



Sakområde: IT, service, säkerhet och miljö

Dokumenttyp: Policy
Beslutsfattare: Rektor
Avdelning/kansli: Avdelningen för infrastruktur
Handläggare: Informationssäkerhetsstrateg
Marcus Nilsson

Beslutsdatum: 2023-06-14
Träder i kraft: 2023-06-14
Giltighetstid: Tills vidare
Bör uppdateras före: 2026-06-14

Ev. dokument som upphävs: SLU ua 2015.2.10-2118 Riktlinjer för informationssäkerhet vid SLU

Bilaga till: Beslut om informationssäkerhetspolicy för Sveriges lantbruksuniversitet

Informationssäkerhetspolicy för Sveriges lantbruksuniversitet

1. Inledning

Informationssäkerhetspolicyen är det dokument där rektor anger viljeinriktningen för informationssäkerhetsarbetet vid Sveriges lantbruksuniversitet (SLU).

SLU:s vision är att ha en nyckelroll i utvecklingen för hållbart liv, grundad i vetenskap och utbildning. Informationssäkerhetsarbetet ska stödja uppfyllandet av SLU:s vision genom att utgå från proportionella avvägningar mellan akademisk öppenhet och skyddsbehovet för universitetets information. Med informationssäkerhet avses skydd av information mot obehörig åtkomst och oönskad förändring, samt att informationen är tillgänglig för rätt person i rätt tid.

All verksamhet inom informationssäkerhet vid universitetet ska vara riskbaserad. Universitetet ska ha ett ledningssystem för informationssäkerhet med utgångspunkt i ISO/IEC 27001 och ISO/IEC 27002. Universitetet bör i tillämpliga fall använda närliggande standarder inom informations- och it-säkerhet.

Universitetets information ska skyddas från förlust av:

Konfidentialitet – så att informationen inte röjs eller tillgängliggörs för obehöriga.

Riktighet – så att informationen inte förändras på oönskat sätt, vare sig det sker obehörigen, av misstag eller på grund av funktionsstörning.

Tillgänglighet – så att informationen är tillgänglig för behöriga när den behövs.

Universitetet åtar sig med denna policy att verka för ständig förbättring av ledningssystemet för informationssäkerhet och att uppfylla tillämpliga krav inom informationssäkerhet. För att stödja fullgörandet av säkerhetsåtgärder enligt ledningssystemet för informationssäkerhet ska policyn kompletteras av underliggande planer, regler, rutiner eller motsvarande interna styrdokument av betydelse för informationssäkerhetsarbetet vid universitetet.

2. Målgrupp

Informationssäkerhetspolicyn riktar sig till samtliga medarbetare, studenter och övriga inom SLU:s verksamheter som hanterar universitetets information.

3. Mål

SLU:s strategiska informationssäkerhetsmål är att:

- Vår information är kartlagd och klassad enligt universitetets informationsklassningsmodell.
- Våra informationssäkerhetsrisker är kända, bedömda och behandlade enligt universitetets riskhanteringsmodell.
- Vår information och våra informationssystem är ändamålsenligt skyddade.
- Vår forskning, undervisning och stödverksamhet beaktar informationssäkerhet.
- Vår informationssäkerhetskultur är mogen.

De strategiska informationssäkerhetsmålen ska omsättas i verkställbara kortsiktiga mål på årlig basis.

4. Ansvar och roller

Rektor har det övergripande informationssäkerhetsansvaret vid SLU, men delegerar ansvar och beslutsbefogenheter enligt rektors delegationsordning. Rektor ansvarar för att informera sig om statusen på informationssäkerhetsarbetet enligt gällande regelverk.

Universitetsdirektören utser ansvarig för ledningen och samordningen av informationssäkerhetsarbetet. Universitetsdirektören ansvarar för att den eller de som utses att leda och samordna informationssäkerhetsarbetet tilldelas nödvändiga beslutsbefogenheter och resurser.

Säkerhetschefen, tillika säkerhetskylldschefen, ansvarar för beslut om akuta åtgärder rörande informationssäkerhet. Säkerhetschefen ansvarar för informationssäkerheten inom de delar som rör universitetets säkerhetskylldssarbete.

It-direktören ansvarar för att besluta om regler för universitetets it-säkerhet. It-direktören ansvarar för att rapportera statusen på universitetets it-säkerhet till den eller de som utses att leda och samordna informationssäkerhetsarbetet.

Chef för verksamhet ansvarar för informationssäkerheten inom sitt respektive verksamhetsområde. Ansvaret innebär att hantera informationssäkerheten utifrån sin kunskap om både verksamhet och informationens skyddsvärde. Med chef för verksamhet avses prefekt eller motsvarande chef.

Informationsägaren ansvarar för att informationsklassa, riskbedöma och skydda information på ändamålsenligt sätt. Informationsägaren är chefen för verksamheten, eller den som chefen för verksamheten bestämmer, som är ansvarig för den verksamhetsprocess som skapar och hanterar informationen. Informationsägaren är tillika riskägare för informationen, i den utsträckning risken kan hänföras till den egna verksamheten. För universitetsövergripande informationssäkerhetsrisker beslutas riskägare av rektor.

Systemägaren ansvarar för den övergripande informationssäkerheten i respektive informationssystem. Systemägaren ansvarar således för uppfyllnad av krav på tillämpliga säkerhetsåtgärder för informationssystemet utifrån genomförd informationsklassning och riskbedömning. Systemägaren är chefen för verksamheten, eller den som chefen för verksamheten bestämmer, som är ansvarig för den verksamhetsprocess som informationssystemet stödjer.

Alla verksamma vid SLU ansvarar för att skydda information i enlighet med denna policy och bidra till en god informationssäkerhetskultur. Med verksam vid SLU avses anställda, studenter eller medarbetare som arbetar på uppdrag av SLU.

5. Avvikelser och undantag

Informationssäkerhetspolicyn uttrycker universitetets grundkrav avseende informationssäkerhetsarbetet. Avvikelser och undantag från denna policy kan endast beslutas av rektor. Ett beslut om undantag ska dokumenteras.

6. Översyn och efterlevnad

Informationssäkerhetspolicyn ska ses över vart tredje år eller vid betydande förändringar av riskbild, regelverkskrav eller andra förutsättningar som påverkar universitetets informationssäkerhet. Efterlevnaden av policyn ska regelbundet kontrolleras.