HÖGSKOLAN
I SKÖVDE

Anvisningar för kontohantering

Dessa anvisningar har fastställts av David Olsson, IT-chef 2023-12-21 och träder i kraft samma datum.

Dnr HS 2023/906

Innehållsförteckning

1 Inledning

Detta dokument anger Högskolans anvisningar för kontohantering i enlighet med identitetsfederationen SWAMIDs krav, samt kraven enligt MSBFS 2020:6 och MSBFS 2020:7.

Nedanstående alternativ för aktivering av användarkonto och lösenordsåterställning gällande användarkonton med inloggning mot SWAMID gäller för Högskolan.

2 Kontoaktivering och återställning av lösenord

Kontoaktivering och återställning av lösenord för medarbetare och studenter antagna till kommande kurs eller program hanteras i kontoportalen (konto.his.se) enligt något av nedanstående alternativ.

Obekräftad användare (AL1):

Student:

- En handläggare skickar i kontohanteringssystemet en engångskod till den e-postadress studenten har i NyA, personnumret i Ladok används för att hämta e-postadressen från NyA och engångskoden knyts till detta personnummer så att det går att koppla rätt personnummer till kontot i kontoportalen.
  Ett CAPTCHA-test genomförs i samband med aktiveringen.
- Inloggning via antagning.se (NyA) med en obekräftad användare (AL1) där personnummer/interimspersonnummer stämmer med vad som finns i Ladok.

Bekräftad användare (AL2):

- Besök vid helpdesk med godkänd identitetshandling
  - Kontroll enligt nedanstående beskriven Rutin för identitetskontroll
  - Användaren får en tidsbegränsad AL2-engångskod
- Inloggning via eduID (se 2.1.1)
- Inloggning via BankID (svensk e-legitimation LoA3)
  - Identifierare för att knyta person till identiteten är svenskt personnummer.
- För medarbetare och student som ej är folkbokförd i Sverige skickas AL2-aktiveringskod till den adress som är bestyrkt genom foto på legitimation och kopia på till personen adresserad hushållsräkning.
- För medarbetare som är folkbokförd i Sverige skickas aktiveringskod till folkbokföringsadress erhållen av HR-avdelningen.
- För de användare som inte har svenskt personnummer kopierar vi godkänd identitetshandling och antecknar användarkonto. Detta sparas i en pärm inlåst i Helpdesk och kontrolleras vid nästa identifiering för att säkerställa att det är samma person som hämtade ut ett användarkonto.

Enbart Student:

- Inloggning via antagning.se (NyA) med en bekräftad användare (AL2) där personnummer stämmer med vad som finns i Ladok.
- För student som är folkbokförd i Sverige skickas aktiveringskod till folkbokföringsadress enligt Ladok (personal.his.se)

2.1 eduID

eduID är en digital identitet för organisationer inom utbildning och forskning. En eduID-identitet kan användas före, under och efter studietiden. Se: https://eduid.se

Användare som kan att skapa ett eduID:

- Personer med svenskt personnummer folkbokförda i Sverige
- Personer från EU/EES med e-legitimation inom eIDAS
- ePassport via SvipeID

För att få tillitsnivå AL2 på digital väg så verifieras inloggningen mot eduID. eduID-kontot måste uppfylla tillitsnivå AL2.
Kriterier för att automatiskt godkännas är att födelsedata, förnamn, efternamn och e-postadress stämmer överens vid kontroll mot uppgifter från Primula (medarbetare) eller Ladok (Student) För personer med svenskt personnummer gäller svenskt personnummer som identifierare. Uppfylls inte kraven blir personen uppmanad att kontakta helpdesk. Helpdeskpersonal med minst AL2-behörighet kontrollerar uppgifterna och använder/föreslår någon av ovanstående metoder för att autentisera personen. Kriterierna för att manuellt godkännas är att:

- födelsedata stämmer överens
- ett av förnamnen stämmer överens när det finns fler förnamn, olika stavningar som ger näst intill eller identiskt uttal av förnamnet
- efternamnet stämmer överens, olika stavningar som ger näst intill eller identiskt uttal av förnamnet
- e-postadress måste stämma överens

Förregistrerade identifierare
För studenter kopplar vi personnummer eller interimspersonnummer de har i Ladok till användarkonto på Högskolan.

För personal som har svenskt personnummer kopplar vi användarkontot till personnummer.

För de användare som inte har svenskt personnummer kopierar vi godkänd identitetshandling och antecknar användarkontot. Detta sparas i en pärm inlåst i Helpdesk.

