IDENTITY AND MANAGEMENT PRACTICE STATEMENT

Högskolan i Borås

Innehållsförteckning

1. Inledning

Högskolan i Borås är medlem i identitetsfederationen SWAMID som omfattar de flesta lärosäten, forskningsinstitut och andra myndigheter som är relaterade till svensk forsknings- och utbildningssektor. Medlemskapet ger förutsättning för samarbete inom digitalt identitetsutbyte. Högskolan använder profilerna SWAMID Assurance Level 1 och 2 inom kontohanteringsprocessen.

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.

Högskolan i Borås, organisationsnummer 202100-3138, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev.

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.

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 enligt aktuell personuppgiftslagstiftning.

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.

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

De lagringsmedia som innehåller eller kan innehålla känsliga data som till exempel lösenord eller personuppgifter tas om hand i säkert förvar för att vid behov destrueras enligt gängse normer.

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.

Användarvillkor finns publicerad på vår webb

- Anställd:
  https://www.hb.se/anstalld/for-mitt-arbete/it/natverk-och-datorer/nyttjande-av-hogskolans-natverk/
- Student:
  https://www.hb.se/student/mina-studier/studiemiljo--sakerhet/rattigheter-och-skyldigheter-som-student/nyttjande-av-hogskolans-datanatverk/

Användarna godkänner att följa föreskrivna regler och hålla sig uppdaterade om gällande regler vid kontoskapandet. Vid förändringar av föreskrivna regler meddelas användarna via e-postutskick.

Tjänstebeskrivning och hantering av personuppgifter vid federerad autentisering SAML2

- Högskolan i Borås använder SWAMIDs best practice policys och aktuell tjänstebeskrivning samt personuppgiftshantering publiceras på högskolans publika webb med länkar på den gemensamma inloggningstjänsten (idp.hb.se).
  https://www.hb.se/anstalld/for-mitt-arbete/it/natverk-och-datorer/gemensam-inloggningstjanst

4.3 Secure Communications

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

IT-personal med teknisk åtkomst

- Personer med behov av administratörsrättigheter har ytterligare ett personalkonto som äger extra behörighet, ett så kallat administratörskonto. Administratörskontot tilldelas endast de personer som har ett behov av detta. När en person får andra arbetsuppgifter eller lämnar sin anställning raderas administratörskontot. För anställda som går på tjänsteledighet inaktiveras administratörskontot men personalkontot är fortsatt aktivt.

Nycklar som behöver lagras i klartext, skyddas av operativsystemets behörighetssystem där endast administratörer har tillgång. Nycklar utfärdas genom tjänsten SUNET TCS och är därmed minst 2048 bitar. Giltighetstiden för nycklarna är som längst ett år. Självsignerade certifikat i tjänstens metadata har längre giltighetstid, dock max tio år, med en nyckelstorlek på minst 2048 bitar.

Ett webbaserat lokalt tillgängligt system med flerfaktorinloggning och kryptering av data hanterar våra delade hemligheter i form av exempelvis lösenord. Vem som får tillgång till systemet hanteras på uppdrag av IT-chef genom beställning via ärendehanteringssystem. Kontohantering för systemet hanteras manuellt av systemansvarig och it-säkerhetsansvarig. Systemet loggar alla händelser.

IdM-systemet vid Högskolan i Borås använder idag Microfocus eDirectory och Microsoft Active Directory för att lagra elektroniska identiteter. Utfasning av eDirectory-tjänster pågår till förmån för Active Directory. Produktsviten NetIQ Identity Manager används för processtöd, behörighetsstyrning och kontohantering. Utöver detta finns det egenutvecklad programvara i .NET samt bakomliggande databaser för att stödja identitetshanteringen, bland annat kontoprovisionering- och självserviceportal. Samtliga ingående delar i IdM-systemet är implementerade enligt respektive leverantörs best practice för att säkerställa säker kommunikation. Krypterat standardprotokoll används mellan de olika tjänsterna inom IdM-systemet.

4.4 Security-relevant Event (Audit) Records

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

Alla statusförändringar för elektroniska identiteter loggas till extern SQL-databas och kan visas vid behov. Denna loggning sker från alla relevanta delar i IdM-system, portaler samt kringliggande stödsystem.

