Linnéuniversitetet
Kalmar Växjö

Document	Linnéuniversitetet / Linnaeus University Identity Management Practice Statement
Version	V 1.9
Last modified	2023-05-09
Pages	11
Status	Final
License	Creative Commons BY-SA 3.0

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

1. Inledning 2
4. Organisational Requirement 2
4.1 Enterprise and Service Maturity 2
4.2 Notices and User Information 3
4.3 Secure Communications 3
4.4 Security-relevant Event (Audit) Records 4
5. Operational Requirements 4
5.1 Credential Operating Environment 4
5.2 Credential Issuing 6
5.3 Credential Renewal and Re-issuing 9
5.4 Credential Revocation 10
5.5 Credential Status Management 10
5.6 Credential Validation/Authentication 11

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, integrationsplattform, MS Active Directory 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 m.m. 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.

Linnéuniversitet 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/
Länk till användaravtal: https://lnu.app.box.com/s/bo1h21ybi7tektekne7j5k1te0lcndd1

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 via Shibboleth, saknas godkännande kommer systemet tvinga användaren att godkänna användaravtalet.

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

- https://lnu.se/medarbetare/organisation/it/styrdokument-it/

Policy för personlig integritet (PP)

- Policy för personlig integritet görs tillgänglig för samtliga i samband med inloggning via Shibboleth.
  https://lnu.se/medarbetare/organisation/it/styrdokument-it/

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 identitetsystemen och underliggande system har tillgång till servrarna 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 Shibboleth/identitetsutgivaren och underliggande system (AD) är krypterad via TLS. Krypteringsnycklar byts ut vart 3år eller vid större uppgraderingar.

4.3.4
Gränssnittet för inloggning via Shibboleth 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 Requirements

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.se/medarbetare/organisation/it/styrdokument-it/ (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.

Linneuniversitets användaravtal:
https://lnu.app.box.com/s/bo1h21ybi7tektekne7j5k1te0lcndd1

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. Systemen används aldrig mer än till deras syfte. Patchning sker kontrollerat och regelbundet.

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 systemförvaltningsmodell 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 administrative 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. Lunaa (Linneaus University Account Administration) 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 identiteteter för studenter och personal. Användaren väljer vilket konto som ska används vid inloggningstillfället. För att säkerställ historiken för ett konto återanvänds inte användarnamn när personen slutar.

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/

Universitetet använder sig av följande identifieringsmetoder vid hantering av autentiseringsuppgifter:

1. Online authenticating the Subject at SWAMID Identity Assurance Level 2 Profile, or higher, using an Identity Provider compliant with SWAMID Identity Assurance Profiles;
2. Online authenticating the Subject at Swedish E-identification Level of Assurance 3, or higher, using an Identity Provider compliant with the Swedish E-identification System;
3. Online authenticating the Subject at eIDAS regulation (EU) No 910/2014 assurance level substantial, or higher, using an Identity Provider compliant with the eIDAS EU regulation;
4. In-person visit at a service desk in combination with identity proofing with approved forms of identification documents, as defined by the Swedish police for issuance of the Swedish passport;
5. In-person visit at a service desk in combination with identity proofing with an

international passport fulfilling ICAO Doc 9303 or an EU/EES national identity card fulfilling the European Commission Regulation No 562/2006;
6. Off-line using a registered address (sv. folkbokföringsadress) in combination with a time-limited one-time password/pin code;
7. Off-line using a copy of the same identification token as described in 4 or 5 above and a copy of a utility bill in combination with a time-limited one-time password/pin code sent to the postal address on the utility bill; or
8. Other equivalent identity proofing method.

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.

Engångskoder som skickas via sms, e-post, till folkbokföringsadress eller till hushållningsadress (adressuppgift i NyA/Ladok) är tidsbegränsade till 90 dagar.

Vid beställning av engångskoder till SMS eller e-post behöver användaren bekräfta med stöd av CAPTCHA eller motsvarande att den inte är en robot.

Internationella studenter (studenter som saknar svenskt personnummer), får automatiskt utskickad engångskod. När en internationell student blivit antagen och överförd till Ladok genereras ett ärende i ärendehanteringssystemet med information om verifierad mailadress (från NyA/Ladok), personnummer* och genererad engångskod. IT-support mailar studenten personnummer och 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

Metoder som resulterar i ett AL1 konto:

1. Studenter som använder sig av engångskod, som de begärt ut via IT-support eller via kontoportalen får AL1, om engångskod levererats via SMS, e-post, folkbokföringsadress eller hushållningsadress.

2. Uppdragsstudenter där engångskod delas ut på plats av kurs/programansvarig till studenterna får AL1, då vi inte kan bekräfta hur utdelningen gått till. Det åligger kurs/programansvarig att identifiera studenten.

Som förregistrerad identifierare används:
- Verifierad e-post från Nya/Ladok

Metoder som resulterar i ett AL2 konto:

1. 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.

2. Antagning.se – efter inloggning kontrolleras att kontot är AL2 från antagningen.se (eduPersonAssurande). Studentkontot sätts till AL2.

3. Eduid.se - efter inloggning kontrolleras att kontot är AL2 från eduid.se (eduPersonAssurande). Studentkontot sätts till AL2.

4. 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**

Chef eller annan behörig kontaktperson beställer personalkonto till personal hos IT-support. Det åligger kontobeställaren att identifiera individen.

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

För att kunna ändra AL-nivån till AL2 krävs något av följande:

- Mot uppvisande av giltig legitimationshandling på plats hos IT-supporten kan personal manuellt tilldelas AL2-nivå. För personal på IT-supporten som hanterar AL-nivåer krävs AL2-nivå.

- Personal loggar in med användarnamn och lösenord samt därefter verifierar sig med svensk e-legitimation. AL-nivån höjs till AL2. I samband med verifiering kontrolleras personnummer och att legitimeringen görs med minst LoA3.

Som förregistrerad identifierare används:
- Personnummer

Vid skapande av användarkonto för **externa personer** (ex konsulter, gästföreläsare):

- Tillfälliga externa personer som får ett externkonto med tidsbegränsat giltighetstid (upp till 1 år) 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.

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

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 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.se/medarbetare/organisation/it/styrdokument-it/
(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.

Skulle en större säkerhetsincident inträffa (major incident) där flera/alla konton påverkas finns ett IRT (Incident Response Team) team där Incident Manager ingår, som omgående hanterar och agerar på säkerhetsincidenten. Vid enstaka tillfällen kan även Linnéuniversitetets IT-krisorganisation aktiveras. Alla IT-incidenter registreras i ärendehanteringssystem och hanteras separat och enligt rutin. Flera säkerhetsincidenter kan knytas till ett huvudärende.

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 Lunaa. 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 verksamhetsviktia, med tillgänglighet på ca. 95%.

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 SWAMID.s 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.