Mittuniversitetet
MID SWEDEN UNIVERSITY

Riktlinjer för styrning av åtkomst

Publicerad: 2020-11-04

Beslutsfattare: Helena Wallskog

Handläggare: Eva Rodin Svantesson

Beslutsdatum: 2020-11-04

Giltighetstid: Tillsvidare

Ansvarig för förvaltning: Riktlinjerna förvaltas av infrastrukturavdelningen.

Målgrupp: Infrastrukturavdelningen (INFRA) och systemansvariga.

Sammanfattning: Riktlinjerna sammanfattar universitetets regelverk gällande styrning av åtkomst. Utifrån riktlinjerna ska rutiner och övriga dokument tas fram. Riktlinjerna har anpassats utifrån Myndigheten för samhällsskydd och beredskaps föreskrifter MSBFS 2020:6-7.

Innehållsförteckning

1. Riktlinjer för styrning av åtkomst

1.1 Verksamhetskrav för styrning av åtkomst

Syfte: Att begränsa åtkomst till information och informationsbehandlingsresurser.

1.1.1 Regler för styrning av åtkomst

Regler för styrning av åtkomst ska finnas, dokumenteras och vara föremål för uppföljning utifrån verksamhets- och informationssäkerhetskrav. Tillgångens ägare ska fastställa lämpliga regler för styrning av åtkomst, rättigheter och begränsningar för specifika roller. Åtkomstkontroller är både logiska och fysiska och dessa bör beaktas tillsammans.

Följande gäller vid Mittuniversitetet:

a) användare beviljas bara tillgång till den information som de behöver för att utföra sina uppgifter (olika aktiviteter/roller innebär olika behöver-veta och därmed olika åtkomstprofil);
b) användare beviljas endast tillgång till de informationsbehandlingsresurserna (IT-utrustning, program, rutiner, utrymmen) de behöver för att utföra sin uppgift, ditt arbete eller din roll.

1.1.2 Tillgång till nätverk och nätverkstjänster

Följande gäller vid Mittuniversitetet:

a) användare ska endast ges tillgång till nätverk och nätverkstjänster som de specifikt beviljats tillstånd för;
b) utrustning ska endast ges tillgång till nätverk och nätverkstjänster som de specifikt beviljats tillstånd för;
c) principer för användning av nättjänster bör vara förenliga med organisationens principer för styrning av åtkomst.

1.2 Hantering av användaråtkomst

Syfte: Att säkerställa behörig användaråtkomst och att förhindra obehörig åtkomst till system och tjänster.

1.2.1 Registrering och avregistrering av användare

En formell process för registrering och avregistrering av användare ska finnas för att möjliggöra tilldelning av åtkomsträttigheter.

Följande gäller vid Mittuniversitetet:

a) unika användarkonton så att användarna kan vara kopplade till och hållas ansvariga för sina handlingar;
b) användning av delade konton tillåtas endast när de är nödvändiga för verksamheten eller av operativa skäl och bör vara godkända och dokumenterade;
c) tilldelade behörigheter är tidsbegränsade och kontrolleras en gång per år;
d) att användarkonton omedelbart avaktiveras eller tas bort för användare som har lämnat organisationen.

1.2.2 Tilldelning av användaråtkomst

En formell process för tilldelning av användaråtkomst ska finnas för tilldelning och återkallande av åtkomsträttigheter för alla typer av användare till alla system och tjänster.

Följande gäller vid Mittuniversitetet:

a) erhålla tillstånd från ägaren av informationssystem eller tjänsten för användning av informationssystem eller tjänst;
b) anpassa åtkomsträttigheter för användare som har bytt roller eller jobb och omedelbart ta bort eller blockera åtkomsträttigheter för användare som har lämnat organisationen;
c) med jämna mellanrum granska åtkomsträttigheter med ägare till informationssystem eller tjänster.

1.2.3 Hantering av privilegierade åtkomsträttigheter

Tilldelning och användning av privilegierade åtkomsträttigheter bör begränsas och styras. Digitala identiteter som ger systemadministrativ behörighet ska endast användas för systemadministration och tilldelas restriktivt. Fördelningen av privilegierade rättigheter bör styras genom ett formellt godkännande.

