Document	Linköpings universitet Identity Management Practice Statement
Version	V3.3
Last modified	2024-06-17
Pages	13
Status	Final
License	Creative Commons BY-SA 3.0

Linköpings universitet
Identity Management Practice Statement

1. Inledning

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

LiU avser att uppfylla kraven för AL1, AL2 samt AL3

4. Organisational Requirement

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

4.1 Enterprise and Service Maturity

This subsection defines the organization and the procedures that govern the operations of the identity provider.

Linköpings universitet, organisationsnummer 202100-3096, 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 centrala katalogsystem, integrationsplattform och behörighetssystem 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. Personuppgiftslagen (SFS 1998:204) 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 lärosätets centrala katalog, integrationsplattform och behörighetssystem.

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.

4.1.3 Lagringsmedia som använts inom identitetshanteringen förstörs fysiskt med säkra metoder om det inte längre skall använda inom identitetshanteringen. Lagringsmedia som ska återanvändas inom identitetshanteringen formateras innan återanvändning.

4.2 Notices and User Information

The Member Organisation provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organisation Subjects. These policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the General Data Protection Regulation (EU) No 679/2016.

LiU har användarvillkor som måste godkännas vid varje aktivering eller återaktivering av ett konto i kontohanteringsportalen. Vid förändring av användarvillkoren meddelas universitetets medarbetare och studenter via personlig kanal t.ex. e-post eller kontohanteringsportalen.

4.2.1, 4.2.2, 4.2.4
Vid aktivering/återställning av lösenord måste användarvillkoren godkännas för att användaren ska få tillgång till kontot. Varje godkännande sparas i databas.

4.2.3
Om användarvillkoren uppdateras notifieras användaren vid inloggning i kontohanteringsportalen där användaren också kan godkänna villkoren. Vid ändring skickas information ut via e-post.

4.2.5
Användarvillkoren finns tillgängliga
via http://styrdokument.liu.se/Regelsamling/VisaBeslut/622846
Tjänstebeskrivning och integritetspolicy rörande identitetshanteringen finns tillgängliga via https://liu.se/artikel/tjanstebeskrivning-for-federerad-inloggning och https://liu.se/artikel/policy-for-hantering-av-personuppgifter-inom-ramen-for-identitetsutgivaren.

4.3 Secure Communications

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

4.3.1-4.3.2
Enbart systemadministratörer av identitetssystemen och underliggande system har tillgång till servrarna som står i avsedda datorhallar, men känslig information skyddas ändå genom operativsystemets inbyggda mekanismer (t.ex. filrättigheter). Nycklar och hemligheter lagras i klartext, vilket bedöms acceptabelt eftersom ingen utan behörighet till dessa har tillgång till systemen. I de fall det finns delade lösenord eller motsvarande lagras dessa i det centrala lösenordshanteringssystemet där åtkomsten loggas och begränsas till behöriga systemadministratörer alternativt i kassaskåp med begränsad åtkomst.

4.3.3

All datatrafik mellan identitetsutgivarna och underliggande system är krypterad med TLS eller SSH. Konfigurationen av dessa protokoll utvärderas och förbättras löpande.

4.3.4
Identitetsutgivarnas entitetsnycklar är minst 2048 bitar RSA eller motsvarande.

4.4 Security-relevant Event (Audit) Records

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

Identitetsutgivartjänsterna med underliggande system så som katalogtjänster och system för att administrera identiteter loggar kontohändelser med tidsstämpel till den centrala loggservern.

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
Nedan visas en tabell över de krav vi ställer på lösenordskomplexitet och längd för de olika teckenkombinationerna. Alla nedan kombinationer uppfyller entropi >24 bitar. När vi räknar antal tecken är inte mellanslag bedräknat.

Typ av konto	*H*	Min	$L_{aB1@}$	L_{aB1}	L_{aB}	L_{ab1}	L_{abc}	L_{123}
Normalt	64	10	10	11	12	13	14	20

$L_{aB1@}$: Minsta längd för lösenord med versaler, gemener, siffror, och symboler.
L_{aB1}: Minsta längd för lösenord med versaler, gemener, och siffror.
L_{aB}: Minsta längd för lösenord med versaler och gemener.
L_{ab1}: Minsta längd för lösenord med siffror samt enbart versaler *eller* gemener.
L_{abc}: Minsta längd för lösenord med enbart versaler eller gemener.
L_{123}: Minsta längd för lösenord med enbart siffror.

