Uppfyllande av tillitsnivån SWAMID AL2 vid Högskolan Kristianstad

1. Inledning

Högskolan Kristianstad (HKR) är en högskola med cirka 14 000 studenter och 500 anställda. Verksamheten är belägen på ett campusområde med adress Elmetorpsvägen 15, i Kristianstad. För mer information se: www.hkr.se

Högskolan Kristianstad är medlem i SWAMID där identitetsfederationen SWAMID-IDP används för validering av användaridentiteter för flertalet tjänster.

Högskolan Kristianstad uppfyller för närvarande tillitsprofilen: AL1 och avser även att uppfylla tillitsprofilen: AL2 för anställda på högskolan, med denna IMPS.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

SWAMID - 4.1.1
Högskolan Kristianstad, organisationsnummer 202100-3195.

SWAMID - 4.1.2
Högskolan Kristianstad är en statlig utbildningsmyndighet vilket gör att högskolans 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 närmaste kalenderåret. I övrigt följer högskolan Sveriges övriga lagar och förordningar.

Högskolans kontohanteringssystem innehåller personuppgifter i formen av konto- och kontaktinformation för anställda och studenter vid Högskolan Kristianstad. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas. Dataskyddsförordningen, GDPR och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.

Studenters personuppgifter hämtas ur högskolans 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 universitetet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.

SWAMID - 4.1.3
Gamla eller trasiga hårddiskar som använts i centrala IT-system och infrastruktur och säkerhetskopiering, monteras ur befintlig hårdvara och destrueras antingen av IT-avdelningen

själva (enligt NIST 800-88), eller genom högskolans upphandlade avfalls- och återvinningsföretag.

4.2 Notices and User Information

SWAMID - 4.2.1
Högskolan i Kristianstad publicerar ”Regelverk för användning av Högskolan Kristianstads (HKR) IT-resurser” via länk under rubriken regelverk på sidan http://www.hkr.se/kontoinfo.

Samt via Högskolan Kristianstads informationssäkerhetspolicy på: www.hkr.se/infosakerhet.

SWAMID - 4.2.2 – 4.2.4
Användarna godkänner användarreglerna i samband med att de aktiverar sitt konto men även vid lösenordsåterställning.

Regelverk och policy uppdateras löpande efterhand som nya revisioner träder i kraft, och finns att ta del av både som anställd och student på www.hkr.se/infosakerhet, dit vi alltid hänvisar då det är relevant.

Information angående förändring av användarregler och informationssäkerhetspolicy skickas ut till samtliga anställda och studenters e-post på HKR.

Information om förändringar publiceras även på studentportal och intranät, med information om fortsatt användning av HKRs IT-tjänster- medför fortsatt/förnyat godkännande av informationssäkerhetspolicyn. Informationen hänvisar även till HKRs dataskyddsombud för eventuella frågor och invändande.

Vid lösenordsbyte tvingas även användaren att på nytt aktivt godkänna rådande informationssäkerhetspolicy.

SWAMID - 4.2.5
Högskolan har på adressen www.hkr.se/utbildningar/student-pa-hkr/it--och-mediastod/kontoinformation/ publicerat allt som handlar om studentens eller den anställdes användarkonto vid lärosätet.

Högskolan har på adressen www.hkr.se/infosakerhet även publicerat högskolans officiella informationssäkerhetspolicy.

Högskolan har publicerat sin SWAMID – Service Definition på följande adresser https://www.hkr.se/swamid-sv och https://www.hkr.se/swamid-en.

4.3 Secure Communications

SWAMID - 4.3.1 – 4.3.2
De tjänster som ingår i ekosystemet för användare och inloggningar, f.n. Active Directory (AD), Shibboleth Identity Provider (IdP), Active Directory Federation Services (ADFS), Microsoft Identity Manager (MIM) och Cisco Identity Services Engine (ISE), driftas på dedikerade servrar som endast driftpersonalen vid högskolan har åtkomst till. Åtkomsten till privata nycklar och delade hemligheter är begränsat till enbart systemets administrativa användare och resp. applikation. Detta gäller även i de fall då privata nycklar i klartext och delade hemligheter används.

SWAMID - 4.3.3 – 4.3.4
All nätverkskommunikation mellan de olika systemen som ingår i ekosystemet för användare och inloggningar är skyddad och krypterad. I de allra flesta fall används TLS-protokollet för kommunikation. Alla privata nycklar och certifikat för SSL/TLS uppfyller SWAMIDS krav och har en nyckelstorlek som är minst 2048 bitar. Replikeringen mellan domänkontrollanter sker enligt Microsofts standardiserade säkerhetsmetod för replikering, i denna ingår Azure AD password synchronization.

