

Regler för behörighetsstyrning vid Högskolan i Halmstad

Dnr:	L 2026/126
Dokumenttyp:	Regler
Beslutsfattare:	Högskoledirektör
Beslutsdatum:	2026-10-12
Ansvarig avdelning:	IT-avdelningen
Dokumentansvarig:	Anna Frederiksen



Syfte

Dessa regler beskriver hur behörighetstilldelning till IT-produkter, tjänster och system på Högskolan i Halmstad hanteras. Styrdokumentet riktar sig till alla som ska tilldela en behörighet på Högskolan. Syftet med reglerna är att säkerställa att Högskolan har en god behörighetsstyrning som sker på ett lagenligt, ändamålsenligt och säkert sätt.

Bakgrund

En fungerande och säker behörighetsstyrning är en viktig grund i Högskolans systematiska IT- och informationssäkerhetsarbete. Behörighetsstyrning säkerställer att användare inte har tillgång till mer information och informationssystem än vad som behövs för att kunna utföra sina arbetsuppgifter. Behörighetsstyrning handlar även om att begränsa antalet privilegierade användare inom verksamheten och säkerställa att inte fler användare i verksamheten än nödvändigt har tillgång till fler personuppgifter och annan information än nödvändigt. Dessa regler utgör en precisering och lokal anpassning av principen om integritet och konfidentialitet i artikel 5 p. 1 f) i Dataskyddsförordningen (EU) 2016/679, som inbegriper skydd mot obehörig eller otillåten behandling av personuppgifter med användning av lämpliga tekniska och organisatoriska åtgärder. Vidare utgör reglerna också en precisering och lokal anpassning av föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter.

Inledning

Definitioner

I detta dokument ska angivna definitioner ha följande mening:

”Behörighet” avser vilka informationsuppgifter en användare har tillgång till och vad personen kan göra med uppgifterna.

”Digital identitet” identifierar en person eller ett visst informationssystem i form av ett användarnamn eller en systembeteckning. Ofta benämns digital identitet med begreppet ”konto”, dvs att en person eller ett informationssystem får ett ”konto” i en IT-miljö som är unikt för denne.

”Privilegierad användare” avser användare med privilegierade behörighetsåtkomster (höga behörigheter). Användaren har högre åtkomst än vad en ”vanlig” användare har. Exempel på privilegierad användare kan vara IT-chef, säkerhetschef, systemägare och systemförvaltare.

Tillämpning

Dessa regler gäller Högskolans samtliga IT-system, IT-produkter och IT-tjänster.

Principer vid tilldelning av behörigheter

Följande principer ska vara styrande vid behörighetstilldelning och utformande av rutiner om detta:

- Varje person ska ha den åtkomst och behörighetsnivå som krävs för dennes roll, vid varje given tidpunkt, varken mer eller mindre. Det innebär därför även att ansvarig medarbetare ska se till så att åtkomst och behörigheter tas bort alternativt omedelbart förändras när någon träder ur eller

förändrar sin roll. Ansvarig för att anställds åtkomst och behörighet justeras när en anställd avslutar/förändrar sin tjänst är den anställdes närmsta chef.

- Högskolan ska kontinuerligt göra översyn av tilldelade behörigheter. Dessutom ska tilldelade behörigheter kontrolleras minst en gång per år, och privilegierade behörigheter kontrolleras minst en gång per halvår.
- Innan en användare ges behörighet att använda Högskolans IT-resurser ska han eller hon informeras om gällande regler för användning och bekräfta att han/hon tagit del av dessa.
- Krav på flerstegsverifiering eller annan form av stark autentisering ska ställas vid inköp av system, produkter och tjänster inom IT-området där det är befogat utifrån användning och tekniska krav.
- För att avgöra vilken aktivitet som ska loggas av Högskolan ska följande aspekter beaktas: känslighet, skyddsvärde och hur verksamhetskritisk informationen i systemet är.
- Användningen av systemadministrativa behörigheter ska begränsas och skyddas. Ju högre behörighet ett konto har, desto mindre ska det användas. Privilegierade användare med hög behörighet ska därför ha olika konton för det dagliga arbetet respektive när man har en anledning att använda konto med hög behörighet.
- En digital identitet med systemadministrativ behörighet ska endast ges åtkomst till en begränsad del av Högskolans digitala produkter, tjänster och system. Användare av dessa identiteter ska instrueras och informeras om hur och när dessa får användas.
- Högskolan ska tilldela behörigheter som ger åtkomst till information av högt skyddsvärde på ett restriktivt sätt.

Behörighetstilldelning

Beslut om behörighet

Systemägare beslutar om behörighetsstruktur (vilka roller som har vilken behörighet) inom respektive IT-system, -produkt eller -tjänst. Vilken person som ska ha vilken roll beslutas av personens närmaste chef.

