IT-STYRNING

2022-04-25 Dnr C2014/59

Regler för digitala identiteter vid Karlstads universitet

1 Syfte

Reglernas syfte är att klargöra de styrande principerna och definitionerna som gäller för användning av digitala identiteter vid Karlstads universitet. Reglerna är framtagen i enlighet med *Tillåten användning/etiska regler för SUNET (https://sunet.se/om-sunet/policy-for-tillaten-anvandning-och-etiska-regler)* samt följer Swamid tillitsnivå AL3 (*https://www.sunet.se/swamid/policy/al3/*).

2 Dokument

- Policy för digitala identiteter vid Karlstads universitet
- Regler för digitala identiteter vid Karlstads universitet
- Handläggningsordning för digitala identiteter vid Karlstads universitet

3 Dokumenthistorik

Datum	**Förändring**
2014-03-05	Första utgåvan. Arbetades fram av It-styrningsfunktionen på Ledningskansliet. Synpunkter hämtades från It-avdelningen, It-säkerhetssamordnaren samt Personalavdelningen. Dokumentet bereddes i It-beställarrådet.
2016-06-01	Anpassningar för ansökan om Swamid Assurance Level 1 och 2: Ändrad längd och ålder på lösenord för KauID. Starkare lösenord för system- och it-specialister. Rapportera misstanke om obehörig användning av lösenord. Utlämning av uppgifter. Innehållsförteckning införd. Två-faktor för systemspecialist och utlämnare av KauID. Har arbetats fram av Informationssäkerhetsansvarig.
2017-09-01	Krav på ålder för KauID borttaget.
2022-04-25	Begreppet *Stark autentisering* införs. Anpassningar till Swamid Assurance Level 3 (AL3). Uppdaterad lista av godkända legitimationshandlingar. Använda termen *KauID* istället för *studentkonto*. Varaktighet för students KauID. Fysisk support för medarbetare/externa.

Regler för digitala identiteter vid Karlstads universitet

Innehåll

4 Skydda uppgifterna

En medarbetare eller student som fått en digital identitet ska alltid skydda identiteten och får inte lämna uppgifterna (varken lösenordet eller en andra faktor) vidare till annan person.

En systemadministratör eller systemspecialist ska alltid behandla digitala identiteter varsamt och aldrig skriva ut listor med användarnamn och lösenord eller i klartext digitalt skicka ett lösenord till en användare.

Ett undantag görs för hantering av Gästkonto eftersom det kontot endast ger åtkomst till begränsade tjänster under en begränsad tid.

Vid misstanke om att någon obehörig känner till ett lösenord ska detta rapporteras till 2525@kau.se eller närmaste chef.

5 Autentiseringsmetoder

5.1 Lösenord

Lösenordet för en digital identitet ska ha en bra säkerhetsgrad, alltså vara svårt att knäcka, men samtidigt ska användaren kunna komma ihåg lösenordet. Det innebär att vissa regler för lösenordets uppbyggnad måste följas.

5.1.1 Grundregler

Följande grundregler gäller för lösenord:

- Ska bestå av minst 8 tecken.
- Är en blandning av
    - versaler (A-Z)
    - gemener (a-z) och
    - siffror, mellanslag eller specialtecken.
- Samma tecken får inte finnas i följd mer än två gånger. Godkänd teckenföljd: *xxXx*. Ej godkänd teckenföljd: *Xxxx*.
- Får inte anknyta till personens namn.
- Är unikt för universitetets verksamhet, att det alltså inte är detsamma som för it-tjänster som används utanför universitetet (så som Facebook, Google el dyl)

5.1.2 Regler för KauID

Då KauID används för inloggning till många system ska lösenordet förutom grundreglerna även följa följande regler:

- Får inte återanvändas.
- Vid byte av lösenord ska det nya skilja markant från det föregående.
- Vid inloggning tillåts tio försök, varpå nya försök kan återupptas efter 30 minuter.
- Vid misstanke om att lösenordet är känt av andra än kontoinnehavaren ska det omgående bytas.

Samtliga regler ska upprätthållas av den tekniska funktion som hanterar lösenord för KauID. Funktion ska även använda ordlistekontroll för att förhindra användning av vanligt förekommande ord.

5.1.3 Regler för system- och it-specialister

För system- och it-specialister som bl a hanterar användare och behörigheter i system gäller samma regler som för KauID med följande modifiering:

- Består av minst 12 tecken.
- Bytas senast var 180:e dag.