4.4 Security-relevant Event (Audit) Records

SWAMID - 4.4.1
Alla förändringar på ett användarkonto- och tillhörande metadata (ex: e-postadress, kontaktuppgifter, etc) loggas.

Autentisering (misslyckad/lyckad) samt förändringar för konton loggas och raderas vid inaktualitet, dock senast efter 2år.

Auditlogging med automatiserad beteendekontroll används för att upptäcka avvikande beteendemönster avseende förändringar av användarkonton och kontoaktiviet, som misstänks kan handla om obehörig åtkomst.

5. Operational Requirements

5.1 Credential Operating Environment

SWAMID - 5.1.1
Lösenord vid Högskolan i Kristianstad måste vara minst åtta tecken samt uppfylla kraven för komplexa lösenord i Active Directory. Detta ger en lösenordskomplexitet om minst 24 bitar.

Komplext lösenord i Active Directory innebär:
- Lösenordet får inte innehålla användarens inloggningsnamn (samAccountName)
- Lösenordet får inte innehålla användarens förnamn, mellannamn eller efternamn såsom det är inskrivet i fullständigt namn (displayName)
- Tidigare lösenord tillåts ej att återanvändas.
- Lösenordet måste innehålla tre av fem teckentyper
    - Versala bokstäver inkl. nationella bokstäver i Europa, dvs. A till Z med eller utan diakritiska symboler samt isländska, grekiska och kyrilliska versala bokstäver
    - Gemena bokstäver inkl. nationella bokstäver i Europa, dvs. A till Z med eller utan diakritiska symboler, tyskt dubbel-s samt isländska, grekiska och kyrilliska gemena bokstäver
    - Siffror, dvs. 0 till 9
    - Specialtecken, dvs. ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
    - Övriga tecken i Unicode

SWAMID - 5.1.2
All kommunikation mellan de olika delarna som används för hantering av användare och lösenord sker krypterat såsom beskrivet under rubriken SWAMID AL1 4.3.3 – 4.3.4.
HKR använder gällande/aktuell TLS-version som har inbyggda skydd mot återspelningsattacker (en. message replay).
Högskolan har inaktiverat kryptosuiter som bedöms utgöra säkerhetsrisker- pga svag kryptoimplementering.

Replikeringen mellan domänkontrollanter i Active Directory sker enligt Microsofts standardiserade säkerhetsmetod för replikering.

För samtlig autentisering mot SWAMID, används SAML2.

SWAMID - 5.1.3
I ”Regelverk för användning av Högskolan Kristianstads (HKR) IT-resurser” finns tydligt angivet att de är personligt ansvariga för användningen av användarkontot och att det inte får göras tillgängligt för andra. Användarna godkänner detta regelverk innan de använder kontot första gången samt när de gör en lösenordsåterställning.

I högskolans informationssäkerhetspolicy anges även de följder/konsekvenser som kan komma att bli aktuella vid misstanke om missbruk avseende användarkonto och IT-resurser.

SWAMID - 5.1.4
Alla servrar som används för kontohantering, webbinloggning och eduroam är uppsatta och konfigurerade så att de endast är tillgängliga på avsedda tjänsteprotokoll såsom Kerberos,

LDAPS, HTTPS, radius osv. för reglerade IP-adresser med hjälp av brandvägg. Vid IT-avdelningen finns ansvar för att hålla servrar och annan hårdvara uppdaterade med avseende på säkerhetsproblem.

Auditlogging med automatiserad beteendekontroll används för att upptäcka avvikande beteendemönster avseende förändringar av användarkonton och kontoaktiviet, som misstänks kan handla om obehörig åtkomst.

Högskolan har inaktiverat kryptosuiter som bedöms utgöra säkerhetsrisker- pga svag kryptoimplementering.

För att detektera och förhindra missbruk, används även flertalet UTM-tjänster på nätverks- och klientnivå (tex: IPS, AV, DLP, Web/DNS-filter, etc).

5.2 Credential Issuing

SWAMID - 5.2.1
Den administrativa DNS-domänen hkr.se används alltid vid attributrelease till det system där användare vill logga in. Detta oberoende om det är SAML2 eller eduroam.

SWAMID - 5.2.2
SAML2-baserad inloggning för Högskolan Kristianstad använder alltid unika identifierare. Identifierare används endast för den SAML2-baserade inloggningstjänsten och inte för någon annan tjänst och ”hkr.se” används alltid i inloggningsserverns identifierare.
Eduroam-baserad inloggning använder alltid radiusservrarna r1.hkr.se& r2.hkr.se för inloggning mot Högskolan Kristianstad.