- Lösenord ska inte förekomma i förteckningar över vanliga, kända, eller läckta lösenord.
- Lösenord ska inte innehålla LiU-ID eller delar av användarens namn. Undantag får göras för sekvenser om tre tecken eller mindre (till exempel ”von”, ”af”, och ”de”, som är vanligt förekommande prefix men skulle begränsa valet av lösenord för kraftigt).

- Vid byte av lösenord får det nya lösenordet inte vara giltigt på något av användarens vanliga, tekniker- eller administratörskonton.

För extra skydd av konton används multifaktorsinloggning (självuppgiven) på alla anställdakonton genom inloggning med autentiseringsapp på telefon (TOTP/Pushnotifering med inmatningskrav*) eller hårvarutoken (TOTP/WebAuthn) då man loggar in på ej hanterad hårdvara utanför LiU:s nätverk. VPN kräver multifaktorsinloggning.

*LiU har gått över till pushnotifiering med inmatningskrav. Det innebär att vid inloggning med multifaktorsinloggning får användaren dels en uppgift om vilken applikation som begär den andra faktorn, dels får se en karta var inloggningen påbörjades. På datorn visas två siffror som användaren måste mata in i appen. Användaren ges endast ett försök. All annan pushnotifiering är avstängd.

Microsoft anser att deras Authenticator-app med pushnotifiering uppfyller kraven för Single-Factor Cryptographic Software enligt NIST 800-63B. Detta beskrivs i Microsofts dokumentation för Achieving NIST AALs, https://docs.microsoft.com/en-us/azure/active-directory/standards/nist-authenticator-types - Microsoft Authenticator App (Notification). Linköpings universitets bedömning är att detta stämmer och att Microsoft Authenticator-appen uppfyller kraven för Single-Factor Cryptographic Software i NIST 800-63B när den används med pushnotifieringar och godkännande av inloggning i appen.

För AL3 utfärdas personverifierad multifaktorsinloggning. Efter verifierat utfärdande läggs användaren i en specifik grupp för ändamålet. Vid inloggning kontrolleras att användaren har gjort en multifaktorsinloggning samt att användaren ligger i ovan grupp innan AL3 signaleras till SP.

5.1.2
Genom användning av TLS samt SAML-protokollet för samtliga transaktioner skyddas systemen mot replay-attacker, avlyssning och förvanskning.

5.1.3
I LiU:s riktlinjer för informationssäkerhet, som alla användare måste godkänna, klargör vi att lösenord aldrig får delas samt att mobiltelefoner och andra faktorbärare inte får lämnas oskyddade/obevakade.

LiU stänger aktivt konton vid brott mot ovan regler.

5.1.4

Antalet systemadministratörer som har behörighet på system som används för identitetshantering är kraftigt begränsade. Alla systemadministratörer måste skriva på en speciell ansvarsförbindelse för personer med hög behörighet.

Vid systemadministration används separata identiteter med högre säkerhetskrav, till exempel:

- Lösenordet kan ej sättas till samma som den personliga identiteten.
- Kontot spärras från att logga in på persondatorer.

- Lösenordslängden har högre krav än personliga identiteter

Systemen som används för identitetshantering skyddas bakom brandvägg och endast de portar som är nödvändiga för inloggning är öppnade. Systemen används aldrig till mer än deras syfte. Patchning sker kontrollerat och löpande.

Användare informeras att aldrig använda sitt LiU-konto någon annanstans än på LiU:s IdP. För att användare ska känna igen sig byts bildtema på inloggningssidan under året och är alltid samma som på informationsskärmar runt om universitetet.

5.2 Credential Issuing

5.2.1 Identitetsutfärdarens administrativa domän i SWAMID ("Scope")
LiU har domänen liu.se, som används som scope på alla användaridentiteter för att göra dem globalt unika.

