SOPHIA HEMMET
HÖGSKOLA

Stockholm den 28 November 2022

SWAMID Identity Management Practice Statement Template

SOPHIAHEMMET HÖGSKOLA
Box 5605, 114 86 Stockholm Valhallavägen 91 D Tel 08-406 20 00
Organisationsnummer 802006-8741 info@shh.se www.shh.se

SOPHIA HEMMET
HÖGSKOLA

1. Inledning

Sophiahemmet Högskola, SHH är en enskild Högskola.
Som medlem i Sunet och användare av dess tjänster och medlem av identitetsfederationen SWAMID.

Sophiahemmet Högskola har idag rutiner som följer AL2:s tillitsnivå,
med det ansöker vi härmed om att bli godkänd för tillitsnivå 2.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

Sophiahemmet Högskola organisationsnummer 802006-8741, är en enskild högskola vilket gör att största delen av lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr universitetets/högskolans arbete är regeringsformen (SFS 1974:152), tryckfrihetsförordning (SFS 1949:105), högskolelagen (SFS 1992:1434) och högskoleförordningen (1993:100), Lagen om tillstånd att utförda vissa tentamina 1993:792. 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 Microsoft Active Directory innehåller uppgifter om lärosätets organisation samt personuppgifter om alla som är verksamma vid lärosätet. Där med måste särskild hänsyn till behandling av personuppgifter tas enligt aktuell personuppgiftslagstiftning.

Som enskilt lärosäte arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informations-säkerhet.

Rutiner för destruering av lagringsmedia (4.1.3)

All kasserad lagringsmedia tas ur maskiner och destrueras i enlighet med säkerställd rutin i vårt dokumenthanteringssystem. Destruering sker hos Stena.

4.2 Notices and User Information

När studenter är antagna får de i antagningsmedelandet inför kursstart, instruktioner om hur de kan hämta ut sitt användarkonto efter de godkänt våra användarvillkor.

Godkännande och uthämtning sker på säkert sätt i vår e-tjänsteportal där studenterna verifierar sig med Bank-ID.

För personal sker kontoutdelning vid uthämtande av IT-arbetsplats(Dator, mobiltelefon, passerkort etc). Kontoutdelning sker då manuellt hos IT med uppvisande av giltig id-handling.

4.2.1
För antagna studenter finns aktuella användarvillkor alltid tillgängliga i vår e-tjänst efter inloggning med Bank-id.
För anställda finns användarvillkor tillgängliga i vårt dokumenthanteringssystem samt i vårt HR-system.

4.2.2
Anställda skriver under alla användarvillkor på papper vid anställningstillfället.
Därefter så hanteras skapande av konto och rättigheter via en beställning i e-tjänst av den anställdes chef innan utlämning av kontouppgifter sedan kan ske mot uppvisande av giltig id-handling.

4.2.3
Ett e-postmeddelande om justering av användarvillkor skickas ut vid eventuella uppdateringar för studenter med information om var de hittar de nya uppdaterade användarvilkoren.
Anställda får avisering via e-post ifrån vårt dokumenthanteringssystem när en justering av dokumentet med användarvillkor görs.

4.2.4
För studenter finns register över godkännande av användarvillkor i E-tjänstesystemet och arkiveras enligt befintlig dokumenthanteringsplan. Innan en student år åtkomst till sina kontouppgifter krävs inloggning med Bank-id och godkännande av användarvillkor.
För anställda lagras och arkiveras avtalen i personalsystem samt personalarkivet.

4.2.5
Swamid tjänstedefinition återfinns publicerad på:
https://www.shh.se/sv/om-webbplatsen/behandling-av-personuppgifter/swamid-tjanstedefinition/

4.3 Secure Communications

Sophiahemmet Högskola använder Microsoft Active Directory för hantering av kontoinformation, med utökad funktionalitet ADFS och SAML2 som inloggningshanterare. Vi använder SHA256 och TLS för kryptering.