SWAMID - 5.2.3
En användaridentitet används bara för en enda person och återanvändas inte för någon annan person. Motsvarande gäller även för olika typer av funktionsanvändare men dessa är inte aktuella för användning inom SWAMID.

SWAMID - 5.2.4
Om en användare har mer än ett användarkonto, dvs. är både student och anställd, väljer användaren vid inloggning vilket användarkonto denna ska använda vid det aktuella tillfället.

SWAMID - 5.2.5

Student:
När antagningsuppgifterna förs över från NyA till Ladok skickas ett e-postbrev ut till alla nyantagna studenter med information om hur de aktiverar sitt användarkonto (AL1).

Det skickas även ”Regelverk för användning av Högskolan Kristianstads (HKR) IT-resurser” till e-postadress som är registrerad i LADOK. De studenter som tackar ja till antagningsbeskedet- utan att registrera/påbörja sin utbildning får sina konton automatisk avstängda/inaktiverade.

Studenten aktiverar sitt konto genom att genomföra en lösenordsåterställning, då ett ursprungligt säkert-, slumpmässigt-, och icke-reversibelt lösenord har genererats för kontot- som varken studenten eller någon personal har tillgång till. Innebärande att inte ens IT-avdelningen har möjlighet att se vad användaren har för lösenord.

Lösenord skickas aldrig ut till studenter, utan det är en länk till lösenordsportalen där de anger sitt användarnamn varpå en säkerhetskod e-postas till deras privata e-postadress, så att de sedan tillåts ange ett nytt lösenord. Säkerhetskoden i sig är tidsbegränsad (5min). Förutom engångskoden används Captcha för att säkerställa att det är en människa som återställer lösenordet.

Det initiala lösenordet slumpas fram och sätts per automatik på kontot och är ej läsbart för någon, inte ens IT-avdelningen kan få fram detta. Således är det omöjligt att extrahera det initiala lösenordet.

Studenter erhåller efter avslutad registreringsprocess för användarkonto, tillitsnivån AL1.

Vid all lösenordsändring/-återställning återställs alltid tillitsnivån till AL1.

Anställd:
När en anställd börjar arbeta vid högskolan beställer beställningsansvarig vid respektive organisation vid högskolan ett användarkonto genom HKRs ärendehanteringsystem.

Kontouppgifterna skickas sedan till den aktuella beställningsansvariga. Den beställningsansvariga lämnar över kontouppgifterna till den nyanställda tillsammans med regelverket. Den anställde godkänner regelverket automatiskt vid första inloggningstillfället då den anställde också tvingas att byta lösenord.

Beställningsansvariga och HR-avd. har som rutin att begära uppvisande av giltig ID-handling** vid anställning, samt IT-avdelningen vid utlämnande av dator, telefon och övrig utrustning.

När handläggare vid IT-avdelningen lämnar ut utrustning till den anställde och hjälper denne att byta det ursprungliga lösenordet (obligatoriskt), genomförs även kontroll av giltig ID-handling, varpå handläggaren markerar användaren som AL2 validerad i personaldatabasen.

** Giltig ID-handling avser något av följande:
- Svenskt körkort utfärdat av transportstyrelsen.
- Svenskt nationellt ID-kort.
- Svenskt SIS-märkt ID-kort.
- Pass giltigt inom Europeiska unionen. (ICAO 9303)

Vid kontroll av giltig ID-handling kontrolleras namn och personnummer på ID-handlingen mot de uppgifter som finns registrerade i personaldatabasen.

Anställda erhåller efter avslutad registreringsprocess för användarkonto, tillitsnivån AL2.

Vid all lösenordsändring/-återställning återställs alltid tillitsnivån till AL1.

SWAMID - 5.2.6
IT-avdelningen kontrollerar giltig ID-handling för den nyanställde vid uthämtning/kvittering av utrustning. Efter godkänd ID-kontroll aktiverar IT-avdelningen manuellt en flagga i personaldatabasen som indikerar att personen är AL2-validerad.

Denna flagga distribueras till AD (Active-Directory) varvid användare med denna flagga tilldelas medlemskap i en AD-grupp specifik för användare med AL2-flaggan.
Vid validering mot SWAMID IDP, signaleras vilken tillitsprofil användaren har i attributet: ”EduPersonAssurance” baserat på grupptillhörighet i AD.

Tex:
if (MemberOf:AL2-VerifiedUsers) → EduPersonAssurance:AL2
Else → EduPersonAssurance:AL1

AL2-flaggan som aktiveras i personaldatabasen nollställs/tas bort automatiskt vid eventuellt lösenordsbyte (tillitsnivån sänks alltså till AL1), så att användaren därefter på nytt måste besöka IT-avdelningens helpdesk för att uppvisa giltig ID-handling, och på nytt få AL2-flaggan inlagd i personaldatabasen.