5.2.2 Identitetsutfärdarens globalt unika identifierare
LiU:s identitetsutgivare har globalt unika identifierare och är utgivare för samma identiteter.

5.2.3 Varje användare ska ha ett eller flera unika användarnamn som inte får återanvändas för andra användare
Identiteter som har varit i bruk återanvänds aldrig. Integrationsplattformen som skapar användarnamn säkerställer att kontonamn aldrig återanvänds.

5.2.4 Om användare har fler än ett användarkonto ska de kunna välja vilken de använder vid inloggning, exempelvis ett studentkonto och ett anställdkonto
Skilda identiteter används för studenter och personal. Inloggnings-id:t ser annorlunda ut för de olika kontona. Användaren väljer vilket konto som ska användas vid inloggningstillfället.

5.2.5 Utlämning av inloggningsidentiteter
Oavsett om man är student eller anställd skapas automatiskt ett konto. För anknutna skapas kontot manuellt av en kontoadministratör efter godkännande av prefekt/motsvarande.

Kontot skapas inaktivt, men kan aktiveras via kontohanteringsportalen genom olika metoder. Kopplingen mellan konto och individ sker vanligtvis via personnummer/motsv. där en del kommer från HR/Ladok eller kontohanteringsportalen och den andra från identifieringstjänsten (se "metoder för identifiering av personen" nedan). I vissa fall kan en automatik eller manuell riskbedömning utföras genom att jämföra namn, födelsedata samt nationalitet med information från HR/Ladok eller kontohanteringsportalen.

Ovan koppling mellan konto och individ kontrolleras på samma sätt då en lösenordsåterställning görs.

Nedan listas metoder man kan använda i kontoaktiveringsportalen för att aktivera sitt konto eller då man glömt sitt lösenord:

a) **Aktiveringsnyckel [AL1/AL2]**
   En aktiveringsnyckel är en engångskod. Aktiveringsnyckeln används i kontoaktiveringsportalen och har en viss giltighetstid som bestäms vid skapandet. Vid användning av aktiveringsnyckeln måste personen ange sitt personnummer/motsvarande (står ej på lappen med aktiveringsnyckeln) samt själva aktiveringsnyckeln.
b) **Svensk e-legitimation [AL2/AL3]**
   Efter lyckad legitimering kontrolleras att den gjordes med minst LoA3 samt att kontot finns i vår kontodatabas och har rätt status.
c) **Antagning.se [AL2]**
   Efter lyckad inloggning kontrolleras att kontot är minst AL2 samt att kontot finns i vår kontodatabas och har rätt status.
d) **Eduid.se [AL2]**
   Efter lyckad inloggning kontrolleras att kontot är minst AL2 (bekräftat) samt att kontot finns i vår kontodatabas och har rätt status.
e) **Region Östergötland [AL2]**
   Efter lyckad inloggning kontrolleras att kontot finns i vår kontodatabas och har rätt status. RÖ använder SITHS kort vilket är en e-legitimation med tillitsnivå 3.

Nedan listas metoder för identifiering av personen. Dessa används vanligtvis tillsammans vid uthämtandet av aktiveringsnyckel (a), men kan också användas för att identifiera en person vid utlämnande av LiU-kort eller återställning av en andra faktor.

1) **Fysisk ID-handling via videomöte [AL1]**
   Personen kontaktar Infocenter och bokar ett videomöte (t.ex. för utlämnandet av aktiveringsnyckel). Under videomötet måste personen uppvisa en godkänd legitimationshandling. Infocenter verifierar att legitimationen är giltig (se 3 nedan), samt att fotot överensstämmer med personen. Om allt ser bra ut visar Infocenter upp aktiveringsnyckeln i kameran från ett utskrivet papper.
2) **Rekommenderat brev med personlig uthämtning [AL2]**
   Används i undantagsfall för personer på annan ort som behöver en aktiveringsnyckel.
3) **Fysisk ID-handling [AL2/AL3]**
   Infocenter har en process för att lära alla medarbetare hur ID-handlingar ska verifieras*. Det gäller även då visstidspersonal tas in vid tillexempel hög belastning/sjukdom. Följande sida används för information om olika ID-handlingars äkthet och utformning:
   https://www.consilium.europa.eu/prado/sv/prado-start-page.html

   *En del av processen är att 365iD maskiner används för att kontrollera äktheten på ID-handlingen. 365iD-maskinen gör en utförlig kontroll av säkerhetsmärkningar och annat på ID-handlingen.

