LEDNINGSKANSLIET

2014-03-05 Dnr C2014/59

# Handläggningsordning för digitala identiteter vid Karlstads universitet

## Syfte

Handläggningsordningens syfte är att klargöra de styrande principerna och definitionerna som gäller för användning av digitala identiteter vid Karlstads universitet. Handläggningsordningen är framtagen i enlighet med *Tillåten användning/etiska regler för SUNET (http://www.sunet.se/Om-sunet/Policyfragor/Tillaten-anvandning.html)*.

Handläggningsordningen har arbetats fram av IT-styrningsfunktionen på Synpunkter har inhämtats från IT-avdelningen, IT-säkerhetssamordnaren samt Personalavdelningen. Dokumentet har beretts i IT-beställarrådet.

## Dokument

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

| | | | | | |
|---|---|---|---|---|---|
| Beslut | RB 35/14 | Dnr. | C2014/59 | Ersätter i delar | C2011/487 |
| Giltighet fr.o.m. | 2014-03-05 | t.o.m. | tillsvidare | Handläggare | Claes Asker |

# Handläggningsordning för digitala identiteter vid Karlstads universitet

## Systemägare och systemgruppsägare

En systemgruppsägare (enligt GFS[1]) eller en systemägare har det formella ansvaret för ett eller flera system. Dessa kan ompröva ett besluta om en användares behörighetsnivå i aktuellt system.

## Systemförvaltare och förvaltningsledare

En systemförvaltare eller en förvaltningsledare ansvarar för att regler och policy för digitala identiteter hanteras korrekt inom respektive system. Dessa är även ansvariga för att en årlig revision genomförs över de digitala identiteter som finns i respektive system.

Det är alltid en systemförvaltare eller en förvaltningsledare som godkänner att en samarbetspartner ges behörigheter till aktuella system.

## Systemadministratörer och systemspecialister

En systemadministratör eller en systemspecialist hanterar det specifika systemets digitala identiteter enligt regler och policy för digitala identiteter.

Med hantering av digitala identiteter menas att upprätthålla ett korrekt och uppdaterat register av systemets användare, att stötta användarna då förändringar i den digitala identiteten behöver genomföras och att en digital identitet har rätt behörighetsnivå i systemet.

## Systemgruppen Identiteter och roller

KauID används för autenticering till flera separata system och kan användas för Single Sign-On mellan dessa system. Det innebär att identitetshanteringen förvaltas av systemgruppen *Identiteter och roller* och därmed gäller en särskild handläggningsordning.

### *GFS-styrgruppen IT-nära*

Beslutar om tillämpning av regler för digitala identiteter som får konsekvenser för användarna.

### *Förvaltningsledaren för Identiteter och roller*

Förvaltningsledaren har ansvar för att:

1. Följa utveckling på identitetsområdet så att universitetet kan upprätthålla en god informationssäkerhet.
2. Utbilda användare och systemspecialister i hantering av digitala identiteter.
3. Ta fram förslag på regeländring för digitala identiteter.
4. Informera samtliga systemförvaltare och övriga förvaltningsledare på universitetet då en anställning avslutas så att de digitala identiteter som den anställde har därmed kan inaktiveras.

---

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

5. Genomföra en årig revision över de digitala identiteter som tillhör KauID.

## Personalavdelningen

Personalavdelningen ansvarar för att förvaltningsledaren för *Identiteter och roller* blir informerad om när en persons anställning upphör samt när viktiga personuppgifter (så som personnummer eller namn) ändras för en anställd person.

## IT-styrningsfunktionen

IT-styrningsfunktionen beslutar om vilka behörighetsnivåer i ett system som ska graderas till säkerhetsklassade och därmed ska säkras med en flerfaktorsautenticering. Även valet av aktuell flerfaktorsautenticering beslutas av IT-styrningsfunktionen.

## Vid oväntade händelser

Vid händelser, så som en kris, som gör att handläggningsordningen sätts ur spel används tillämplig förvaltningsplan enligt aktuell systemförvaltningsmodell.

## Chefer

En chef i organisationen beslutar om eventuell behörighetsdispens då en anställning upphör. Det är även en chef som avgör om en person ska få en digital identitet som associerad.