HÖGSKOLAN
I SKÖVDE

SWAMID Identity Management Practice Statement

Denna tillitsdeklaration har godkänts av IT-chef David Olsson 2023-12-05

Dnr HS 2023/866

Innehållsförteckning

Dokumenthistorik

Datum	Utförare	Kommentar
2023-08-25	Karina Malik	Utkast, inskickat till Swamid Operations för en första granskning
2023-11-13	Karina Malik / Anders Gustavson	Reviderad och kompletterad efter Fredrik Domeij´s (SWAMID) synpunkter, inskickad till Swamid Operations för ytterligare granskning
2023-11-21	Karina Malik / Anders Gustavson	Reviderad och kompletterad efter Fredrik Domeij´s, Björn Mattssons och Pål Axelssons synpunkter, inskickad till Swamid Operations för ytterligare granskning
2023-12-01	Karina Malik / Anders Gustavson	Reviderad och kompletterad efter Fredrik Domeij´s, Pål Axelssons och Björn Mattssons synpunkter, inskickad till Swamid Operations för ytterligare granskning
2023-12-05		SWAMID Operations har granskat vår IMPS och anser att vi uppfyller kraven i profilen och kommer att rekommendera SWAMID Board of Trustees att godkänna vår uppdatering

1. Inledning

Högskolan i Skövde (Högskolan) har varit medlemmar i SWAMID sedan 2010. Vi använder oss av SWAMID´s inloggningstjänst för att våra användare på ett säkert och enkelt sätt ska få tillgång till nationella och internationella IT-resurser.

Vi uppfyller SWAMID Assurance Level 1 och 2 och ansöker om förnyat uppfyllande.

Högskolan i Skövde kommer att använda svensk e-legitimation som komplement vid kontoaktivering samt kommer även att bekräfta personer utan svenskt personnummer för SWAMID AL2 genom eduID.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1

Högskolan i Skövde, med organisationsnummer 202100-3146, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev.

4.1.2

De viktigaste lagarna och förordningarna som styr 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 identitets- 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. Gällande personuppgiftslagstiftning och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med skyddade personuppgifter.

Studenternas personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok och därför gäller även förordningen (SFS 1993:1153) om redovisning av studier, m.m. vid universitet och högskolor för hanteringen av studenternas personuppgifter vid användaradministration.

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

4.1.3

Lagringsmedia (hårddiskar, m.m.) i datorer och serversystem som innehåller information om elektroniska lösenordsuppgifter eller annan känslig information, m.m. får ej överlåtas.

Vid återanvändning inom verksamheten raderas innehållet på enheten med raderingsprogramvara och ominstalleras.

När hårdvaran tas ur drift skrivs innehållet i lagringsmediat över med raderingsprogramvara samt lämnas för destruktion till kontrakterad mottagare.

4.2 Notices and User Information

4.2.1

För åtkomst till Högskolan i Skövdes datorsystem krävs ett användarkonto. Högskolans användarvillkor finns tillgängliga på: https://www.his.se/styrdokument/

4.2.2

Innan användarkontot kan börja användas så måste Högskolans användarvillkor godkännas.

Detta sker genom att:

- behörig användare tar del av och godkänner användarvillkoren vid aktivering av konto på Högskolans webbsida

4.2.3

När nya datorregler fastställs skickas ett e-postmeddelande till alla användare som har ett aktivt användarkonto som exponeras mot SWAMID.

En nyhet publiceras även på vår interna Medarbetarportal samt i vår Studentportal.

4.2.4

Vid elektroniskt godkännande sparas ett godkännande av användarvillkoren i Högskolans system för användaradministration.

Vid undertecknande av en ansvarsförbindelse sparas denna i befintligt arkiv.

4.2.5

Högskolan i Skövde har en generell tjänstebeskrivning av SAML2 WebSSO (IdP) samt en integritetspolicy för hantering av personuppgifter inom ramen för identitetsutgivaren. Båda dessa finns tillgängliga på Högskolans webbsidor. https://www.his.se/styrdokument/

4.3 Secure Communications

4.3.1

Högskolans nätverk är uppdelad i zoner där system placeras utifrån grad av känslighet och risknivå. Åtkomst till de olika zonerna regleras i första hand genom accesslistor.