För personer utan svenskt personnummer som loggat in till konto.his.se via eduID görs en automatiserad riskbaserad bedömning om inloggad person går att unikt koppla samman med en person i Ladok, där födelsedata måste vara samma, för- och efternamn vara tillräckligt lika, e-postadress i eduID ska vara samma som i Ladok samt att användaren måste vara bekräftad AL2 i eduID

2.2 Återställning av lösenord

- Ovanstående metoder kan också användas för återställning av lösenord.
    - Används en AL1-metod för återställning av lösenord på ett AL2-konto så nedgraderas kontot till ett AL1-konto
- En engångskod erhålles i Helpdesk mot uppvisande av identitetshandling.
- För personer utan svenskt personnummer ska alltid kontroll göras av tidigare uppvisad identitetshandling vid återställning av lösenord samt upphöjning av tillitsnivå. Kontrollera t.ex passnummer, utgivande land eller att passet innehåller samma namn och födelsedata
- Helpdesk kontaktas för att få engångskod skickad till folkbokföringsadress
- Beställning av två separata tidsbegränsade engångskoder som var och en skickas till e-post och SMS och som behöver användas i kombination
    - Om en student har ett aktivt användarkonto samt har en e-postadress och mobilnummer registrerat i Högskolans användardatabas.
    - Om en medarbetare har registrerat e-postadress och mobilnummer i Högskolans användardatabas och har ett aktivt personalkonto.
    - E-postadress och mobilnummer ska i förhand vara registrerade och verifierade

För att kunna få en engångskod via e-post+SMS som kan användas för att logga in i kontoportalen, och där göra en lösenordsåterställning, så krävs att personen har förregistrerade och verifierade uppgifter om e-postadress och mobilnummer i vår kontodatabas.

För att kunna registrera och verifiera kontaktuppgifter behöver personen logga in i kontoportalen, via antingen

- eduID eller antagning.se med AL2 bekräftat konto,
- eller ett befintligt HS-konto (AL2),
- eller mha en engångskod (har personen inga verifierade uppgifter sedan tidigare så erhålles den via folkbokföringsadress, besök i helpdesk etc, dvs AL2).
- antagning.se med ett obekräftat konto eller ett befintligt HS-konto (AL1). Engångskoder som skickas till kontaktuppgifter som har verifierats efter dessa typer av inloggningar betraktas som AL1-engångskoder.

Verifieringen görs genom att en kod skickas till angiven e-postadress resp. SMS-nummer från formuläret, koden kan bara användas så länge personen är inloggad i portalen (sessionen ”lever”).

När personen verifierar kontaktuppgifter så sparas på vilken AL-nivå personen var inloggad, när konton aktiveras sparas på vilken AL-nivå de är skapade.

2.3 Ändring av tillitsnivå

Antagna internationella AL1-studenter visar identitetshandling för utsedd högskolepersonal med tillitsnivå AL2. Dessa kontrollerar identitetshandlingen enligt ”Anvisningar för identitetskontroll”, kopierar identitetshandlingen och lämnar över kopian till Helpdesk som höjer upp användaren till AL2

2.4 Lösenordsbyte

- Lösenordsbyte sker i webmail (mail.his.se) eller i Windowsklienten.
- Vid lösenordsbyte måste det ”gamla” lösenordet angivas.

2.5 Kontaktuppgifter

- Kontaktuppgifter såsom mobilnummer och privat e-postadress bör registreras av användaren i kontoportal för att senare kunna återställa sitt lösenord.
- Student och medarbetare ska ha möjlighet att uppdatera sina kontaktuppgifter.
- Då nya uppgifter registreras eller uppdateras ska detta verifieras genom SMS respektive e-postmeddelande.

3 Rutin för identitetskontroll

Manuell kontroll av legitimationshandling innebär att användaren visar upp en giltig legitimationshandling för högskolepersonal (kontrollören) som av Högskolan är utsedda att utföra en kontroll av legitimationshandlingens giltighet samt att legitimationshandlingen tillhör den person som kontrolleras.

Vid kontrollen används modellen KÄNN PÅ, SE PÅ, VIPPA PÅ för att kontrollera identitetshandlingens äkthet. Om kontrollören misstänker att identitetshandlingen är förfalskad ska identitetshandlingens utfärdare kontaktas eller identifieringen nekas.

Kontrollen ska innefatta att:

- legitimationshandlingen är äkta (ej förfalskad) och godkänd,
- legitimationshandlingen är giltig (kontrollera utgångsdatum) och
- legitimationshandlingen tillhör personen som visar upp den för kontroll (jämför foto med personen framför dig).

Med giltig legitimationshandling menas:

- ett pass eller identitetskort som uppfyller Polisen krav[1],
- ett pass som uppfyller ICAO Doc 9303 eller

[1] https:/polisen.se/tjanster-tillstand/pass-och-nationllt-id-kort/giltiga-id-handlingar

- ett nationellt identitetskort inkl. information om medborgarskap enligt EU-förordning 562/2006.

På PRADO[2] (Public Register of Authentic Identity and Travel Documents Online) finns en lista med giltiga legitimationshandlingar för de olika länderna i EU/EES men även för vissa andra länder. För svenska pass och identitetskort finns förtydligande kontrollinformation hos utfärdaren:

- Svenska pass och nationella identitetskort[3] inkl. webbaserad giltighetskontroll[4].
- Skatteverkets Identitetskort[5] för folkbokförda i Sverige inkl. giltighetskontroll via telefon.
- Svenskt körkort[6] inkl. giltighetskontroll via telefon.
- För SiS-märkta identitetskort måste utfärdaren kontaktas för giltighetskontroll.