   Vid utlämnande av aktiveringsnyckel loggas ID-handlingens typ i kontohanteringsportalen.
   Om personnummer saknas görs en riskbedömning att det är rätt individ och personens nationalitet samt födelsedata sparas undan.
   Följande typer av legitimationer accepteras:

   a. Godkänd svensk ID-handling för ansökan om pass enligt polisen (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.

4) **Digitalt ID via BankID, kontrollerad via BankID app [AL2]**
   Personen tar fram sitt Digitala ID i Mobilt BankID - appen. För att göra det måste en verifiering göras med sitt mobila BankID. Det digitala ID:t visas under en begränsad tidsperiod.

   Infocenter/kontoadministratören skannar QR-koden på mobilskärmen med en BankID-app på en egen mobiltelefon.

   Om Infocenter/kontoadministratörens BankID-app visar användarens uppgifter inkl. bild går man vidare med kontrollen. Fotot i handläggarens BankID-app jämförs med personen som står framför och om de stämmer är en korrekt legitimering genomförd. Om det stämmer är identiteten verifierad och personnummer finns i BankID-appen. Det används vidare i kontoportalen.
5) **Digitalt ID via BankID, kontrollerad via API [AL2/AL3]**
   Personen tar fram sitt Digitala ID i Mobilt BankID - appen. För att göra det måste en verifiering göras med sitt mobila BankID. Det digitala ID:t visas under en begränsad tidsperiod.

   Infocenter/kontoadministratören skannar QR-koden på mobilskärmen med en QR-kodsscanner.

   QR-kodens värde skickas via kontoutlämningsapplikationen till BankID:s API för verifiering (https://www.bankid.com/utvecklare/guider/verifiering-av-digitalt-id-kort/introduktion).

   Om BankIDs API godkänner QR-koden skickas användarens personnummer och namn tillbaka till kontoutlämningsapplikationen och processen kan fortsätta med det verifierade personnumret.

   Om BankIDs API inte godkänner QR-koden returneras endast en felkod med beskrivning som visas i kontoutlämningsapplikationen.

Nedan listas metoder som resulterar i ett AL1 konto:

1. Kontoaktiveringsmetod a tillsammans med identifieringsmetod 1
   Infocenter lägger till användaren manuellt i en grupp för att signalera AL1 till SWAMID:s tjänster vid inloggning.

Nedan listas metoder som resulterar i ett AL2 konto:

2. Kontoaktiveringsmetod a tillsammans med identifieringsmetod 2-4
3. Kontoaktiveringsmetod b, c, d, e

För att kunna få ett AL3 konto måste användaren först ha ett AL2 konto. Användaren måste dessutom redan ha en andra faktor kopplad till kontot (ej personverifierad).

Nedan listas metod för att få ett AL3 konto:

1. Användaren startar processen i kontohanteringsportalen och får först välja om verifieringen ska ske via en extern elektronisk identitet:
    1. Svensk e-legitimation LoA3
    2. AL3-identitet inom SWAMID

    eller Infocenter

2. Kontohanteringsportalen tvingar en inloggning där inloggningsuppgifterna behöver uppges även om användaren redan är inloggad (ej SSO) samt krav på multifaktorsinloggning.

3. Kontohanteringsportalen kontrollerar att en multifaktorsinloggning har gjorts och att användaren endast har en andra faktor registrerat på sig. Om det finns fler än en andra faktor kan endast Infocenter-processen nedan väljas. Det sparas dessutom i databasen att alla faktorer måste kontrolleras manuellt i utlämnandeprocessen.