Åtkomst till servrar regleras utifrån sina arbetsområden och via särskilda domänadministratörskonton samt AD-grupptillhörighet (olika säkerhetsgrupper inom AD:et).

4.3.2

Nycklar finns endast på de servrar som använder dem och lagras inte på andra håll.

Dessa skyddas med Windows autentisering via AD-konto.

4.3.3

Ingen okrypterad åtkomst är tillåten över nätverket för kataloganslutna servrar.

All nätverkskommunikation ska skyddas med användning av TLS eller motsvarande kryptering.

4.3.4

Samtliga entitetsnycklar använder minst 2048 RSA.

4.4 Security-relevant Event (Audit) Records

4.4.1

Gjorda förändringar avseende användarkonton och behörigheter i Högskolans katalog och behörighetssystem loggas vid exekvering av tillhörande systemskript. I loggarna sparas datum, tidstämpel och information om användarobjektet som behandlats samt vad som utförts.

Vid automatisk och manuell körning av skripten sparas också ytterligare information i systemets databas, t ex utförarens användar-id och eventuella fel.

Förändringar avseende befintliga användarkonton handläggs i ett ärendehanteringssystem där information om användare, handläggare och åtgärd sparas.

På Högskolan loggas all trafik för att kunna säkerställa spårbarhet i den händelse Högskolan behöver utreda incident eller annan negativ händelse. Även lyckade och misslyckade inloggningsförsök sparas för att i efterhand kunna utreda eventuella säkerhetsincidenter.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1

Ett lösenord ska vara sammansatt enligt kraven för komplexa lösenord i Active Directory, samt minst vara 8 tecken långt.

Högskolans samtliga autentiseringstjänster SAML2 (IdP- Shibboleth), CAS samt Radius (primärt för eduroam) autentiserar samma konton som även används vid direkt inloggning via Högskolans gemensamma behörighetskatalog Active Directory. AD begränsar även återanvändning av lösenord samt vanligt förekommande ord och kontonamn.

5.1.2

All kommunikation mellan de olika delarna som används för hantering av användare och lösenord sker krypterat.

TLS-SSL skyddar under transport mot avlyssning och förvanskning av data.

Replikeringen mellan domänkontrollanter i Active Directory sker enligt Microsofts standardiserade säkerhetsmetod för replikering. Högskolan synkroniserar inte lösenord med externa leverantörer, t.ex. molntjänster.

5.1.3

Användarna upplyses om att skydda och att inte dela med sig av sina inloggningsuppgifter till någon annan i Högskolans användarvillkor för datorkonto. De uppmanas även att använda olika lösenord för olika system, speciellt inte samma lösenord som för Högskolans användarkonto i privata sammanhang.

5.1.4

Som skydd mot missbruk finns tekniska protokoll men Högskolans behörighetssystem Active Directory förhindrar också användning av så kallade ”enkla ord” som val av lösenord.

Som skydd samt hantering för hot mot Högskolans IT-system övervakas system och nätverkstrafik, i realtid. Även loggfiler kontrolleras regelbundet efter misstänkta aktiviteter och Högskolans användare informeras löpande om ökade hotbilder utifrån ett IT-säkerhetsperspektiv.

Ett skydd mot skadlig kod finns i Högskolans system för e-post men finns även lokalt på både server- och klient-sidan.

Högskolan har en organisation för IT-incidenthantering som samverkar med Myndigheten för samhällsskydd och beredskap. Syftet är att stärka samarbetet mellan myndigheter och andra organisationer inom IT-incidenthantering.

Enligt *Policy för vägledande principer för Högskolan i Skövdes IT-utveckling* ska det säkerställas att äldre befintliga system och tjänster avvecklas när nyare ersättningsystem och tjänster införs.

Högskolan genomför uppdateringar av Högskolans servrar (patchhantering) enligt ett schema, samt patchar servrar vid avisering om kritiska korrigeringar.

5.2 Credential Issuing

5.2.1

Den administrativa DNS-domänen his.se används alltid vid attributrelease till det system där användare vill logga in. Detta oberoende om det är SAML2 eller eduroam.