Auditing- och systemloggar för alla ingående delar i IdM-systemet och IdP skickas till en extern ELK-stack. Detta innefattar säkerhetshändelser, lyckade och misslyckade inloggningsförsök och sparas så länge det behövs för att kunna utreda säkerhetsincidenter.

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.

De protokoll som används är i enlighet med SWAMIDs tekniska profiler SAML WebSSO och Eduroam. Det protokoll som framför allt används för kommunikation är TLS/SSL. Som autentiseringstjänster stöds SAML2, LDAPS samt Radius (Eduroam).

För användarkonton krävs att lösenord skall uppfylla Microsoft AD Complex password policy, motsvarande i eDirectory. Minsta längd på lösenordet är åtta tecken. Lösenorden kan ej återanvändas vid lösenordsbyte.

Kontouppgifterna för Eduroam lagras i ett eget Active Directory skilt från primär användarkatalog. Ett 7-siffrigt lösenord genereras på användarens begäran för att säkerställa att inte samma lösenord används i övriga katalogtjänster.

Användaren uppmanas att hålla kontouppgifter hemliga genom användarvillkor och lösenordspolicy.

Systemet för kontoadministration använder egna systemkonton mot katalogtjänsten.

För skydd mot hot finns brandvägg aktiverat på alla system och loggning sker till ELK-stack med larm. Rutiner finns för att hålla systemen uppdaterade och för att begränsa skada vid säkerhetsrelaterade incidenter.

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process including issuing of credentials and binding of other information to the Subject. Furthermore, the Identity Provider and its Subjects must be uniquely identified.

Högskolan i Borås identitetshanterare ingår i DNS-domänen hb.se och har namnet idp.hb.se vilket är globalt unikt.

Kontoutdelning

Studenter initierar kontoskapningsprocessen genom att från systemet konto.hb.se begära ut ett konto, välja lösenord och kontrollera sina uppgifter. Informationen till detta konto samlas från Ladok och skickas som ett uppdrag till IdM-systemet. IdM-systemet skapar sedan identiteten samt kontot och meddelar sedan kontoskaparsystemet att kontot är färdigt för användning.

Ny personalidentitet läses in från lärosätets personalsystem men kan också läggas upp som en så kallad manuell timanställning efter beställning via formulär i IdM-systemets användargränssnitt.

Legitimering

För vad som räknas som giltig legitimation används identitetshandlingar enligt polisens regler för utlämning av pass. Vi godkänner även nationellt ID-kort utfärdat av land inom EU/ESS samt pass.

Identifieringsmetoder

För användare med svenskt personnummer används normalt detta. För användare utan svenskt personnummer används normalt födelsedata, namn och utfärdandeland av pass kombinerat med en riskbaserad bedömning.

De fördefinierade identifierare som vi tillåter vid federerad inloggning är personnummer (svenskt/interim) från SWAMID-godkänd IdP eller svensk e-legitimation tillitsnivå 3 eller 4.

Kontoutdelningsprocesser

Personal/extern

Kontotyp personal och extern kan skapas antingen automatiskt via HR-system eller manuellt av servicedesk. Alla personal-/externkonton skapas som AL2.

Anställd personal via HR-system:

- Etablering av identitet i HR-system vid anställning
- Identitet synkas över till katalogsystem och konto skapas

- Användaren kvitterar ut kontouppgifter och sätter ett personligt lösenord efter uppvisande av giltig legitimation vid personligt besök till servicedesk

Övrig personal och externa:

- Etablering av identitet sker i IdM-system av servicedesk
- Konto skapas
- Användaren kvitterar ut kontouppgifter och sätter ett personligt lösenord efter uppvisande av giltig legitimation vid personligt besök till servicedesk

Studenter

All kontoutdelning för studenter sker på AL1-nivå om ej högre nivå uppnåtts vid autentisering.

