2022-11-22

Identity and Management Practice Statement

Högskolan Väst

Högskolan Väst
Mattias Andersson

1 Inledning

Detta dokument beskriver hur Högskolan Väst system och rutiner för konto- och behörighetshantering genom Högskolan Västs katalog- och behörighetstjänst MittKonto. Beskrivningen omfattar kontots fulla livscykel. Syftet är att uppfylla kraven för SWAMID AL1 och AL2.

Högskolan Väst
Mattias Andersson

4 Organizational Requirement

4.1 Enterprise and Service Maturity

4.1.1 Lärosätets/myndighetens/stiftelsens organisationsnummer

Högskolan Väst är en statlig utbildningsmyndighet som regleras av lagar, förordningar och regleringsbrev med organisationsnummer 202100–4052.

4.1.2 Tillämpbara lagrum

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 högskolans uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

Högskolan Väst katalog- 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 samt 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 kontohanteringssystemet.

Personaluppgifter hämtas och behandlas i personalsystemet Primula. Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.

4.1.3 Rutiner för destruering av lagringsmedia

Lagringsmedia innehållandes elektroniska identiteter får ej säljas eller överlåtas. Använd lagringsmedia skickas för destruktion.

4.2 Notices and User Information

4.2.1 Användarvillkor

Användarvillkor och regler finns publicerade på högskolans webb
https://www.hv.se/student/it-support/regler-och-riktlinjer/

4.2.2 Godkännande

I samband med att användaren skapar sitt konto godkänner personen användarvillkoren.

4.2.3 Ny ansvarsförbindelse

Användare godkänner en eventuell uppdatering genom att mottaga och läsa ett informationsmejl som skickas ut till samtliga användare inom organisationen. Inloggning i något av våra system innebär automatiskt en bekräftelse på att användaren läst och accepterat den nya ansvarsförbindelsen.

4.2.4 Loggning av ansvarsförbindelse

Eftersom inget förnyat godkännande vid uppdatering av reglerna krävs så sparas inte när användaren godkänt reglerna.

4.2.5 Service Definition

Tjänstedefinition finns publicerad på vår webb https://www.hv.se/student/it-support/tjanstedefinition/

Behandling av personuppgifter - GDPR finns beskrivet på vår webb https://www.hv.se/om-webbplatsen/integritetspolicy/

4.3 Secure Communications

4.3.1 Personal med teknisk åtkomst

Administrativ tillgång till system för behörighetskontroll är begränsad till ett fåtal individer på SIT-avdelningen. Beslut om administrativ tillgång till systemen fattas av IT-chef.

Administrativa konton profil- och gruppstyrs, och efter avslutad anställning stängs personens konto automatiskt.

4.3.2 Nyckel och lösenordshantering

All form av hantering av privata nycklar och lösenord är krypterade förutom vid ett tillfälle. Det är när MittKonto synkroniserar användaruppgifter till Active Directory (AD) genom Microsoft Forefront Identity Manager (FIM). Lösenorden står i klartext tidsmässigt under mindre än en minut. Detta sker i vår virtuella servermiljö på ett internt nät där enbart Databas-administratörer har åtkomst till den aktuella informationen.

4.3.3 Kryptering

All nätverkskommunikation till och från identitets-system skyddas med användning av TLS eller likvärdig kryptering.

4.3.4 Enhetsnycklar (Entitiy Keys)

Alla nyckellängder är av typen 2048-bitars RSA eller längre.

4.4 Security-relevant Event (Audit) Records

4.4.1 Loggning av säkerhetsrelaterade händelser

Alla förändringar som sker på ett användarkonto loggas i MittKonto med korrekta tidsstämplar lokalt på det interna servernätet. Dessa loggar sparas i minst 12 månader. Inloggningsförsök, sparas med korrekta tidsstämplar i Azure, loggarna sparas i 30 dagar och kan endast kommas åt av begränsad mängd personal på SIT-avdelningen med rätt behörighet.

Alla inloggningsförsök som görs genom ADFS loggas i en Log Analytics workspace i Azure i 30 dagar.

5 Operational Requirements

5.1 Credential Operating Environment

5.1.1 Lösenordspolicy

Lösenord måste vara minst 9 tecken långa och innehålla minst en gemen (liten bokstav) och en versal (stor bokstav), en siffra och specialtecken. Det innebär en entropi på mer än 24-bitar. Lösenorden kan ej återanvändas vid nästa lösenordsbyte.