5.2.2

Samtliga identitetsservrar vid Högskolan använder unika identifierare.

5.2.3

Varje användare har ett eller flera unika användarnamn som inte återanvänds till andra användare.

5.2.4

Om en användare har mer än ett användarkonto, dvs. är både student och anställd, väljer användaren vid det aktuella inloggningstillfället vilket användarkonto som ska användas.

5.2.5

Aktivering och återställning av lösenord för person som arbetar på Högskolan och registrerade studenter görs enligt något av nedanstående alternativ.

Kontoaktivering och återställning av lösenord för medarbetare och studenter antagna till kommande kurs eller program hanteras i kontoportalen (konto.his.se) enligt något av nedanstående alternativ.

Obekräftad användare (AL1):

Student:

- En handläggare skickar i kontohanteringssystemet en engångskod till den e-postadress studenten har i NyA, vi använder personnumret i Ladok för att hämta e-postadressen från NyA och engångskoden knyts till detta personnummer så att vi i kontoportalen kan koppla rätt personnummer till kontot.
  Ett CAPTCHA-test genomförs i samband med aktiveringen.
- Inloggning via antagning.se (NyA) med en obekräftad användare (AL1) där personnummer/interimspersonnummer stämmer med vad som finns i Ladok.

Bekräftad användare (AL2):

- Besök vid helpdesk med godkänd identitetshandling
  - Kontroll enligt nedanstående beskriven Rutin för identitetskontroll
  - Användaren får en tidsbegränsad AL2-engångskod

- Inloggning via eduID (se 2.1.1)
- Inloggning via BankID (svensk e-legitimation LoA3)
    - Identifierare för att knyta person till identiteten är svenskt personnummer.
- För medarbetare och student som ej är folkbokförd i Sverige skickas AL2-aktiveringskod till den adress som är bestyrkt genom foto på legitimation och kopia på till personen adresserad hushållsräkning.
- För medarbetare som är folkbokförd i Sverige skickas aktiveringskod till folkbokföringsadress erhållen av HR-avdelningen.
- För de användare som inte har svenskt personnummer kopierar vi godkänd identitetshandling och antecknar användarkonto. Detta sparas i en pärm inlåst i Helpdesk och kontrolleras vid nästa identifiering för att säkerställa att det är samma person som hämtade ut ett användarkonto.

Enbart Student:

- Inloggning via antagning.se (NyA) med en bekräftad användare (AL2) där personnummer stämmer med vad som finns i Ladok.
- För student som är folkbokförd i Sverige skickas aktiveringskod till folkbokföringsadress enligt Ladok (personal.his.se)

eduID

Användare som kan att skapa ett eduID:

- Personer med svenskt personnummer folkbokförda i Sverige
- Personer från EU/EES med e-legitimation inom eIDAS
- ePassport via SvipeID

För att få tillitsnivå AL2 på digital väg så verifieras inloggningen mot eduID. eduID-kontot måste uppfylla tillitsnivå AL2.
Kriterier för att automatiskt godkännas är att födelsedata, förnamn, efternamn och e-postadress stämmer överens vid kontroll mot uppgifter från Primula (medarbetare) eller Ladok (Student) För personer med svenskt personnummer gäller svenskt personnummer som identifierare. Uppfylls inte kraven blir personen uppmanad att kontakta helpdesk. Helpdeskpersonal med minst AL2-behörighet kontrollerar uppgifterna och använder/föreslår någon av ovanstående metoder för att autentisera personen. Kriterierna för att manuellt godkännas är att:

- födelsedata stämmer överens
- ett av förnamnen stämmer överens när det finns fler förnamn, olika stavningar som ger näst intill eller identiskt uttal av förnamnet
- efternamnet stämmer överens, olika stavningar som ger näst intill eller identiskt uttal av förnamnet
- e-postadress måste stämma överens

Förregisterade identifierare

För studenter kopplar vi personnummer eller interimspersonnummer de har i Ladok till användarkonto på Högskolan.

För personal som har svenskt personnummer kopplar vi användarkontot till personnummer.

För de användare som inte har svenskt personnummer kopierar vi godkänd identitetshandling och antecknar användarkontot. Detta sparas i en pärm inlåst i Helpdesk.