Kontotyp student ges möjlighet att välja en av följande aktiveringsmetoder:

- OTP-kod till e-postadress och/eller mobilnummer som finns registrerat i Ladok
- OTP-kod via personligt möte
- Inloggning via federerad SAML2

Vid aktivering med OTP-kod via e-post och/eller svenskt mobilnummer:

- Beställning av OTP-kod initieras av att användaren anger sitt personnummer varpå e-postadress och/eller mobilnummer läses in från Ladok. Kod med begränsad giltighetstid genereras och skickas till dessa.
- Om koden har slutat att gälla kan en ny kod beställas genom att börja om aktiveringsprocessen.
- Metod loggas och identiteten får via denna metod AL1-nivå vilket noteras på identiteten.
- Vid inloggning med OTP-kod krävs CAPTCHA

Vid aktivering med OTP-kod från servicedesk via personligt möte eller telefon:

- Beställning av OTP-kod inkommer via servicedesk.
- Vid personligt möte uppvisar användaren giltig legitimation och mottager utskrift av tidsbegränsad OTP-kod. Vid telefonsamtal görs kontroll av att inringande telefonnummer stämmer med det som angivits i Ladok för personen med det uppgivna personnumret varpå OTP-kod skickas som SMS.
- Metod loggas och kontot får via denna metod AL1-nivå vilket noteras på identiteten.
- Vid inloggning med OTP-kod krävs CAPTCHA

Vid val av inloggning via federerad SAML (t.ex. antagning.se eller eduId.se):

- Användaren väljer sin önskade inloggningskälla.
- Användaren genomför en inloggning mot vald källa vilket levererar de attribut som behövs för att processen ska kunna fortsätta.

- Kraven för detta, förutom ett konto vid källan, är även att identitetsutgivaren skickar med personnummer (svenskt/interim). Om ett komplett personnummer ej kan erhållas från identitetsutgivaren så skapas inte heller något konto.
- I dagsläget har kontot som skapas samma AL-nivå som uppnåddes vid inloggningen, dock högst AL2.
- För att säkerställa att rätt AL-nivå uppnåtts vid federerad inloggning kontrolleras att assurance-attributet innehåller önskad AL-nivå. Detta kontrolleras även mot IdP'ns certifieringsnivå i metadata.

Vid val av inloggning via svensk e-legitimation tillitsnivå 3 eller 4:

- Användaren väljer sin önskade e-legitimation.
- Användaren genomför en inloggning mot vald e-legitimation vilket levererar de attribut som behövs för att processen ska kunna fortsätta.
- I dagsläget har kontot som skapas AL2-nivå.
- Matchning görs mellan personnummer från inloggning och fördefinierat personnummer på konto.

Gemensamt för studenternas aktiveringsmetoder:

- Systemet kontrollerar att identiteten finns öppen för aktivering.
- Aktivering av kontot och sättande av lösenord sker automatiskt efter att kontot skapats av IdM-systemet.
- Kontot får högst samma tillitsnivå som uppfylls av autentiserat konto (AL1/AL2).
- Kontots behörigheter sätts utifrån de uppgifter vi har i IdM-systemet, som t.ex kurser och program.
- För att kontoskapande ska kunna genomföras måste det finnas möjlighet att uppnå minst en registrering. Detta innebär minst en antagning till kurstillfälle som är öppet för registrering och ej har hinder för registrering, eller minst en registrering på ett kurstillfälle för pågående termin.

Gästanvändare/Walkin

Kontotyp Gästanvändare genereras och delas ut av servicedesk eller av anställd personal som härrör från personalsystemet. Kontotyp Walkin genereras och delas ut av biblioteket. För båda kontotyperna uppnås tillitsnivå AL1.

Gästanvändare:

- Konto skapas i IdM-systemet med en giltighetstid på maximalt 48 timmar (maximalt två veckor om det genereras av servicedesk).
- Vid kontoskapandet anges en ansvarig för gästkontot.
- Inloggningsuppgifterna skrivs ut för överlämning till gästen.
- Inga identifierare sparas för kontot. Dessa konton kan inte återställa sitt lösenord.

Walkin:

- Konto skapas i IdM-systemet med en giltighetstid som är som längst till bibliotekets normala stängningstid samma dag.
- Inloggningsuppgifterna skrivs ut av bibliotekspersonal för överlämning.
- Inga identifierare sparas för kontot. Dessa konton kan inte återställa sitt lösenord.

Höjning av tillitsnivå

Höjning av tillitsnivån kan ske via IdM-systemets användargränssnitt och kräver då att supportpersonal gör en godkänd identifiering av individen enligt tidigare beskrivna regler. Denna identifikationsnivå loggas även i samband med höjningen.

Användaren kan själv höja sitt konto till AL2-nivå via självhjälpsportal om detta kan uppnås vid inloggning med annan SWAMID-godkänd IdP eller svensk e-legitimation tillitsnivå 3 eller 4. Denna identifikationsnivå loggas även i samband med höjningen.

