SWAMID Identity Management Practice Statement

1. Inledning

Högskolan i Halmstad är en statlig högskola vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. Högskolan är medlem i SWAMID. Detta dokument beskriver hur Högskolan uppfyller SWAMID AL1 och SWAMID AL2.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1 Lärosätets organisationsnummer

Högskolan i Halmstad, organisationsnummer 202100-3203, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev.

4.1.2 Tillämpbara lagrum

De viktigaste lagarna och förordningarna som styr högskolans arbete är regeringsformen (SFS 1974:152), tryckfrihetsförordningen (SFS 1949:105), myndighetsförordningen (SFS 2007:515), högskolelagen (SFS 1992:1434) och högskoleförordningen (1993:100). Regleringsbrevet utställs årligen av regeringen och styr lärosätets uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

Lärosätets centrala användardatabas userdb (som är källa till AD och LDAP) 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. Dataskyddsförordningen (EU 2016/679) och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.

Studenters personuppgifter hämtas huvudsakligen 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 userdb. Ett mindre antal studenter hanteras manuellt. Detta gäller kurser som ges i samarbete med andra lärosäten.

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

4.1.3 Rutiner för destruering av lagringsmedia

Uttjänta datorer och diskar returneras till leverantören. I avtalet definieras hur leverantören hanterar diskdata för returnerade diskar.

4.2 Notices and User Information

Vid aktivering av användarkonto samt vid byte av lösenord accepterar användaren aktivt användarreglerna (AUP). Reglerna finns också länkade bl.a. från aktiveringssidan.

Högskolans service definition inkl. policy för hantering av personuppgifter har diarienummer I 2020/36 och är publicerad här.

Anvisningar för användning av IT-resurser samt kontoregler har diarienummer I 2018/68.

Vid ändring av regler informeras samtliga användare via intranät och lärplattform om att ändring gjorts.

Support ges via Helpdesk; helpdesk.hh.se eller helpdesk@hh.se.

4.3 Secure Communications

Lösenorden i den lokalt lagrade databasen är krypterade med ett asymmetriskt krypto med nyckellängd på 4096 bitar. Krypteringsnycklar skyddas mot åtkomst genom rättighetsstyrning i filsystemet. Delade hemligheter skyddas genom att de förvaras säkert och åtkomstskyddat med begränsad åtkomst till enbart behöriga personer utanför IT-systemen.

Kommunikationen mot stödsystemen AD och LDAP från klienter och konsumenter av användardata sker över krypterade protokoll och är begränsad av brandväggsregler och accesslistor.

Backup av servrar som hanterar skyddsvärda användaruppgifter överförs krypterat till backup-systemet.

Krypteringsnycklar som används för säker kommunikation är minst 2048 bitar.

4.4 Security-relevant Event (Audit) Records

4.4.1 Loggning av säkerhetsrelaterade händelser

I Userdb loggas namnbyte, personnummerbyte eller lösenordsbyte. Lyckade och misslyckade inloggningar till centrala system loggas på resp. server.

Userdb är endast åtkomligt för ett begränsat antal personer, och inloggning loggas (identitet och IP-nummer).

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1 Autentiseringsmekanismer

Användarkontonas lösenord ska innehålla:

- Minst 14 tecken
- Minst en versal
- Minst en gemen
- Minst en siffra eller specialtecken

Lösenord får inte bytas till ett lösenord man har, har haft eller som finns med i lista över vanliga lösenord.

Vid inloggning i helpdesksystemet uppmanas användare med lösenord som inte bytts på länge att byta.

5.1.2 Protokoll

All inloggning som görs med våra användarkonton sker krypterat med HTTPS, LDAP-TLS, IMAP-S eller POP3S.

5.1.3 Information till användare rörande missbruk

Enligt Högskolans användarregler ska inte de lösenord som används till Högskolans tjänster återanvändas på andra platser eller meddelas till andra personer.

