Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

STYRANDE DOKUMENT SLU ID: SLU.ua 2019.2.8.3-4147

Sakområde: Säkerhet och informationssäkerhet

Dokumenttyp: Anvisning/Instruktion	Beslutsdatum: 2019-11-07
Beslutsfattare: Säkerhetschef Johan Sjöblom	Träder i kraft: 2019-11-07
Avdelning/kansli: Säkerhetsenheten	Giltighetstid:
Handläggare: Christian Nähl	Bör uppdateras före: 2022-11-07

Ev. dokument som upphävs:

Bilaga till: Riktlinjer för informationssäkerhet vid SLU Dnr ua 2015.2.10-2118

Instruktion åtkomsthantering av system

1 Administration och styrning av åtkomst

Identitets- och åtkomsthantering ska i samband med andra säkerhetshöjande åtgärder säkerställa att SLU:s system erhåller ett adekvat skydd från obehörig eller otillåten åtkomst. Med en bra och tillförlitlig behörighetshantering säkerhetsställs att information inte kommer i orätta tillhanda samt att systemet används på ett sådant vis att konfidentialitet tillgänglighet och riktighet säkerhetsställs. Utgångspunkt ska vara att användare endast ska ha tillgång till de uppgifterna som behövs för sitt arbete men även att behörighet till IT-system automatiskt inte betyder att man har rätt att ta del av alla uppgifter som finns där.

1.1 Regler

1) Samtliga konton som förekommer i SLU:s IT-miljö ska var och en gå att härleda till en unik identitet som kan härledas till en fysisk person.
2) Administratörskonton som inte är nödvändiga för att säkerställa systemets funktionalitet ska avaktiveras eller raderas.
3) Vid leverans av IT-system från extern leverantör ska åtkomst till systemet vara reglerade med för SLU:s unika lösenord.
4) Det ska alltid vara möjligt att härleda en användares identitet, även om åtkomst har skett med en grupp- eller rollbaserad identitet.
5) Vid tilldelning av administrativa rättigheter avseende system som behandlar uppgifter som har ett högt skyddsvärde[1] för SLU ska beslutet dokumenteras och göras tillgänglig vid ev. kontroll.

[1] Högt skyddsvärde innebär att SLU:s verksamhet är beroende av systemet funktionalitet.

1.2 Behörighet till IT-system

1) En användares åtkomst till SLU:s informationstillgångar ska styras och tilldelas individuellt alternativt vara rollbaserad. Rollbaserade behörigheter ska beslutas och dokumenteras av systemägaren.
2) Behörighet till IT-system som innehar känsliga uppgifter [2] för SLU:s verksamhet får endast tilldelas till den som
    1. har erforderliga kunskaper för att använda IT-systemet
    2. har behov av uppgifterna i systemet för att kunna fullgöra sina arbetsuppgifter
3) När någon förutsättning för behörighetstilldelning enligt ovan inte längre är uppfyllt ska behörigheten omgående förändras eller raderas så att användaren inte längre kan utnyttja IT-systemet.
4) En användares åtkomsträttigheter till IT-systemet som behandlar informationstillgångar som innehar känsliga uppgifter för SLU:s verksamhet får endast nyttjas för utförandet av arbetsuppgifter.
5) Vid ansökan om behörigheter till system med högt skyddsvärde för SLU:s verksamhet bör avsedd giltighetstid anges.
6) Användares personliga användarkonto får inte användas som administratörskonto till system med högt skyddsvärde, i dessa fall ska två konton finnas åtskilda från varandra. Detta för att förhindra att systemet ex. ”smittas” med skadlig kod eller att ett läckt lösenord till användarkonto kan användas till administratörskontot.

1.3 Systemkrav

1) IT-system ska ha ett behörighetskontrollsystem.
2) IT-system ska kunna presentera information om vilka behörighetsnivåer som finns tillgängliga.
3) IT-system ska kunna presentera information om samtliga användare som har tilldelats åtkomst, minst följande ska presenteras.
    1. användarens identitet
    2. aktuella åtkomsträttigheter
4) IT-systemet ska tillhandahålla funktionalitet som möjliggör tilldelning av tidsbegränsade åtkomsträttigheter, finns inte den möjligheten i systemet ska dokumentation finnas vilka roller och individer som innehar tidsbegränsade behörigheter.

1.4 Behörighetsrevision

1) Ansvarig systemägare ska säkerställa att det minst en gång per år och med högst 13 månaders mellanrum görs en inventering av de behörigheter som gäller för dennes IT-system.
2) En sammanställning av resultatet ska dokumenteras och finnas tillgänglig för ev. kontroll.

[2] System som bl.a. behandlar känsliga personuppgifter, sekretessinformation eller annan viktig information för SLU:s verksamhet.

3) Utöver de årliga revisionerna ska granskningar av åtkomsträttigheterna även ske vid större organisations- och systemförändringar.

1.5 Autentisering av användare

1) IT-system som behandlar information med ett högt skyddsvärde för SLU ska autentisera användare och administratörer med hjälp av minst två faktorer.
   Om det inte är tekniskt eller ekonomiskt möjligt att autentisera användare med hjälp av två faktorer ska systemägare motivera varför i systemets förvaltningsdokumentation.

1.6 Extern informationsåtkomst

1) Extern användare får endast delges tillgång till information med ett högt skyddsvärde för SLU efter godkännande av systemägare eller av denne utsedd person. Beslut ska dokumenteras.
2) Extern användares åtkomst till IT-system ska alltid inneha ett slutdatum, detta bestäms utifrån hur läng tid uppdraget på SLU sker. Finns inte den möjligheten i systemet ska dokumentation finnas med slutdatum för den externa användaren.

1.7 IT-system som är tillgängliga för allmänheten

1) E-tjänster för att tillgodose allmänhetens rätt till service eller som är till för att informera allmänheten via webbsidor får endast hanteras om:
    1. Det med hänsyn till informationens skyddsvärde och allmänhetens behov är lämplig.
    2. Systemet har adekvata säkerhetsfunktioner.
    3. En riskanalys har genomförts och relevanta säkerhetshöjande åtgärder har vidtagits.
    4. Information om ovan dokumenteras och godkännes av systemägaren.