Alla ovanstående förändringar loggas i respektive berört system.

SWAMID - 5.2.7
Studenter ändrar den personinformation som inte hämtas från folkbokföringen i Ladok genom självservicegränssnitt.

Anställda uppdaterar sin personinformation genom att ta kontakt med sin chef som ser till så att informationen uppdateras i högskolans interna personaldatabas, avseende tex: namnändringar. Avseende kontakt & adressuppgifter, ändrar den anställde dessa uppgifter själv i självservicegränssnitt i tjänsten Primula från Statens Service Center.

SWAMID - 5.2.8
Alla kontohanterare är personal vid Högskolan Kristianstad och uppfyller SWAMID AL2. Åtkomstbegränsningar på samtliga kontohanteringssystem, kräver att användaren är medlem i den dedikerade AL2-användargruppen i Active-Directory. Således krävs det att kontoadministratören är AL2-validerad för att beviljas åtkomst till kontohanteringssystemet.

5.3 Credential Renewal and Re-issuing

SWAMID - 5.3.1 – 5.3.2
Alla användare kan byta sitt lösenord genom den inbyggda funktionen i operativsystemen för domänanslutna datorer, t.ex. genom att på Windows trycka Ctrl-Alt-Delete och välj att ändra lösenord. När användaren gör lösenordsbyte på detta sätt anges först det gamla lösenordet innan man anger det nya två gånger. Det nya lösenordet måste uppfylla kraven i SWAMID AL1 5.1.1 ovan.

De som inte har en domänansluten dator genomför sitt lösenordsbyte genom att göra en lösenordsåterställning, se SWAMID AL1 5.3.3 nedan. Även användare med domänanslutna dator, kan byta lösenord genom denna metod.

SWAMID - 5.3.3
Lösenordsåterställning sker via en webbsida där en tidsbegränsad (5min) engångskod skickas till förregistrerad e-postadress för studenter och till förregistrerad mobiltelefon via SMS för anställda. Förutom engångskoden används Captcha för att säkerställa att det är en människa som återställer lösenordet.

Studenten aktiverar sitt konto genom att genomföra en lösenordsåterställning, då ett ursprungligt säkert-, slumpmässigt-, och icke-reversibelt lösenord har genererats för kontot- som varken studenten eller någon personal har tillgång till. Innebärande att inte ens IT-avdelningen har möjlighet att se vad användaren har för lösenord.

Lösenord skickas aldrig ut till studenter, utan det är en länk till lösenordsportalen där de anger sitt användarnamn varpå en säkerhetskod e-postas till deras privata e-postadress, så att de sedan tillåts ange ett nytt lösenord. Säkerhetskoden i sig är tidsbegränsad (5min).
Det initiala lösenordet slumpas fram och sätts per automatik på kontot och är ej läsbart för någon, inte ens IT-avdelningen kan få fram detta. Således är det omöjligt att extrahera det initiala lösenordet.

Studenter erhåller efter avslutad registreringsprocess för användarkonto, tillitsnivån AL1.

Vid all lösenordsändring/-återställning återställs alltid tillitsnivån till AL1.

Högskolan är medveten om att ovan verifieringsvägar (SMS eller epost [singular]) inte är tillräckliga för tillitsnivå AL2. Därför nollställs/raderas AL2-flaggan med automatik vid lösenordsbyte- och lösenordsåterställning (se 5.2.6).

Studenter använder den e-postadress som de anmält till LADOK för att genomföra återställningen. Vill studenten byta e-postadress dit engångskoden skickas måste studenten ändra sin e-postadress i LADOK.

Anställda förregistrerar sitt mobiltelefonnummer via en webbsida när de är inloggade på sin domänanslutna HKR-dator eller uppkopplad via VPN. På webbsidan börjar användaren med att ange sitt nuvarande lösenord och därefter det mobiltelefonnummer som användaren vill använda för lösenordsåterställningen. Har inte den anställda anmält något mobil-telefonnummer för lösenordsåterställning- och inte heller har tillgång till kontot, måste ett personligt besök genomföras i helpdesk på IT-avdelningen.

5.4 Credential Revocation

SWAMID - 5.4.1

Konton för studenter inaktiveras per automatik 18månader efter sist avslutade kurs- eller program.

Avslut av användarkonto/tjänst:
När en användare ska lämna organisationen, inkommer en beställning av avslut ifrån avdelningschef/HR-avdelningen, till högskolans helpdesk, där slutdatum/datum för genomförande anges.