Systemförvaltare ansvarar för löpande användar- och behörighetsadministration, inklusive uppföljning av att tilldelade behörigheter är korrekta.

Beslut om att tilldela en person privilegierade behörigheter ska dokumenteras och det ska i beslutet framgå vilket verktygsprogram som avses samt vad som är tillåtet vid användande.

Rollseparering

Som utgångspunkt ska samma person inte ha i uppgift (och behörighet) att både utföra en åtgärd och granska den. Exempelvis ska den som ansvarar för analys av loggar inte ha behörighet att ändra i eller radera loggarna. Om det inte finns tillräckligt med medarbetare för att införa nödvändig rollseparering, ska Högskolan se till att samma person har olika konton för olika uppgifter och kompensera med extra kontroller. Det gäller särskilt arbetsuppgifter som kräver privilegierade behörigheter.

Behörighetshantering

Högskolan ska kunna hantera de digitala identiteternas behörigheter på ett sätt som garanterar att rätt behörighet knyts till rätt digital identitet.

Innan Högskolan tilldelar en person en digital identitet och ett konto i Högskolans IT-miljö ska Högskolan kontrollera identiteten på personen. Beroende på hur säkerhetskänslig information individen ska hantera ska dessa kontroller göras på olika sätt enligt närmare rutiner från IT-chef.

Priviligierade åtkomstbehörigheter

Hantering av privilegierade åtkomstbehörigheter

Tilldelning och användning av privilegierade åtkomstbehörigheter ska begränsas och styras.

I de fall en användare ges behörighet att konfigurera funktioner som kan påverka Högskolans IT- och informationssäkerhet, ska detta riskbedömas och beroende av resultatet eventuella lämpliga säkerhetsåtgärder införas.

Vid tilldelning av privilegierade åtkomstbehörigheter gäller alltid följande:

- a) genomförande och dokumentation av risk- och sårbarhetsanalys ska ske innan behörighet definieras för en roll,
- b) användare ska tilldelas privilegierade åtkomstbehörigheter på grundval av deras behov av åtkomst och baserat på kravet för deras roller,
- c) giltighetstid för privilegierade åtkomstbehörigheter ska definieras,
- d) privilegierade åtkomstbehörigheter ska tilldelas ett användarkonto som skiljer sig från de konton som används för ordinarie verksamhet, och
- e) användare ska instrueras och informeras om hur och när de får använda sina tilldelade behörigheter.

Systemkonfigurationer ska utföras logiskt och administrativt separerat från ordinarie användarkonton för att minimera risker och upprätthålla principen om minsta behörighet.

När användare träder ur eller förändrar sin roll som motiverar aktuell privilegierad användarbehörighet ska den privilegierade åtkomstbehörigheten omedelbart upphöra.

Akut behörighetsåtkomst

Akut behörighetsåtkomst (så kallad break glass) får endast tillämpas i undantagssituationer där ordinarie process för behörighetstilldelning inte kan iakttas utan att det medför oacceptabel risk för verksamheten.

Förutsättningar för beviljande

Akut behörighetsåtkomst får beviljas endast om det föreligger ett omedelbart och dokumenterat behov grundat på någon av följande omständigheter:

- a) allvarlig driftstörning eller teknisk incident som riskerar att påverka Högskolans verksamhet,
- b) pågående eller befarad allvarlig IT- och/eller informationssäkerhetsincident, innefattande intrång, dataläckage eller otillåten åtkomst,

- c) situation där skydd av liv, hälsa eller fysisk säkerhet kräver omedelbar åtkomst till information eller system,
- d) behov av att omedelbart fullgöra rättslig förpliktelse, myndighetsbeslut eller annan bindande skyldighet,
- e) annan verksamhetskritisk händelse där dröjsmål med behörighetstilldelning kan medföra betydande skada för Högskolan.

Villkor för användning

Beslut om akut behörighetsåtkomst ska uppfylla följande krav:

- a) åtkomsten ska begränsas till vad som är strikt nödvändigt för ändamålet (principen om minsta privilegium),
- b) åtkomsten ska vara tidsbegränsad och automatiskt eller manuellt återkallas så snart behovet upphör, och
- c) samtliga åtgärder som vidtas med stöd av akut behörighet ska om det är tekniskt möjligt loggas på ett spårbart och manipulationssäkert sätt.

Dokumentation och uppföljning

Varje beslut om och användning av akut behörighetsåtkomst ska utan dröjsmål dokumenteras.

Dokumentationen ska minst innehålla:

- a) namn och roll på beslutsfattare och användare,
- b) tidpunkt för tilldelning och avslut,
- c) skälen för åtkomsten, samt
- d) vidtagna åtgärder.

Användningen ska i efterhand granskas av behöriga funktioner, vilket kan innefatta säkerhetschef, IT-chef, dataskyddsombud eller högskolejurist.