För personer som kommer från tredje land, d.v.s. länder utanför EU och Schengen, gäller pass som legitimationshandling. Vid tveksamhet kring giltigheten av utländskt pass äger kontrollören rätt att i stället kräva giltig svensk legitimationshandling.

3.1 Ansvar

Om du misstänker eller upptäcker att en medarbetare eller student använder en förfalskad identitetshandling eller utger sig för att vara någon annan och visar upp en annan persons identitetshandling ska nedanstående genomföras.

- Kopiera identitetshandlingen
- Skriv ner datum, tidpunkt och en beskrivning av situationen
- Kontakta HR eller Studentservice och rapportera händelsen

3.2 Undantag

Personer med skyddad identitet hanteras på annat sätt.

[2] https://www.consilium.europa.eu/prado/sv/prado-start-page.html
[3] https://polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/kontroll-av-passnationellt-id-kort/kontroll-giltighet-pass-nationellt-id-kort/
[4] https://etjanster.polisen.se/egid/giltighetskontroll/
[5] https://skatteverket.se/privat/folkbokforing/idkort/kontrolleranagonannansidkort
[6] https://www.transportstyrelsen.se/sv/vagtrafik/Korkort/har-korkort/korkortet-som-id-handling/

4 Identitetstyper

4.1 Personalkonto

En medarbetare på Högskolan är berättigad till ett användarkonto för personal. En beställning av ett användarkonto för en medarbetare görs till Helpdesk av prefektsekreterare, prefekt, avdelningschef eller motsvarande senast 1 dag innan kontot ska aktiveras.

4.2 Studentkonto

Student som är antagen till program eller kurs på Högskolan är berättigad till ett användarkonto för student.

Medarbetare som behöver ett studentkonto för att kunna genomföra sina arbetsuppgifter innehar studentkonto för att kunna utföra felsökning, underhåll samt kontrollera installerade applikationer i datorsalar.

4.3 Gästkonto

Uthämtas via biblioteket, IT-Helpdesk och Högskolans huvudreception mot uppvisande av legitimation.

Bibliotek och reception ger ut gästkonton för en dag. Helpdesk får skapa gästkonton som gäller upp till 3 månader, längre tid behöver godkännas av prefekt, avdelningschef eller motsvarande.

4.4 Delade konton

Med delade konton menas användarkonton som innehas av flera användare. Delade konton medger inte spårbarhet och därmed uppfylls inte de säkerhetskrav som ställs. Denna typ av användarkonto är därför inte tillåtna.

4.5 Administratörskonton

Administratörskonton med utökade behörigheter medges endast för systemadministratörer och supportpersonal anställda vid avdelningen för Service, IT och Säkerhet vid Högskolan. Dessa konton hanteras enligt särskilda rutiner.

4.6 Konsultkonto

Gästkonto för anlitad konsult. Kontot kan ha olika typer av behörigheter beroende på uppdraget. Speciell sekretess- och ansvarsförbindelse för konsulter ska signeras. Kontot inaktiveras efter att konsultens uppdrag är slutfört.

4.7 Sammanfattning av identitetstyper

Nedan följer en sammanfattning av hur varje identitetstyp relaterar till förtroendenivå samt om identitetstypen kan användas för identifiering inom SWAMID (Swedish Academic Identity Federation) eller inte. Huruvida en ansvarsförbindelse med signeras anges i kolumnen ”ansv.förb.”

Identitetstyp	**Förtroendenivå**	**SWAMID**	**Ansv.förb**
Personalkonto	AL1 / AL2	Ja	Ja
Studentkonto	AL1 / AL2	Ja	Ja
Gästkonto	Obekräftad	Nej	Varierande
Adminkonto	AL2 + MFA	Nej	Ja
Konsultkonto	Obekräftad	Nej	Varierande

5 Upphörande av användarkonto

Den som överträder, eller misstänks överträda Högskolans ”Riktlinjer för datoranvändning” (Dnr HS 2023/782) kan få sitt användarkonto avstängt under utredning. Dessutom kan disciplinära eller rättsliga åtgärder komma att vidtas.

Behörigheten till användarkontot är tidsbegränsad och kommer att upphöra när studierna, anställningen, projektet eller motsvarande upphör. Högskolan har rätt att avsluta användarkonton som varit inaktivt mer än sex månader om ingen annan överenskommelse finns, såsom vid t.ex studieuppehåll, tjänstledighet, med mera.

En användare kan få sitt användarkonto inaktiverat på egen begäran.

Ett användarkonto får aldrig återanvändas till annan person

6 Ikraftträdande

Dessa anvisningar träder i kraft 2023-12-21 och ersätter HS 2021/725 och HS 2023/599