Vid slutdatum inaktiverar handläggare från IT-avdelningen användarkontot i fråga, via personaldatabasen. Information om inaktivering av användarkontot synkroniseras sedan till respektive berört system (tex: AD, Azure, Exchange, etc).

I samband med inaktivering av användarkontot, ändras AL2-flaggan till AL1 i personaldatabasen.

Användaren kan även själv begära att få sitt användarkonto inaktiverat genom att kontakta högskolans helpdesk.

Misstänkt intrång & missbruk:
Vid misstänkt obehörigt intrång i användarkonto, byter IT-avdelningen lösenord på användarkontot i fråga, och loggar sedan ut samtliga sessioner.
Vid sådant lösenordsbyte, ändras AL2-flaggan till AL1 i personaldatabasen automatiskt.

Vid misstänkt missbruk eller obehörigt intrång av användarkonto, inaktiverar IT-avdelningen användarens användarkonto i Active-Directory, vilket förhindrar användaren från att logga in- och/eller genomföra en lösenordsåterställning.

SWAMID - 5.4.2
Vid missbruk eller misstänkt missbruk av användarkonto, byter IT-avdelningen lösenord på användarkontot i fråga, och loggar sedan ut samtliga sessioner.
Vid sådant lösenordsbyte, ändras AL2-flaggan till AL1 i personaldatabasen automatiskt.

Därefter kontaktas kontoinnehavaren via antingen:

- telefonsamtal
- sekundär epostadress (om sådan finns)
- fysiskt besök på användarens arbetsplats.

Varpå användaren informeras om hur-, varför- och att- denne behöver byta lösenord via självbetjäningsportalen för lösenordsbyte (se 5.3.3).

Vid återanställning tillämpas rutinen enligt avsnittet: 5.2.5 ovan.

SWAMID - 5.4.3
Användaren informeras om säkerhetsrisker och best practices för bland annat lösenords- och kontohantering.

Användaren tilldelas även information om dennes skyldigheter avseende att bedriva god informationssäkerhet på högskolan enligt informationssäkerhetspolicyn, och hänvisningar till denna.

Högskolan bedriver även aktiv säkerhetsövervakning och omvärldsbevakning i syfte att kunna arbeta proaktivt kring diverse säkerhetshot som kan komma att uppstå.

5.5 Credential Status Management

SWAMID - 5.5.1
Högskolans primära register för utfärdade identiteter förs i respektive:
- Personaldatabas (PDB)
- Studentdatabas (WDM)
- TillfälligaID databas (TillfID)

Högskolan för register över samtliga tilldelade identiteter och användarkonton även i Active-Directory, dit relevanta data synkroniseras för att kunna garantera funktion och interoperabillitet mellan system.

Alla förändringar på ett användarkonto- och tillhörande metadata (ex: lösenord, e-postadress, kontaktuppgifter, etc) loggas.

Högskolan behandlar personuppgifter i dessa register i enlighet med Dataskyddsförordningen GDPR.

SWAMID - 5.5.2
Inloggningsservern för SAML2 (Shibboleth IdP) och inloggningsservern för eduroam (Cisco ISE) har en erfarenhetsmässigt högre tillgänglighet än 95%.

Inloggningsservern uppfyller SWAMIDs krav på tillgänglighet för interna system.

5.6 Credential Validation/Authentication

SWAMID - 5.6.1
Både SAML2- och radiusinstallationerna uppfyller dessa krav eftersom protokollen är konfigurerade enligt instruktioner från SWAMID och eduroam.org.

SWAMID - 5.6.2
När en användare byter lösenord tas det gamla lösenordet bort ur Active Directory och ersätts med det nya. Därmed kan det gamla lösenordet inte användas för inloggning.

Då kontot stängs av, upphör eller spärras är det inte längre möjligt att logga in enligt standardfunktionalitet i Active Directory eller annan autentiseringstjänst (tex: RADIUS).

Konton för studenter inaktiveras per automatik 18månader efter sist avslutade kurs- eller program.

När en anställd avslutar sin anställning vid högskolan inaktiveras kontot direkt och eventuell AL2-tillitsnivå ändras till AL1.

SWAMID - 5.6.3
SAML2-baserad webbinloggning och eduroam kräver att användaren anger 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 kan oftast spara sina inloggningsuppgifter i den klientprogramvara som finns för eduroam.

SWAMID - 5.6.4
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.

För eduroam finns ingen SSO-session för inloggning utan där finns en maxtid för hur lång tid en klient får på sig för att genomföra inloggningen. Denna maxgräns är mindre än en minut.