5.1.2 Tekniska Protokoll

All kommunikation mellan olika system sker krypterat se punkt 4.3.3, 4.3.4. Protokollet TLS har per automatik inbyggt skydd mot återspeglingsattacker. Spegling av domänkontrollanter i Active Directory (AD) sker i enlighet med den metod och praxis från Microsoft gällande säkerhet för replikering. Högskolan Väst synkroniserar inga lösenord med externa leverantörer, t.ex. molntjänster så som Azure eller likvärdigt. Vi använder ADFS för SSO login.

5.1.3 Personligt ansvar

I den ansvarsförbindelse som användaren godkänner vid kontoskapandet framgår det att innehavaren är personligen ansvarig för användandet av kontot och att det ej får nyttjas av andra.

5.1.4 Rutiner för skydd mot missbruk

All hantering av hårdvara som har med kontohantering att göra har en begränsning till enbart säkra tjänsteprotokoll såsom HTTPS, SSH, LDAPS, Radius mm. De aktuella enheterna ligger på egna segmenterade IP-nät skyddade bakom Fortigate brandväggar, där också nätverkstrafiken loggas och analyseras i Fortianalyzer. Ansvar för hantering av säkerhetsuppdateringar och generella uppdateringar ligger på högskolans IT personal. Se även rubrik 4.3.3 ovan.

5.2 Cridential Issuing

5.2.1 Identitetshanterarens DNS-domän

Den administrativa toppdomänen HV.SE, som ägs av högskolan, används alltid vid inloggning till de system som användaren vill få tillgång till.

5.2.2 Globala unika identifierare för inloggningstjänsterna

Alla inloggningstjänster har en global unik identifierare. Till exempel entityID för SAML.

5.2.3 Hantering av användarnamn/konton

Samtliga identitetsservrar på Högskolan Väst använder unika identifierare.

Användarnamn är unika och representerar enbart en enskild person, dessa namn återanvänds inte.

5.2.4 Flera Användaridentiteter

I de fall där personen är student och övergår i anställd form görs studentens konto om till ett anställt konto. Det finns vissa så kallade studentmedarbetare som både är student och anställd, dessa konton är delvis begränsade i behörighet och administreras manuellt av IT personal.

5.2.5 Identifieringsmetoder

Samtliga konton som skapas blir AL1, metoder för att skapa konton beskrivs nedan

Personal

- **MittKonto**
  De anger sitt personnummer vilket genererar en kontroll av lagrade uppgifter om den angivna personen i högskolans system, som i sin tur har hämtat användarens personuppgifter från Primula. Om det angivna personnumret finns registrerat i högskolans system får de fylla i persondata och en captcha, de får då ett konto och ett användarnamn, lösenordet skapar de själva enligt punkt 5.1.1. Personal bekräftar sitt konto genom att få e-post med en unik tidsbegränsad engångslänk till privat e-post eller ett sms med en tidsbegränsad fyrsiffrig kod till privat mobiltelefon. Detta konto kan sedan användas direkt.
- **Folkbokföringsadress**
  Konto kan även skapas genom att en unik tidsbegränsad engångskod skickas till personens folkbokföringsadress.

Student

- **MittKonto**
  De studenter som har blivit antagna till kurs eller program på högskolan skapar sitt konto under MittKonto, de anger sitt personnummer vilket genererar en kontroll av lagrade uppgifter om den angivna personen i högskolans system, som i sin tur har hämtat användarens personuppgifter från Ladok. Om det angivna personnumret finns registrerat i högskolans system får de fylla i persondata och en captcha, de får då ett konto och ett användarnamn, lösenordet skapar de själva enligt punkt 5.1.1. Studenten bekräftar sitt konto genom att få e-post med en unik tidsbegränsad engångslänk till privat e-post eller ett sms med en tidsbegränsad fyrsiffrig kod till privat mobiltelefon. Detta konto kan sedan användas direkt.
- **Folkbokföringsadress**
  Konto kan även skapas genom att en unik tidsbegränsad engångskod skickas till personens folkbokföringsadress.

HÖGSKOLAN VÄST

2022-11-22

Studenter och personal som skall lyfta sitt konto till AL2 från AL1 behöver de identifiera sig vilket sker på nedan fyra sätt.