För system- och it-specialister som har åtkomst till system på maskinell nivå kan särskilda regler tillkomma. Dessa regler beslutas av respektive system- eller systemgruppsägaren i samråd med it-säkerhetssamordnaren.

5.1.4 Exempel på konstruktion av lösenord

För att underlätta för användare att hantera lösenord visas här ett exempel på hur ett lösenord kan konstrueras:

- Starta med en mening. Exempel: *Svårt lösen är säkert*
- Rensa bort åäö-tecken: *Svart losen ar sakert*
- Förkorta eller felstava ord: *Svort losen ar sekert*
- Ta bort mellanslag: *Svortlosenarsekert*
- Lägg till ett tal med betydelse för dig i meningen: *Svort1066losenarsekert*

5.2 Stark autentisering

Stark autentisering innebär en identitetskontroll med krav på två eller flera faktorer som styrker lämnad identitet. Faktorer kan vara något man *har* (besittningsfaktor), något man *vet* (kunskapsfaktor) eller något man *är* (biometrisk faktor). Stark

autentisering innebär att det krävs två eller flera identitetsverifieringar vid åtkomst till konton eller tjänster. Därmed ges extra skyddslager i inloggningsprocessen.

Vanliga metoder för identitetsverifieringar är bestående lösenord, engångs lösenord, kort av olika slag, säkerhetsdosor, appar i mobiltelefoner (ex BankID) och biometrisk identifiering.

Användare som i it-system hanterar känsliga personuppgifter, integritetskänsliga personuppgifter, information som skyddas av sekretess eller annan skyddsvärd information, ska vid inloggning genomgå process för stark autentisering. Exempel på it-system med sådan hantering är:

- NAIS
- Sunet Drive för forskningsdata
- KauID

6 För medarbetare

6.1 Efter avslutad anställning

Efter avslutad anställning så ska medarbetarens samtliga digitala identiteter inaktiveras. Undantag kan ges för:

1. Fortsatt associering: Vilket innebär att medarbetaren har någon typ av fortsatt koppling till universitetet.
2. Tidsbegränsad dispens: Vilket innebär att medarbetaren får fortsatt åtkomst till relevanta system under en begränsad tid. Tidsgränsen rekommenderas till maximalt sex månader efter avslutad anställning.

Det är medarbetarens chef som beslutar om något av alternativen är giltiga och i beslutet ska alltid aktuella system förtecknas. Systemägaren eller systemgruppsägaren har dock alltid rätt att överpröva beslutet.

Identiteten KauID kommer aldrig att tas bort (endast vara aktiv eller inaktiv), vilket säkerställer att användarnamnet aldrig kan återanvändas.

6.2 Samarbetsparter och associerade personer

En samarbetspartner eller en person associerad till universitetet kan få digital identitet för åtkomst till ett eller flera av universitetets system. Åtkomsten beslutats av en chef i organisationen är alltid tidsbegränsad. Både slutdatum för åtkomst och aktuella system som ska kommas åt ska anges i beslutet. Beslutet kan alltid överprövas av systemägaren eller systemgruppsägaren.

Regeln ovan gäller inte Gästkonto, som varje anställd har möjlighet att hantera.

6.3 Behörigheter till system

Behörighet till information i system är beroende av vilka arbetsuppgifter man har samt vilket system det gäller. Regler för hur behörigheter handläggs för respektive system beskrivs i förvaltningsplanen (enligt GFS[1]) eller systemförvaltningsplanen.

[1] GFS = Systemförvaltningsmodellen Gemensam förvaltningsstyrning (Universitetsdirektörsbeslut Nr 2/13)

7 För studenter

7.1 Förberedelse av KauID för studenter

KauID förbereds för alla studenter som sökt och antagits till studier vid universitetet och sker så snart det är tekniskt möjligt.

Olika metoder för förberedelse används beroende av hur antagningen gått till; nationell antagning via Universitets- och högskolerådet (UHR), lokal reservantagning eller manuell antagning. KauID kan därför förberedas vid olika tidpunkter beroende av antagningsprocessen.

7.2 Aktivering av KauID för studenter

En students kan få sitt KauID på två sätt:

- Student vars antagningsuppgifter kommit från UHR till universitetet kan hämta ut konto via självbetjäningstjänsten *Aktivera ditt KauID* (http://konto.kau.se).
- Student som av någon anledning inte kan aktivera sitt KauID via självbetjäningstjänsten kan vända sig till universitetets Välkomstcenter (http://www.kau.se/valkomstcenter).