Tillitsnivån kan endast sänkas manuellt av en kontoadministratör. Denna åtgärd kan beställas via servicedesk och innebär att kontots AL-nivå sänks. För att åter höja AL-nivån kan användaren genomföra aktiviteterna enligt ovan. Alla förändringar loggas.

Användning av unikt användarnamn för olika identiteter över tid

En identitet kan återanvändas för kontotyp personal och extern om det är samma identitet, d.v.s. samma personnummer.

Identitetstyp	**Unikt användarnamn**	**Exponeras till SWAMID**	**Återanvändning av unikt användarnamn**
Personal	JA	JA	NEJ (Ja, om samma identitet)
Extern	JA	JA	NEJ (Ja, om samma identitet)
Student	JA	JA	NEJ
Gästanvändare för lokal nätaccess	JA	NEJ	NEJ
Gästanvändare	JA	JA (affiliate)	NEJ
Walkin	JA	JA (library-walk-in)	NEJ
Funktion	NEJ	NEJ	JA

Om en användare (identitet) har både student- och anställdkonto, kan användaren välja att logga in som student eller anställd genom att autentisera sig med respektive konto.

Självserviceportal

Självserviceportal ger användare möjlighet att byta eller återställa lösenord på rätt AL-nivå samt generera ett separat lösenord för tjänsten Eduroam.

Självuppgiven information

För personal måste all information ändras via personalsystem vilket sköts av HR-administratör. Denna information distribueras sedan ut till alla kringliggande system.

För studenter tas all självuppgiven information från Ladok och måste uppdateras via Ladoks studentportal. Vid förändring i Ladok distribueras denna information ut till alla kringliggande system.

Krav för användarhantering

Vid tilldelning av rollen för kontoadministration i IdM-systemet kontrolleras manuellt att personen har minst AL2-nivå. En person med kontoadministrationsroll får inte sänkas till AL1 utan att rollen först tagits bort (detta kan enbart göras av ett fåtal personer på IT som har en rutin att följa).

5.3 Credential Renewal and Re-issuing

The purpose of this subsection is to ensure that Subjects can change their credential and get new credentials when lost or expired.

Lösenordsbyte

Lösenord kan bytas i självserviceportalen. Detta sker genom att användaren loggar in med sina aktuella inloggningsuppgifter och sedan byter aktuellt lösenord mot ett nytt. Innan byte tillåts måste användaren ange sitt nuvarande lösenord i direkt samband med lösenordsbyte. Kontroll sker mot lösenordspolicyn i katalogtjänsten innan lösenordet kan bytas. Byte kan även ske i Windowsklienten genom ”Ctrl+Alt+Del”-menyn och loggas av auditfunktion.

Lösenordsåterställning

Ett konto tillåts inte att sänka sin tillitsnivå, tex genom att använda AL1-metoder vid lösenordsåterställning. Dock kan en kontoadministratör manuellt sänka tillitsnivån på kontot till AL1 vilket gör att AL1-metoder kan användas vid lösenordsåterställning. Alla förändringar loggas. Lösenordsåterställning kan göras via självserviceportalen med hjälp av samma metoder som vid kontoutdelning enligt ovan, men med nedan undantag.

- **AL1**
  Engångskod via tidigare uppgivna kontaktuppgifter såsom bekräftad e-postadress eller tidigare bekräftat SMS-nummer på minst AL1-nivå. Uppgifterna är bekräftade under tiden som kontot hade tillitsnivå AL1. Koden har begränsad giltighetstid. Vid beställning av engångskod krävs CAPTCHA.
- **AL2**
  Engångskod via tidigare uppgivna kontaktuppgifter: bekräftad e-postadress och bekräftat SMS-nummer. Två olika koder skickas till de angivna uppgifterna. Båda koderna skall anges för att lösenordsåterställning skall ske. Koderna har begränsad giltighetstid. Vid beställning av engångskoder krävs CAPTCHA.

Lösenordsåterställning via federerad inloggning kräver, på samma sätt som för kontoutdelning i avsnitt ovan, att den federerade inloggningen uppnår samma eller högre AL-nivå som kontot i källan. De fördefinierade identifierare som vi tillåter vid federerad inloggning är personnummer (svenskt/interim) från SWAMID-godkänd IdP eller svensk e-legitimation tillitsnivå 3 eller 4. Vid federerad inloggning tillåter vi endast personnummer som förregistrerad identifierare och ej riskbaserad bedömning baserad på annan information.