1. För att identifiera sig och erhålla AL2 status på sitt konto behöver användaren påvisa att användaren har kontroll på kontot. Detta görs genom att en unik tidsbegränsad engångstoken, kopplad till användarens konto, på 5 siffror kan skrivas ut av en servicecenteradministratör efter att användaren uppvisat en av nedan godkända identitetshandlingar. Användaren loggar sedan in i MittKonto och bekräftar sin identitet genom att ange den unika engångstoken man fått utskriven vid uppvisande av en av nedan godkända identitetshandlingar för servicecenteradministratör. Användaren identifierar sig genom att mata in den unika tidsbegränsade engångstokenen i MittKonto.
2. För individer som inte har möjlighet att besöka högskolans servicecenter finns också möjligheten att genom MittKonto begära ut en unik tidsbegränsad engångstoken till användarens folkbokföringsadress. Användaren loggar sedan in i MittKonto och anger den unika tidsbegränsade engångstoken den fått skickad till sin Folkbokföringsadress. Folkbokföringsadress hämtas för personal ur högskolans personaladministrationssystem Primula, för studenter från Ladok. Denna metod ger AL2.
3. Användaren kan också identifiera sig med BankID när användaren är inloggad i MittKonto. Denna metod ger AL2.
4. Användaren kan också identifiera sig genom NyA när användaren är inloggad i MittKonto. Om kontot i NyA är AL2 ger det AL2 hos Högskolan Väst.

Samtliga alternativ kräver att det finns minst ett förnamn, efternamn och personnummer. För utländsk personal och studenter som ännu inte erhållit svenskt personnummer används interimsnummer för utländska stunder, och ett samordningsnummer för personal. Personal som ej har fått ett samordningsnummer får av högskolan de fyra sista siffrorna i personnummer genererat enligt standarden Sxxx. Även utländska studenter som ej finns i Ladok kan manuellt läggas in i MittKonto och då få personnummer genererade enligt standarden Sxxx.

Godkända identitetshandlingar

Högskolan Väst
Mattias Andersson

- Inom Sverige giltig identitetshandling enligt Skatteverkets föreskrifter om identitetskort (SKVFS 2009:14).
- Ett pass som uppfyller ICAO Doc 9303.
- Ett nationellt identitetskort inkl. information om medborgarskap enligt EU-förordningen 562/2006.
- Ett körkort utfärdat från och med 2013 inom EU/ESS enligt EU-direktiv 2006/126/EC.

5.2.6 Förändring av AL nivåer

I MittKonto visas på individens informationssida vilken AL-nivå som personen erhåller. Samt en logg på när vederbörande erhöll sin nuvarande AL nivå, med tid och datum. Denna information visas enbart för teknisk och administrativ personal med adekvata rättigheter.

5.2.7 Ändring av självuppgiven information

Information om anställd personal hämtas från Högskolan Västs personalsystem Primula per automatik. Fullständigt namn och adress hämtas från folkbokföringsregistret till Primula och uppdateras per automatik.

Information om studenter hämtas från Ladok per automatik.

Gäster läggs upp manuellt av personal på SIT-avdelningen, se punkt 4.3.1. Ett tidsbegränsat intervall sätts på kontot vid kontots skapande.

Anställda kan ändra alla uppgifter som ej är hämtade ur personalsystemet Primula, detta görs på sidan MittKonto. Studenter kan ändra personinformation som inte hämtats från Skatteverket genom Ladok som inloggade i MittKonto. Detta innefattar exempelvis privat telefon och e-post eller ICE-kontakter.

5.2.8 Krav på identitetsgranskningen

Vid Högskolan Väst är all personal som hanterar användaridentiteter eller som är systemadministratörer identifierade enligt SWAMID AL2 och har inloggning på motsvarande nivå.

5.3 Credential Renewal and Re-issuing

5.3.1 Möjlighet till lösenordsbyte

Alla användare, studenter och personal, har möjlighet att byta sitt lösenord via inloggning på MittKonto.

5.3.2 Lösenordsbyte

Vid byte av lösenord via websidan MittKonto kan användaren byta sitt lösenord, för att göra detta måste personen ange sitt befintliga lösenord för att aktivera det nya.

5.3.3 Lösenordsåterställning

Återställning av lösenord kan ske genom att ett tidsbegränsat engångslösenord skickas till av användare tidigare registrerad privat e-post. Detta genererar AL1 nivå på användarkontot.

Återställning av lösenord kan också ske genom att ett tidsbegränsat engångslösenord skickas till av student tidigare registrerat telefonnummer som SMS. Detta genererar AL1 nivå på användarkontot.

Återställning av kontot kan också ske genom att en tidsbegränsad engångstoken skickas till användarens folkbokföringsadress. Användarens folkbokföringsadress hämtas från Primula för personal, och Ladok för studenter. Detta genererar en AL2 nivå på användarkontot.

BankID kan användas som ett alternativ. Om användaren verifierar sig med BankID vid lösenordsåterställning erhåller användaren AL2 status. Vi säkerställer att kontots förregistrerade personnummer matchar personnumret som ges vid BankID-inloggning.

