UMEÅ UNIVERSITET

ANVISNING FÖR SYSTEMADMINISTRATIV BEHÖRIGHET VID UMEÅ UNIVERSITET

Typ av dokument:	*Anvisning*
Datum:	*År-månad-dag (beslutsdatum)*
Dnr:	FS 2.5-173-23
Beslutad av:	*Universitetsdirektör*
Giltighetstid:	*Tillsvidare*
Område:	*IT*
Ansvarig förvaltningsenhet:	*ITS*
Ersätter dokument:	

Innehållsförteckning

1. Beskrivning

Anvisningen beskriver systemägares ansvar för systemadministrativ behörighetshantering och vilka kompetenskrav som ska säkerställas för personer som tilldelats systemadministrativa behörigheter. Anvisningen beskriver även det ansvar som personer som tilldelats systemadministrativa behörigheter har.

2. Definitioner

Systemadministrativ behörighet definieras som behörighet med priviligierade rättigheter som ger möjlighet att förändra grundläggande funktioner och säkerhetsfunktioner i ett informationssystem. Systemadministrativa behörigheter har indelats i tre nivåer:

Systemadministrativ behörighet på teknisk nivå definieras som behörighet på systemnivå med priviligierade rättigheter som ger möjlighet att förändra avancerade funktioner och säkerhetsfunktioner som kan ge stor eller mycket stor påverkan på en eller flera applikationer och dess informationsinnehåll. Det kan exempelvis avse drift på servernivå och nät. Säkerställer säkerhetsåtgärder på systemnivå enligt systemägarens och driftsansvarigs instruktioner.

Avancerade systemadministrativ behörighet på applikationsnivå definieras som behörighet med priviligierade rättigheter som ger möjlighet att förändra grundläggande funktioner och säkerhetsfunktioner i ett informationssystem som ger stor eller mycket stor påverkan på applikationen och dess information, samt tilldela administrativ åtkomst till systemet. Säkerställer säkerhetsåtgärder på applikationsnivå enligt systemägarens instruktion.

Grundläggande systemadministrativ behörighet på applikationsnivå definieras som behörighet med priviligierade rättigheter som ger möjlighet att förändra enklare funktioner i ett informationssystem med begränsad påverkan på applikationen och dess information, samt att tilldela åtkomst till vanliga användare i systemet, utan systemadministrativa behörigheter. Säkerställer åtkomst till information enligt informationsägarens instruktion.

Systemägare har ett överordnat ansvar för administration, drift och säkerhet för informationssystem.

Informationsägare har ett utpekat ansvar för information inom ett eller flera verksamhetsområden.

3. Allmänt

Systemägaren är den som ansvarar för systemet och behörighetsstyrningen. Systemägaren är även ägare av systemkonton, det vill säga konton som inte specifikt används av en individ utan används för systemtjänster eller systemfunktioner.

Informationsägaren ansvarar för behörighetsstyrning med avseende på åtkomst till information

I de fall server eller applikationsdrift sköts av annan än systemägaren skall respektive driftsfunktion tillämpa behörighetsstyrning inom ramen för och begränsat till vad som krävs för att kunna utföra sitt uppdrag. Detta innebär även att driftsfunktionen på anmodan från systemägaren vid var tid skall redogöra för vilka som har behörighet inklusive behörighetsnivåer för varje system.

Denna anvisning baseras på det regelverk som finns vid Umeå universitet samt berörda delar i Myndigheten för Samhällsskydd och Beredskap, MSB:s föreskrift MSBFS 2020:7 Kap 4, §4-5

4. Anvisning

4.1. Systemadministrativa behörigheter

Behörighetsstyrning innebär en livscykelhantering av behörigheter. Detta inkluderar tilldelning, kontroll samt avslut av behörigheter. Beslut rörande behörighetsstyrning ska dokumenteras och finnas tillgängliga i enlighet med för systemet gällande krav.

Principer för behörighetstilldelning ska vara att:

- systemadministrativ behörighet ska tilldelas restriktivt genom att användandet av systemadministrativa behörigheter ska minimeras och endast nyttjas när det är nödvändigt.
- varje person inte ska ha mer åtkomst till information än arbetsuppgiften kräver.
- systemadministrativ behörighet endast ska ge åtkomst till en begränsad del av produktionsmiljön.
- systemadministrativa behörigheter ska vara tidsbegränsade och det ska vid behov, minst en gång per år, kontrolleras att utdelade behörigheter är korrekta.
- konto för systemadministrativa behörigheter ska användas för systemadministrativa behörigheter på teknisk och avancerad nivå
- särskilda arbetsstationer bör användas för systemadministrativa uppgifter på teknisk nivå. Isolera arbetsstationerna från internet och säkerställ att dessa endast innehåller nödvändig mjukvara för den systemadministrativa uppgiften så att en användare i sitt dagliga arbete inte använder sig av ett konto med höga behörigheter.

För system som är anslutna till universitetets centrala identitetsinfrastruktur gäller:

- att en användare kan ha ett centralt hanterat konto som ger systemadministrativ behörighet på teknisk eller avancerad nivå för flera system, förutsatt att MFA kan användas vid inloggning.
- i de fall MFA inte stöds så ska ett unikt systemspecifikt centralt hanterat konto med systemadministrativa behörigheter tilldelas.

För system som inte är anslutna till universitetets centrala identitetsinfrastruktur gäller:

- att man inte får använda samma namnstandard på konton som för den centrala infrastrukturen.

4.2. Systemkonton

Systemkonton är icke personliga konton som används vid t.ex. integrationer och andra automatiska systemflöden.

För systemkonton gäller:
- systemkonton ska ej tilldelas högre behörighet än vad som explicit behövs för specifik tjänst eller funktion. Därmed bör systemkonto som innehar flera behörigheter inom samma system undvikas.
- systemkonton ska vara systemspecifika.

4.3. Kompetenskrav

Personer som tilldelas systemadministrativ behörighet ska ha god kännedom om Umeå universitets regler och andra styrdokument gällande informations- och IT-säkerhet.

Systemägare och driftsansvarig/närmast ansvarig chef för systemdriften ansvarar för att personer som tilldelats systemadministrativa behörigheter innehar rätt kompetens både gällande t.ex. teknik, säkerhet och gällande regler, anvisningar och andra styrdokument. Personer som tilldelas åtkomst med systemadministrativ behörighet ska delta på de utbildningar gällande informations- och IT-säkerhet vid Umeå universitet som ITS rekommenderar.

4.4. Ansvar

Det åligger innehavare av systemadministrativ behörighet att hålla sig uppdaterad gällande rutiner, regler, anvisningar och andra relevanta styrdokument.

Personer med systemadministrativ behörighet på teknisk nivå eller avancerad systemadministrativ behörighet ska, i enlighet med gällande lagar, regler samt systemägarens eller driftsansvariges instruktioner:
- hindra användares tillgång till IT-resurser vid grundad misstanke om regelbrott eller vid felaktig användning.
- anmäla misstanke om brott mot gällande regler och lagstiftning samt bistå verksamhetsansvarig, universitetets funktioner, incidenthanteringsgruppen, universitetsledning och IT-chef samt polis vid utredningar om brott mot universitetets regler och gällande lagstiftning.
- inhämta medgivande vid granskning och kontroll av data i informationsfiler.
- följa Umeå universitets rutin för incidenthantering samt dess tidsramar.
- arbeta aktivt för att upprätthålla överenskommen säkerhetsnivå.

Notera att tilldelad systemadministrativ behörighet inte omfattar rätten att ta del av information i form av till exempel e-post eller filer.