Lösenordsåterställning kan även ske genom personligt möte med vår servicedesk. Vid manuell lösenordsåterställning används identitetshandling mot personnummer eller riskbaserad bedömning gjord av teknisk personal baserad på jämförelse av namn, födelsedata och kontaktuppgifter (e-post/mobilnummer).

5.4 Credential Revocation

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

Vid misstanke om missbruk har kontoadministratörer skyldighet att spärra en användares konto genom att inaktivera kontot samt sätta ett nytt okänt lösenord. Det som föranledde spärren meddelas genom att information skickas till de privata kontaktuppgifterna, om dessa saknas måste innehavaren själv kontakta servicedesk. Innehavaren av kontot kan sedan återfå kontrollen genom att kontakta servicedesk och genomföra en lösenordsåterställning.

Vid säkerhetsincident inaktiverar kontoadministratör aktuellt konto. Det som föranledde spärren meddelas genom tex privat e-postadress eller SMS om dessa finns. Om dessa saknas måste innehavaren själv kontakta servicedesk. Innehavaren av kontot kan sedan återfå kontrollen genom att kontakta servicedesk och genomföra en lösenordsåterställning.

Spärr av konto kan ske på användarens begäran. Innehavaren av kontot kan sedan återfå kontrollen genom att kontakta servicedesk och genomföra en lösenordsåterställning.

Giltighetstiden beräknas från källsystemen eller är manuellt inlagda. Då giltighetstiden har passerats inaktiveras kontot, det flyttas till karantän, kontot stängs och behörigheter tas bort. Ett halvår efter karantäntiden raderas kopplade konton och tjänster. Identitetsobjektet ligger kvar med endast personnummer och användar-id för att garantera att kontonamnet är unikt över tid. Då studenten enligt Ladok inte längre har några registreringar flyttas kontot efter 12 månader till karantän. Om ny kontoaktivering sker och användaren identifieras som samma individ återaktiveras konton i karantän förutsatt att kontot ännu inte har raderats. IdM-systemet återanvänder tidigare utfärdade kontonamn för personal och extern om det är samma individ som kommer tillbaka. För studenter utfärdas alltid ett nytt konto om det tidigare är raderat.

För gästkonton och walkinkonton inaktiveras och raderas dessa omedelbart när giltighetstiden för kontot passerats.

I händelse av att ett konto spärras eller nedgraderas till lägre tillitsnivå på grund av incident så upprättas alltid en incident-rapport där orsaken utreds och dokumenteras och vilka åtgärder som tas för att förhindra att händelsen kan uppstå igen.

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.

IdM-systemet innehåller en komplett historik över utfärdade identiteter och via ett sökgränssnitt kan kontoadministratörer söka fram information knuten till individer med både aktiva och inaktiva konton. Historiken rensas efter fem år men användarnamn samt personnummer eller motsvarande sparas för evigt för kontotyp personal och extern. Studenternas grundläggande identitetsuppgifter sparas men användarnamn tas bort och återanvänds aldrig.

För kontotyp personal och extern lagras tidigare använt användarnamn så denna ej kan användas på en annan identitet.

För kontotyp student lagras det senast använda användarnamnet och kan återanvändas så länge som kontot endast är arkiverat. När kontot sen slutligen tas bort skapas ett helt nytt användarnamn med prefix baserat på det innevarande året. På grund av längden på arkiveringen och giltighetstiden innebär detta att inget studentanvändarnamn kommer att återanvändas på en annan identitet.

IdM-systemet och dess katalogtjänst, kontoadministrationssystem, SAML2 inloggningstjänst samt medräknat underliggande infrastruktur som nätverk mm ska ha samma upptid som interna tjänster.

5.6 Credential Validation/Authentication

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

Högskolan I Borås har implementerat samtliga tekniska protokoll enligt SWAMIDs rekommenderade best practice och använder SWAMIDs rekommenderade installation för Shibboleth som utgångspunkt för lokal konfiguration.

För att inloggning ska kunna ske måste kontot vara aktivt och öppet för inloggning.

Om det inte finns någon aktiv inloggningssession måste användaren logga in på nytt.

Idag tillåter vi SSO-sessioner på maximalt 12 timmar.