I de fall användaren vid kontoskapande angivit och verifierat både privat e-post och mobiltelefonnummer kommer en tidsbegränsad engångslänk skickas till användarens privata e-post, och en unik tidsbegränsad engångstoken (sifferkod) skickas till användarens privata mobiltelefon via SMS. Används den unika tidsbegränsade engångstoken tillsammans med den unika tidsbegränsade engångslänken i e-posten så kan användaren behålla sin AL2 status.

5.4 Credential Revocation

5.4.1 Inaktivering av användarkonton

Samtliga konton kan inaktiveras för användning. Konton kan även inaktiveras och kräva lösenordsåterställning vid exempelvis misstanke om kontointrång, missbruk eller disciplinärende. Manuell inaktivering och tvingande lösenordsbyte genomförs av AL2 verifierad och behörig IT-personal med adekvat behörighet.
Användaren har möjlighet att begära att sitt eget konto inaktiveras.

När ett konto stängs av administrativa skäl förläggs det med en spärr som omöjliggör att användaren kan återta kontrollen av kontot genom lösenordsåterställning till dess att spärren manuellt lyfts av AL2 verifierad och behörig IT-personal.

5.4.2 Återaktivering av användarkonton

Återaktivering av personalkonto kan ske på begäran av närmsta chef. Aktiveringen av personalkonton genomförs av behörig personal i ServiceCenter eller behörig IT personal.

Studenter kan själva återaktivera sitt konto via MittKonto. Maximal förlängning av kontot för studenter är 12 månader efter sista datum i senast avslutade kurs. Kontot kan öppnas även efter 12 månader, men då är det en månad åt gången som kontot är aktivt. Väljer student att 6 månader efter datum för senast avslutade kurs återaktivera sitt konto så kommer kontot vara aktivt i 6 månader, tills tiden om 12 månader efter sista datum för senast avslutade kurs är uppnådd. När ett konto stängs av administrativa skäl, blir användaren informerad via sin verifierade SMS eller privata e-post om skälet till att kontot stängs. När kontot återaktiveras informeras användaren via sin verifierade sms eller privata e-post att de måste göra en lösenordsåterställning för att komma åt sitt konto. Kontot blir AL1 efter återaktivering.

5.4.3 Rutin vid incidenthantering

Högskolan Västs rutinbeskrivning kring hantering av incidenter, inklusive säkerställande att samma incident inte sker igen finns beskrivet i bilaga ”IT-Incidenthantering v.1.4.pdf”.

I samband med säkerhetsincidenter minimerar vi risken att dessa återuppstår genom ett retrospektiv som görs som en del av vår incidenthanteringsrutin efter hanterad incident.

5.5 Credential Status Management

5.5.1 Historik över utfärdade identiteter

Högskolan Väst loggar alla konto och lösenordsändringar. Tillgång till dessa loggar är begränsade till ett fåtal personer på SIT-avdelningen med särskild behörighet. MittKonto bevarar information om varje UID (User ID) som utfärdats och säkerställer att ett användarnamn är unikt och aldrig återanvänds.

5.5.2 Tillgängligheten för identitetstjänsten

Identitetsutfärdaren (IDPerna) har samma tillgänglighetskrav som uppfyller behoven till interna system, så som Ladok.

5.6 Credential Validation/Authentication

5.6.1 Validering av rättigheter

Både SAML2- och Radius-installationerna uppfyller dessa krav eftersom protokollen är konfigurerade enligt instruktioner från SWAMID och eduroam.org.

5.6.2 Inaktivering av konton

När ett konto inaktiveras eller stängs deaktiveras det i Active Directory så att autentisering ej kan göras. Studentkonton hos studenter som avslutat sina studier stängs automatisk efter avslutade studier. Studenter kan själva återaktivera kontot efter avslutade studier. (5.4.2) Personalkonton med tidsbegränsad anställning stängs så snart tiden för personens slutdatum uppnåtts i personalsystemet. Konton med tillsvidareanställningar stängs per automatik när anställningen upphör, vilket regleras i personalsystemet Primula.

5.6.3 Autentisering vid inloggning

SAML2-baserad webbinloggning och eduroam kräver att användaren matar in sitt användarnamn och lösenord för att användaren ska få tillgång till tjänsten. Webbinloggning har en SSO-funktionalitet som aktiveras efter att användaren loggat in. Eduroam har ingen sådan men användaren får ett certifikat efter inloggning.

5.6.4 Sessionstider

För SAML2-baserad webbinloggning uppfyller Högskolan kraven med att den maximala längden för SSO-sessionen är tolv timmar. Den maximala giltighetstiden från att användaren gör inloggningen, eller använder SSO-sessionen, tills att tjänsten släpper in användaren i tjänsten är fem minuter.