Delade hemligheter och krypteringsnycklar skyddas enl gällande standard och rutiner.
Endast utpekad personal och tjänster har tillgång.

Sophiahemmet Högskolas IT-avdelning säkerställer att samtliga system har säkra rutiner för krypterad lagring och uppdaterade säkerhetscertifikat i enlighet med Sophiahemmet Sjukhus säkerhetspolicys. All datatrafik är krypterad enl standard TLS.
Krypteringsnyckel för Saml /ADFS är minst 2048 bitar RSA.

4.4 Security-relevant Event (Audit) Records

Samtliga händelser loggas. Loggning sker genom Active Directory, via Success and fault funktionalitet.
Loggning sker även på Exchange, ADFS, och shibboleth.
All trafik loggas i Fortigate brandväggen.
Loggar sparas I 6 månader I respektive system. Utöver detta skapas backuper, dagligvis, veckovis och månadsvis separat. Dessa sparas säkerhetsklassat ställe.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1(*5.2.5*)

Komplext lösenord med minst åtta tecken varav minst en stor bokstav, en liten bokstav och en siffra och en symbol krävs. Användarkonton låses efter 3 felaktiga försök.

5.1.2
Protokoll som skyddar mot ”message replay” är standardprotokoll, SSL/TLS, SHA 128, 256 kryptering.

5.1.3
I användarvillkor som användaren godkänner anges att kontouppgifter ej får spridas och att lösenord inte skall återanvändas i andra system.

5.1.4 Brandväggar hanterar all datatrafik. System för filtrering av spam används för e-post. Antivirusprogramvara används på all befintlig maskinvara.
Allting loggas I Active directory, befintliga program och tjänster.
Alla system och tjänster uppdateras löpande till senaste version för att tillhandahålla hög säkerhet.

Vid eventuellt missbruk låses konton efter 3 försök och IT informeras automatiskt via e-post till servicedesk@sophiahemmets.se. Missbruk av externt kopplade system anmäls via e-post abuse@sophiahemmet.se

5.2 Credential Issuing

5.2.1. Sophiahemmet Högskola äger och använder sig av domänen shh.se för dns uppslag.

5.2.2 IDP och radius server har unika identifierare under domänen shh.se

5.2.3 För varje användare skapas en unik användaridentitet som aldrig kommer återskapas.

5.2.4 Personal med student och personalkonto får välja vilket konto som skall användas.

5.2.5
Sophiahemmet Högskola använder AD Manager som portal för att skapa och säkerställa personalens användarkonton. Kopplingen till Ladok används för att skapa studentkonton i AD:t genom LIS-adaptern. Skapat konto synkas sedan över till vår e-tjänst där identifierare i båda systemen blir personnr. Utdelning av unika konton hanteras från AD:t, för alla användare knutna till högskolan. Kontouppgifter delas ut efter att identitet fastställts antigen via BankID och e-tjänsteportalen eller via uppvisande av giltig id-handling.

För studenter sker uthämtning av konto automatiskt i vår E-tjänst där Bank-ID krävs för åtkomst och fastställande av identitet, godkännande av Högskolans policys krävs även innan åtkomst kan ske till kontouppgifter.

Vid behov av manuell hantering sker Identifiering genom uppvisande av giltig id-handling och granskning av kontouppgifter mot giltig id-handling hos IT-stöd innan utlämnande.
Med giltig id-handling menas ett pass eller identitetskort som uppfyller Polis och passmyndigheternas krav enl ICA0 Doc9303 respektive EU-förordning 526/2006.
Riskbedömd för utrikesfödda pass eller id-handling.
Vidare för användare utan svenskt personnummer används identifierare så som passnummer, utfärdandeland och namn.

För nyanställda sker detta vid uthämtande av IT-arbetsplats(Dator, mobiltelefon etc).
Kontoutdelning sker då manuellt hos IT med uppvisande av giltig id-handling.
Giltig Identifierare är personnummer. Riskbedömd för utrikesfödda pass eller id-handling.
Vidare för användare utan svenskt personnummer används identifierare så som passnummer, utfärdandeland och namn.