4. Om extern elektronisk identitet med AL3 har valts av användaren

    a) Användaren skickas till den externa IdP:n för att logga in med multifaktorsinloggning
    b) Efter inloggningen görs följande kontroll(er):
        a) för Svensk e-legitimation kontrolleras att inloggning med LoA3 verkligen utförts
        b) för AL3-identitet inom SWAMID kontrolleras IdP:n är godkänd för AL3 i metadatat samt att inloggning med AL3 verkligen utförts
        c) att personnumret matchar mellan de två inloggningarna
    c) Om ovan stämmer läggs kontot i en AD-grupp som kan signalera AL3.

5. Om Infocenter har valts av användaren
    a) Det genereras en engångskod som visas för användaren.
    b) I bakgrunden sparas engångskoden i en databas tillsammans med tidpunkt och en koppling till inloggad användare.
    c) Användaren går till Infocenter och ber att få aktivera sin personverifierade multifaktorsinloggning
    d) Personal kontrollerar ID-handling* enligt metod 3 eller 5 och skriver därefter in engångskoden i Kontohanteringsportalen. Om information hittas i databasen att användaren påbörjat en personverifiering (enligt 5.b ovan) och att den inte är äldre än 24 timmar får personalen upp information om användaren (namn, personnummer), inkl. bild ifall sådan finns.
    e) Om det är flaggat att användaren har fler andra faktorer och att andrafaktorerna måste kontrolleras manuellt kommer de olika faktorerna att listas i Kontohanteringsportalen tillsammans med en textbox bredvid. Personalen ber användaren att göra om steg 1-3 för varje faktor och kontrollerar att rätt metod används samt noterar varje ny engångskod i Kontohanteringsportalen vid rätt metod. Inte förrän alla metoder har en korrekt kod kan personalen fortsätta.
    f) Om personnumret stämmer överens med ID-handlingen och att ID-handlingen är giltig väljer personalen vilken typ av ID-handling som använts och fyller i ID-handlingens referensnummer och personens

nationalitet i kontohanteringsportalen.

Om personnummer saknas görs en riskbedömning att det är rätt individ och ID-handlingens referensnummer, personens namn, nationalitet samt födelsedata sparas undan.

g) Personalen godkänner personverifieringen och personens konto läggs i en AD-grupp som kan signalera AL3. För att personal ska kunna godkänna personverifiering måste denne vara inloggad i kontohanteringsportalen med AL3.

5.2.6
Alla AL-nivå ändringar sparas på användaren och kan kontrolleras i databasen vid behov.

5.2.7
Uppgifter som har lagts in av användaren själv kan även ändras av användaren. Rättningar av övriga uppgifter görs i källsystemen av behöriga användare.

5.2.8
Endast användare som är identifierade på AL2 eller högre, och som är systemadministratör i identitetssystemen eller kontoadministratör kan hantera konton och då endast de konton som de är behöriga att hantera.

Personal som hanterar AL3-aktivering (se ovan) måste vara inloggade med AL3 nivå för att kunna utfärda AL3-aktiveringar.

5.3 Credential Renewal and Re-issuing

5.3.1
I kontohanteringsportalen kan alla användare byta sitt lösenord och sin andra faktor.

5.3.2
För att byta lösenord måste användaren först ange sitt nuvarande lösenord och sedan det nya lösenordet direkt i webbläsaren (ej SAML/SSO). Det nya lösenordet måste följa lösenordspolicyn för att få bytas.

För att uppdatera en andra faktor måste användaren först logga in med multifaktorsinloggning.

5.3.3
Användare som behöver återställa sitt lösenord måste åter genomgå utlämningsprocessen enligt 5.2.5. Kontroll av personnummer eller ID-handlingens referensnummer, namn, nationalitet och födelsedata görs för att säkerställa att det rör sig om samma individ.

Om ovan information saknas görs en riskbedömning att det är rätt individ genom att till exempel kontakta den anställdes chef eller kontrollera studentens kurstillhörighet (fråga studenten vilka kurser hen går och jämför med Ladok).

Användare som behöver återställa sin andra faktor kan göra det genom att hämta ut en engångskod via kontohanteringsportalen. Engångskoden, som endast är giltig i en timme, används för inloggning i portalen för hantering av andra faktorer.