Följande gäller vid Mittuniversitetet:

a) användare ska tilldelas privilegierade åtkomsträttigheter på grundval av deras behov av åtkomst och anpassat till situationen i enlighet med regler för styrning av åtkomst d.v.s. baserat på kravet för deras roller;
b) det ska finnas en godkännandeprocess över alla tilldelade privilegier;
c) krav på giltighetstid för privilegierade åtkomsträttigheter bör definieras;
d) privilegierade åtkomsträttigheter bör tilldelas ett användarkonto som skiljer sig från de konton som används för ordinarie verksamhet.

e) för administratörskonton ska autentiseringsinformation behållas konfidentiell när den delas (t.ex. täta byten av lösenord och så snart som möjligt när en privilegierad användare lämnar eller byter jobb, samt kommunicera den mellan privilegierade användare genom lämpliga mekanismer).
f) en digital identitet med systemadministrativ behörighet bör endast ges åtkomst till en begränsad del av produktionsmiljön.

1.2.4 Flerfaktorsautentisering

Vid Mittuniversitetet ska flerfaktorsautentisering användas för;

a) egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk,
b) systemadministrativ åtkomst till informationssystem, och
c) åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd.

1.2.5 Hantering av autentiseringsuppgifter

Vid Mittuniversitetet ska lösenordsregler för autentiseringsuppgifter finnas med som minst följande innehåll;

a) längd och komplexitet,
b) när byte ska ske,
c) hur distribution ska ske, och
d) hur autentiseringsuppgifterna ska skyddas.

1.2.6 Hantering av användares lösenord

Tilldelningen av lösenord ska styras genom en formell hanteringsprocess.

1.2.7 Granskning av användares åtkomsträttigheter

Ägare av tillgångar ska med jämna mellanrum (minst två gånger/år) granska användarnas åtkomsträttigheter.

Följande gäller vid Mittuniversitetet:

a) en användares behörigheter ska ses över och omfördelas när användaren byter från en roll till en annan inom samma organisation;
b) tillstånd för privilegierade åtkomsträttigheter ska ses över oftare.

1.2.8 Borttagning eller justering av åtkomsträttigheter

Åtkomsträttigheterna för alla anställda, och externa användare ska tas bort vid avslutande av deras anställning, avtal eller uppdrag eller justeras vid förändringar.

Följande gäller vid Mittuniversitetet:

a) vid avslutande av anställning ska individens åtkomsträttigheter till information och tillgångar som är kopplade till informations-behandlingsresurser och -tjänster avlägsnas eller avslutas.
b) förändringar i anställningen ska återspeglas i avlägsnande av alla rättigheter som inte är godkända för den nya rollen.

1.3 Användaransvar

Syfte: Att göra användare ansvariga för att skydda sin autentiseringsinformation.

1.3.1 Användning av konfidentiell autentiseringsinformation

Användare ska följa organisationens regler gällande hantering av autentiseringsinformation.

1.4 Styrning av åtkomst till system och tillämpningar

Syfte: Att förhindra obehörig åtkomst till system och tillämpningar.

1.4.1 Begränsning av åtkomst till information

Begränsningar i åtkomst ska baseras på specifika verksamhetskrav och på universitetets definierade regler för styrning av åtkomst.

1.4.2 System för lösenordshantering

Systemet för lösenordshantering ska säkerställa kvalitativa lösenord.

Följande gäller vid Mittuniversitetet:

System för lösenordshantering ska:

a) framtvinga användning av individuella användarkonton och lösenord så att individuellt ansvar kan utkrävas.
b) låta användare välja och ändra sina egna lösenord och innehålla en rutin som ger meddelande om inmatningsfel.
c) säkerställa att lösenord följer gällande lösenordsregler.
d) tvinga användarna att ändra sina lösenord vid den första inloggningen.
e) kräva ändring av lösenord regelbundet samt vid behov.

1.4.3 Användning av privilegierade program

Användning av program som kan ha förmåga att kringgå säkerhetsåtgärder i system och tillämpningar ska begränsas och styras strikt.

1.4.4 Åtkomstkontroll till källkod för program

Tillgång till källkod och relaterade objekt (t.ex. designspecifikationer, kravspecifikationer, planer för verifiering och validering) ska styras noggrant för att förhindra införandet av obehörig funktionalitet och undvika oavsiktliga ändringar.