Återställning sker i första hand i med ärende via e-tjänst och verifiering av identitet med Bank-ID eller vid uppvisande av giltig id-handling hos IT-avdelningen för anställda och hos IT-stöd för studenter.

Ovan metoder används för att säkerställa att konto är verifierat på SWAMID AL2-nivå.

5.2.6 Inte tillämpningsbar då alla användare är identifierade med AL2.

5.2.7 För studenter sker ändring av självuppgiven information utanför Ladok genom kontakt med Ladokansvarig. Detta sker via studieadministrativ E-tjänst där verifiering sker med Bank-ID.
Vid vissa justeringar kan det behövas att det styrks i e-tjänsten med personuppgiftsutdrag ifrån Skatteverket. För personal sker detta i IT servicedesk med underlag ifrån Skatteverket.

5.2.8
Kontoadministratörer och systemadministratörer uppfyller AL2

5.3 Credential Renewal and Re-issuing

5.3.1 -5.3.2 Frivilligt lösenordsbyte sker på eget initiativ av användaren via självbetjäningsportalen Iforgot(AdManager) med hjälp av befintligt lösenord.

5.3.3
Lösenordsåterställning sker med samma metoder och enl 5.2.5

5.4 Credential Revocation

5.4.1 Spärrande av inloggning sker vid upptäckt missbruk för all kontohantering, per automatik via brandväggar och filter eller felaktig inloggning. Användaren kan även själv begära att kontot stängs av.

Användarkonton inaktiveras efter avslutad tjänst/studier på högskolan via personalrutin via e-tjänst för personal samt för studenter efter besked ifrån Ladokansvarig. Inaktivering av användarkonton sker även automatiskt om kontot har varit inaktivt i 90 dagar.

5.4.2 Återaktivering av konto för både personal och studenter sker efter uppvisande av ID-handling och säkerhetsställande av uppgifter och ny lösenordsregistrering. Kan även ske via datumsatt period som är förutbestämd.

Framtvingande av lösenordsbyte sker genom spärrat konto och kontakt med användaren via e-tjänsten IT-stöd med BankID för sättande av nytt lösenord eller manuell återställning efter säkrad ID-kontroll vid Studentexpeditionen.

Kontoavstängning vid säkerhetsincident stängs kontot av och den berörde informeras vid avstängning om varför och ombeds kontakta IT-avdelningen för att kunna aktivera kontot igen. Efter kontakt med IT-avdelningen kan återaktivering ske enligt rutin 5.3.3.

5.4.3 Genomgång av befintliga säkerhetsrutiner genomförs kontinuerligt vid en incident och uppdateras vid behov. Övriga förändringar och viktig information skickas även ut vid behov.

5.5 Credential Status Management

5.5.1 Historiken över utfärdade identiteter sparas i Microsoft Active Directory och rensas aldrig. Allting loggas och tas daglig backup på. Utöver detta skapas backuper, dagligvis, veckovis och månadsvis separat. Dessa sparas säkerhetsklassat ställe.

5.5.2 Tillgängligheten för identitetstjänsten är över 98% med säkerställd redundans av nät och servrar. Därigenom säkerställer vi att identitetsgivaren alltid kan användas för interna system.

5.6. Credential Validation/Authentication

5.6.1
Sophiahemmet Högskola har implementerat och använder samtliga tekniska protokoll enligt SWAMIDs rekommenderade riktlinjer, installerare för Shibboleth och ADFS för den lokala konfigurationen.

5.6.2
Avstängda konton går inte att logga in med.

5.6.3
När användare använder inloggningstjänsterna anger de alltid användarnamn och lösenord.

5.6.4
Inloggningstjänsterna är konfigurerade så att längsta inloggningstid för single-sign on är 12 timmar.