För att få möjlighet att hämta ut en sådan engångskod krävs en sessionskod. Den kan erhållas via en extern elektronisk identitet med AL3 eller infocenter. Sessionskoden är unik för varje tillfälle, kan bara användas en gång, och är giltig i 24 timmar.

Om användaren valt extern elektronisk identitet med AL3 måste användaren genomgå utlämnandeprocessen, men i stället för att användaren läggs med i en AL3-grupp i sista steget genereras sessionskoden.

Om användaren valt infocenter måste användaren gå till infocenter och visa giltig ID-handling som verifieras enligt 5.2.5. Infocenter kan sedan generera sessionskoden i kontohanteringsportalen och lämna den till användaren.

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 spärras genom beslut av LiU:s IT-säkerhetsgrupp. En användare kan också begära att få sitt eget konto spärrat.

Spärren innebär att lösenordet slumpas, befintliga tokens revokeras och att kontot spärras för återaktivering. Detta gäller omedelbart i identitetshanteringssystemen.

Om en användare förlorar kontrollen över en andra faktor kan användaren logga in portalen för multifaktorsinloggning med sitt lösenord och en annan andra faktor och ta bort den förlorade faktorn. Om användaren saknar en annan andra faktor kan användaren spärra multifaktorsinloggning via kontohanteringsportalen.

Vid en sådan spärr tas alla andra faktorer bort från användarens konto och en ”dummy faktor” läggs till för att förhindra inloggning utan multifaktorsinloggning.

Spärrning av multifaktorsinloggning kan också genomföras av LiU:s IT-säkerhetsgrupp, kontoadministratörer eller kundcenter.

Då en användare inte längre är verksam vid LiU påbörjas en avvecklingsfas av identiteten. Beroende på om användaren är student, anknuten eller anställd ser avvecklingsfasen olika ut men resulterar alltid i att kontot stängs av och rättigheter tas bort. I alla ovan fall tappar kontot affiliering vid avstängningsögonblicket.

5.4.2
Om ett konto spärrats av säkerhetsskäl måste spärren tas bort av behörig personal för att användaren ska kunna återaktivera inloggningen. Innan spärren tas bort informeras användaren om anledningen till spärren och om eventuella åtgärder (utöver lösenordsbyte) som behöver tas.

Användaren måste sedan åter gå igenom kontoutlämningsprocessen enligt 5.2. Efter spärrning av multifaktorsinloggning måste användaren genomgå re-issuing enligt 5.3.

Användare vars konto stängts då de inte längre varit verksamma vid kan återöppna sitt igenom kontoutlämningsprocessen enligt 5.2 om de har ny verksamhet vid LiU. Efter aktivering måste anställda även aktivera multifaktorsinloggning.

5.4.3
Om ett konto spärrats på grund av en säkerhetsincident informeras användare om anledningen samt vad den bör tänka på för att det inte ska hända igen.

Om en större säkerhetsincident händer där många konton påverkas eller om en enskild säkerhetsincident sker på grund av tekniska- eller organisatoriska processbrister, sker en utredning av händelsen och åtgärder planeras där det är möjligt.

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
Alla användarnamn som genereras sparas i kontohanteringsportalen för att aldrig återanvändas. I de fall då en användare åberopar radering av personuppgifter genom GDPR, raderas all data förutom användarnamnet. Om användaren kommer tillbaka kommer den få ett nytt användarnamn.

Alla kontohändelser som rör inloggningsinformation loggas centralt.

5.5.2
System som används för kontohantering bedöms ha en tillgänglighet högre än 95% och ingår i bevakning utanför kontorstid. LiU har dock ingen formell SLA för dessa eller andra system.

5.6 Credential Validation/Authentication

5.6.1

LiU:s identitetsutgivare följer SWAMID:s rekommendationer och teknikprofiler.

5.6.2

Stängda konton kan ej autentisera och inloggningsuppgifter valideras alltid vid autentisering.

5.6.3

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

5.6.4

En SSO session är endast giltig i 8 timmar. Efter det måste användaren logga in på nytt.