5.1.4 Rutiner för tekniskt skydd mot missbruk

Systemen patchas regelbundet, loggning sker, dedikerade maskiner används. Separerat eduroam-lösenord från andra tjänster.

5.2 Credential Issuing

5.2.1 DNS-domän

Högskolan i Halmstad har dnsdomän hh.se.

5.2.2 Each Identity Provider instance MUST have a globally unique identifier

Högskolan har unika ID för SAML WebSSO och radius (eduroam).

5.2.3 Hantering av användarkonton

Personliga konton är unika och återanvänds inte till annan person.

Högskolan i Halmstad strävar efter att uppnå SWAMID AL2 på alla personliga konton.

5.2.4 Kontoinnehavare med flera konton

Vid inloggning väljer kontoinnehavaren vilket konto som ska användas, i de fall innehavaren har mer än ett konto.

5.2.5 Etablering av personliga konton

All normal etablering av konton sker via en webbtjänst vid Högskolan.

Studenter med gällande antagning eller registrering kan själva skapa sitt studentkonto.

Personalkonto skapas på begäran från HR-avdelningen eller tjänstestället.

Studentkonto för personal knyts till personens personalkonto via personnumret och hanteras i övrigt på samma sätt som övriga konton.

Alla konton registreras med namn och personnummer (födelsedata när inte personnummer är tillgängligt). För personer med svenskt personnummer används detta vid framtida kontroll av kontoinnehavaren, för personer utan verifierbart svenskt personnummer görs en riskbedömning baserat på namn och födelsedata.

För varje skapat konto loggas vilken metod som använts. I de fall engångskoder skrivits ut loggas vem som gjort utskriften. Engångskoder är giltiga i tre veckor från utskriftstillfället.

SWAMID AL2-verifiering kan ske via

- bekräftad id på minst SWAMID AL2-nivå via de godkända tjänsterna eduID eller antagning.se
- användning av engångskoder, skickade till digital brevlåda via Mina meddelanden eller folkbokföringsadressen, alternativt hämtade på Servicecenter mot uppvisande av legitimation.
- inloggning via svenskt BankID (motsvarar tillitsnivå 3)

SWAMID AL2-verifiering för person med skyddade personuppgifter uppnås genom att brev skickas via skattemyndigheten, alternativt hämtas med äkta legitimation på servicecenter.

Godkända svenska legitimationer vid utlämning är de legitimationer som Polisen godtar vid utlämning av pass. Legitimationens äkthet kontrolleras i systemet 365-id.

När ingen av ovanstående metoder kan användas (t ex personer utan svenskt personnummer som inte kan besöka Servicecenter) kan användarkonto på AL1-nivå skapas enligt följande:

- Student som sökt via universityadmissions: efter angivande av T-nummer skickas engångskod till den e-postadress som användes för ansökan i antagningssystemet.
- Personal och övriga studenter: Personen e-postar in ett foto på en legitimationshandling. Namn och födelsedatum skall stämma med uppgifter kända av lärosätet. Engångskod skickas då till självuppgiven e-postadress. Captcha måste användas.

eduroam
Alla personliga konton kan användas på eduroam, men med ett annat lösenord. Lösenordet kan bytas till ett lösenord som sätts av systemet.

5.2.6 Byte av tillitsnivåer för enskilda användare

Tillitsnivån kan höjas av användaren

a) genom inloggning med ett konto (från annan inloggningsmetod i 5.2.5) med högre AL/LOA-nivå.
b) genom lösenordsbyte. Vid lösenordsbyte uppnås den AL-nivå (dock högst SWAMID AL2) som är knuten till den inloggningsmetod som använts enligt 5.2.5. Kontot får den nya AL-nivå som verifieringen motsvarar.

Tillitsnivån kan vid särskilda händelser sänkas av behörig administratör inom IT-avdelningen.

Ändring av AL-nivå loggas i userdb.

