser som verksamhetskritiska eller verksamhetsviktiga. IdP är tillgänglig minst så mycket att man kan logga in på interna system.

Det finns inga formella SLA för system på Linnéuniversitetet, men genom dess höga klassificering hanteras de med hög prioritet.

## 5.6 Credential Validation/Authentication

*The purpose of this subsection is to ensure that the implemented Validation/Authentication processes meet proper technical standards.*

### 5.6.1

Linnéuniversitetets identitetsutgivare följer SWAMIDs rekommendationer och best practice.

### 5.6.2

Konton som är avstängda eller låsta kan inte användas av IdP tjänsten för inloggning till interna Lnu och externa SWAMID tjänster.

### 5.6.3

En användare måste logga in med sina inloggningsuppgifter eller giltig SSO biljett för att autentisera sig mot en tjänst.

### 5.6.4

En SSO session är giltig i en timme, om det pågår aktivitet. Efter denna tid måste användaren logga in på nytt.