7.3 Studenters rättigheter och skyldigheter

Studenten äger under hela studietiden rätten till sitt KauID och rätten att använda de tjänster och system som KauID ger tillgång till. Ett KauID är personligt och får endast användas av kontoinnehavaren. Det innebär att varken användarnamn eller lösenord får lånas ut till annan person.

Universitet har skyldighet att informera studenterna när förändringar görs som påverkar deras möjlighet att använda KauID.

7.4 Efter studietiden

18 månader efter sista kurstillfällets slutdatum ändrar studentens KauID status från *student* till *alumn* och därmed stängs kontot. Eftersom kontot fortsatt finns kvar säker. Eftersom kontot fortsatt finns kvar säkerställs att användarnamn inte återanvänds. Om studenten återupptar sina studier kan KauID återaktiveras för samma användarnamn.

Studenter som har behov av åtkomst till sina studieresultat efter att KauID stängts kan få det med nationella studentidentiteten eduID (https://www.eduid.se).

8 Service

8.1 Utlämning av uppgifter

Vid utlämning av uppgifter för digital identitet ska den som lämnar ut uppgifterna bekräfta att den som får uppgifterna är densamma som den utger sig för att vara. Den som lämnar ut uppgifterna ska använda någon av följande metoder för bekräftelse av identitet:

- Godkänd svensk ID-handling (SIS-märkt ID-kort, körkort).
- Svenskt nationellt ID-kort eller pass.
- Utländskt pass som uppfyller ICAO Doc 9303.

- EU/EES nationellt ID-kort som uppfyller European Commission Regulation 562/2006.

Rutiner för granskning av legitimation finns dokumenterade i tjänsten som används för utlämning av uppgifter.

Utlämning av uppgifter för digital identitet kan även ske per brev till folkbokföringsadress eller via e-post. Detta sker med en tidsbegränsad engångskod.

8.2 Självservice

Om ett system har möjlighet för självservice för att återställa förlorat eller bortglömt lösenord så får detta inte skickas i klartext till användaren via e-post eller via annat elektroniskt meddelande. Användaren ska alltid hänvisas till en krypterad del av systemet där lösenordet kan återställas.

8.3 System för hantering av KauID

8.3.1 Central autentiseringstjänst

För att universitetet it-system ska kunna använda KauID behövs en central autentiseringstjänst som tillhandahåller identiteter och andra relevanta personuppgifter till anslutna it-system. Tjänsten ska göra det möjligt för användare att bibehålla en inloggning vid byten mellan olika webbaserade system. Tjänsten ska även kunna överföra relevanta uppgifter om inloggande personer till anslutna it-system. Tjänsten ska vara en del i Sunets identitetsfederation SWAMID[2] och vara uppsatt och köras i enlighet med SWAMIDs styrdokument.

De personuppgifter som tillhandahålls av den centrala identitetstjänsten ska hållas till ett minimum och vara nödvändiga för funktionen i respektive anslutande system. Detta oavsett om uppgifterna överförs direkt från identitetstjänsten till det anslutande systemet eller via SWAMID-federationen. Detta förfarande följer intentionerna i den svenska personuppgiftslagen.

System vars primära syfte är att stödja forskning och utbildning får tillgång till personuppgifter motsvarande de som automatiskt skickas med varje e-postbrev, dvs. namn, e-postadress, användaridentitet.

System vars syfte är att för studenter hantera antagning, kursregistrering, tentamensanmälan, ansökan om examen, verksamhetsförlagd utbildning, lärande och självservice för användarkonton får tillgång till användarens personnummer.

8.3.2 Användarkataloger

KauID ska finnas lagrat för alla användare i universitetets två primära användarkataloger, LDAP och AD, och alltid vara synkroniserade.

8.3.3 Nödbroms

Det ska finnas en funktion, *en nödbroms*, för att kunna stänga av en enskild användares nyttjande av KauID. Avstängningen ska då få genomslag i samtliga anslutna system.

---

[2] https://www.sunet.se/swamid/

8.4 Support

Dialog mellan studenter/verksamma/externa intressenter och ansvariga för identitetstjänsten sker via universitetets funktioner för användarstöd:

- Student:
    - Telefon: 054 - 700 1695
    - E-post: studentsupport@kau.se
    - Fysiskt möte: Välkomstcenter
- Medarbetare/externa intressenter:
    - Telefon: 054-700 2525
    - E-post: 2525@kau.se
    - Fysiskt möte: It-avdelningens reception