5.2.7 Ändring av självuppgiven information

Studenter kan ändra självuppgivet mobiltelefonnummer och e-postadress i Ladok. Dessa uppgifter kan läsas online från kontodatabasen.

För personal används inte självuppgivna uppgifter.

5.2.8 Krav på identitetsgranskningen

Anställda som arbetar med kontohanteringen har användarkonton enligt SWAMID AL2, och har genomgått en grundläggande utbildning i regelverk och rutiner.

5.3 Credential Renewal and Re-issuing

5.3.1 Användares frivilliga lösenordsbyte

Användare byter lösenord via självservice.

5.3.2 Krav vid lösenordsbyte

Vid lösenordsbyte måste användaren ange tidigare lösenord för att kunna sätta nytt lösenord.

5.3.3 Återställning av användares lösenord (bortglömt lösenord)

Återställning av lösenord sker med de metoder och de fördefinierade identifierarna som beskrivs i 5.2.5. Förutom metoderna som beskrivs i 5.2.5 kan användaren logga in med sin HH-identitet för att byta lösenordet.

Personal som loggat in med ett SWAMID AL2-konto kan byta lösenord på såväl sitt personalkonto som ett ev studentkonto. Båda kontona uppnår då AL2.

5.4 Credential revocation

5.4.1 Stängning av konto

Studentkonton stängs 18 månader efter senaste registrering.

Personalkonton stängs

a) 2 månader efter anställningens slut enligt Högskolans löneadministrativa system
b) När det datum som sattes vid kontobeställningen inträffar. Detta datum kan maximalt vara 1 år från senaste beställning (gäller personer som inte har aktiv månadsanställning). Beställning av sådant konto görs vid resp. tjänsteställe.

När användare begär att dess konto ska stängas utförs stängningen direkt (om studier/anställning är avslutad).

Vid upptäckt säkerhetsrelaterad händelse spärras kontot och inloggade sessioner bryts. Därefter informeras användaren via andra kanaler än det berörda kontot om vad som hänt. Användaren kan först därefter återöppna sitt konto.

5.4.2 Återöppning av stängt konto

Identifiering i samband med återöppning av stängt konto görs med metoderna i 5.2.5.

5.4.3 Minimering av risken av upprepning

Vid missbruk eller intrång utreds vad som hänt, för att dra slutsatser kring hur en upprepning kan motverkas och nya rutiner kan implementeras. Löpande ges utbildning till användare för att de ska använda sina kontouppgifter på säkert sätt.

5.5 Credential Status Management

5.5.1 Historik över utfärdade identiteter

Userdb loggar vem som skapar konto och hur det skapas. Användaren kopplas till sitt personnummer eller motsvarande. När studentkonton tas bort raderas all information om kopplingen mellan kontonamnet och studenten. För personalkonton behålls en lista över utfärdade användaridentiteter innehållande namn, personnummer, användarnamn. I studentidentiteter ingår alltid årtalet då kontot skapades, så om en student återkommer efter att kontot raderats får studenten ett nytt konto. Studentidentiteter raderas inte samma kalenderår som de skapas. Personal som återkommer, även efter att kontot raderats, får normalt samma kontonamn som tidigare.

5.5.2 Tillgängligheten för identitetstjänsten

Identitetstjänsten är avsedd att alltid vara tillgänglig för inloggning och kontoskapande. Korta planerade stopp kan inträffa i samband med uppdateringar av programvara.

5.6 Credential Validation/Authentication

5.6.1 Högskolan i Halmstad följer SWAMIDs profiler och rekommendationer, och strävar efter att använda SAML eller Azure-inloggning för alla outsourcade system.

5.6.2 Stängda konton

Avstängda eller inaktiverade konton kan inte användas för inloggning.

5.6.3 Inloggning

Vid inloggning måste användare använda sitt lösenord.

5.6.4 Återautentisering

Användare som använder en IT-tjänst måste ange sitt lösenord på nytt minst var 12e timma.