För personer utan svenskt personnummer som loggat in till konto.his.se via eduID görs en automatiserad riskbaserad bedömning om inloggad person går att unikt koppla samman med en person i Ladok, där födelsedata måste vara samma, för- och efternamn vara tillräckligt lika, e-postadress i eduID ska vara samma som i Ladok samt att användaren måste vara bekräftad AL2 i eduID

Godkända identitetshandlingar:

- ett pass eller identitetskort som uppfyller Polisen krav,
- ett pass som uppfyller ICAO Doc 9303 eller
- ett nationellt identitetskort inkl. information om medborgarskap enligt EU-förordning 562/2006.

5.2.6

Högskolan sparar samtliga utfärdade användarkonton och deras statushistorik i huvuddatabasen för lärosätets katalog- och behörighetssystem

5.2.7

- Kontaktuppgifter såsom mobilnummer och privat e-postadress registreras av användaren på konto.his.se.
- Student och personal har möjlighet att uppdatera sina kontaktuppgifter.
- Då nya uppgifter registreras eller uppdateras ska detta verifieras genom SMS eller e-postmeddelande.

5.2.8

Behörighet till kontohanteringssystem tilldelas endast till personal som behöver det i sin tjänst. Samtliga innehar bekräftade identitet, alltså AL2. Tillitsnivå kontrolleras vid inloggning

Vid Högskolan verifieras personal som hanterar användaridentiteter genom en id-kontroll. Detta sker samtidigt som individen godkänner en särskild ansvarsförbindelse för administratörskonton.

5.3 Credential Renewal and Re-issuing

5.3.1

Samtliga användare på Högskolan kan byta lösenord på sitt användarkonto.

5.3.2

Lösenordsbyte sker i webmail samt i Windows klienten, användaren behöver då ange sitt gamla lösenord samtidigt som de skriver in det nya.

5.3.3

- Metoderna beskrivna i 5.2.5 kan också användas för återställning av lösenord

    - Används en AL1-metod för återställning av lösenord på ett AL2-konto så nedgraderas kontot till ett AL1-konto

- En engångskod erhålles i Helpdesk mot uppvisande av identitetshandling.
- För personer utan svenskt personnummer ska alltid kontroll göras av tidigare uppvisad identitetshandling vid återställning av lösenord samt upphöjning av tillitsnivå. Kontrollera t.ex passnummer, utgivande land eller att passet innehåller samma namn och födelsedata
- Kontakt med Helpdesk för att få engångskod skickad till folkbokföringsadress
- För lösenordsåterställning kan beställning göras av två separata ”tidsbegränsade” engångskoder som var och en skickas till e-post och via SMS och som behöver användas i kombination

    - Om student är registrerad vid Högskolan för innevarande termin samt har en förregistrerad e-postadress och mobilnummer registrerat i Högskolans användardatabas.
    - Om personal har förregistrerad e-postadress och mobilnummer i Högskolans användardatabas

För att kunna få en engångskod via e-post+SMS som kan användas för att logga in i kontoportalen, och där göra en lösenordsåterställning, så krävs att personen har förregistrerade och verifierade uppgifter om e-postadress och mobilnummer i vår kontodatabas.

För att kunna registrera och verifiera kontaktuppgifter behöver man logga in i kontoportalen, via antingen

- eduID eller antagning.se med AL2 bekräftat konto,
- eller ett befintligt HS-konto (AL2),
- eller mha en engångskod (har man inga verifierade uppgifter sedan tidigare så får man den via folkbokföringsadress, besök i helpdesk etc, dvs AL2).
- antagning.se med ett obekräftat konto eller ett befintligt HS-konto (AL1). Engångskoder som skickas till kontaktuppgifter som har verifierats efter dessa typer av inloggningar betraktas som AL1-engångskoder.

Verifieringen görs genom att vi skickar en kod till angiven e-postadress resp. SMS-nummer från formuläret, koden kan bara användas så länge man är inloggad i portalen (sessionen ”lever”).

När man verifierar kontaktuppgifter så sparar vi på vilken AL-nivå man var inloggad, när konton aktiveras sparas på vilken AL-nivå de är skapade.

5.4 Credential Revocation

5.4.1

Den som överträder, eller misstänks överträda Högskolans datorregler kan få sitt användarkonto avstängt under utredning.

Behörigheten till användarkontot är tidsbegränsad och kommer att upphöra när studierna, anställningen, projektet eller motsvarande upphör. Högskolan har rätt att avsluta ett användarkonto som varit inaktivt mer än sex månader om ingen annan överenskommelse finns, såsom vid t.ex studieuppehåll, tjänstledighet, m.m.

Samtliga användarkonton kan inaktiveras för att hindra inloggning. Detta sker genom att:

- användaren försöker använda fel lösenord fler än 50 gånger i en följd
- IT-personal inaktiverar kontot manuellt

En användare kan få sitt användarkonto inaktiverat på egen begäran.

5.4.2

Se avsnitt 5.3.3 för metoder om återställning av användares lösenord.

Vid informationssäkerhetsincidenter eller om Högskolan får kännedom om att ett lösenord inte längre är hemligt inaktiveras användarkontot och användaren blir informerad om metoder för att kunna återställa lösenordet.

Om användaren har registrerat en privat e-postadress eller mobilnummer i vår användardatabas skickar vi meddelande på det sättet. I annat fall skickar vi brev till folkbokföringsadressen.

5.4.3

För att reducera risken för obehörig åtkomst till lösenord gäller följande policy för lagring och transport av lösenord:

- Lösenord ska aldrig presenteras i läsbar form.
- Lösenord ska aldrig kommuniceras via epost, telefon eller motsv. Undantag konsulter som anlitas vid akuta ärenden som får ett tillfälligt lösenord via telefon.

För att reducera risken för automatiserade gissningsattacker mot lösenord ska inloggningen vara skyddad genom s.k. rate limiting som förhindrar en inkräktare att göra många upprepade lösenordsgissningar på kort tid.

I Högskolans gemensamma inloggningstjänst är detta utformat enligt följande:

- 50 felaktiga gissningar innan automatisk kontolåsning.
- 5 minuters automatisk kontolåsning efter maximalt antal felaktiga gissningar.
- Räknaren över antalet felaktiga gissningar nollställs efter korrekt inloggning eller efter 60 minuter efter senaste felaktiga inloggningsförsök.

Vi granskar orsaken till avstängningen från fall till fall och hanterar det antingen genom utbildningsinsats till berörda användaren eller en teknisk lösning om sådan är relevant.

5.5 Credential Status Management

5.5.1

Högskolan sparar samtliga utfärdade användarkonton och deras statushistorik i huvuddatabasen för lärosätets katalog- och behörighetssystem.

5.5.2

Högskolans separata identifieringstjänster SAML2 samt RADIUS kommunicerar med den centrala katalogtjänsten (AD). De är samtliga konfigurerade utifrån höga krav avseende tillgänglighet och följer uppsatta riktlinjer avseende kontinuitetsplanering gällande IT-drift.

5.6 Credential Validation/Authentication

5.6.1

Högskolans identifieringstjänster SAML2 och RADIUS är uppsatta och installerade utifrån rekommenderade installationsskript och instruktioner som finns för respektive tjänst. Detta innebär att det inte sker några avvikelser från bestämda protokoll vilket uppfyller de rekommendationer som kommer från externa kravställare såsom SWAMID.

5.6.2

När ett användarkonto inaktiverats eller tagits bort i behörighetssystemet Active Directory, kan en lyckad autentisering för det berörda användarkontot inte längre genomföras.

5.6.3

För samtliga av Högskolans identifieringstjänster krävs att användaren matar in sitt användarnamn och lösenord. I vissa fall förekommer möjligheten för användaren att spara inloggningsuppgifter för förenklad inloggning, t ex för den specifika tjänsten eduroam, vilket sker på användarens eget ansvar.

5.6.4

Maximal sessionstid för en inloggad användare via IdP för en tjänst med en his.se-adress följer SWAMIDS rekommendationer på maximalt 12 timmar.

6 Tidigare version

Denna tillitsdeklaration ersätter SWAMID Identity Management Practice Statement med diarienummer HS 2021/62