Dnr SLU ua 2015.2.10-2118
Exp. den: 2015-05-18/AL

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

SLU Säkerhet | **STYRANDE DOKUMENT**

Sakområde: Säkerhet och informationssäkerhet

Dokumenttyp: Riktlinjer	Beslutsdatum: 2014-05-06
Beslutsfattare: Rektor	Träder i kraft: 2014-05-06
Avdelning/kansli: SLU Säkerhet	Giltighetstid: Tills vidare
Handläggare: Anette Lindberg	Bör uppdateras före: [Datum]

Ev dokument som upphävs: Bilaga till Dnr ua 2014.2.10-1368

Bilaga till: Dnr ua 2014.2.10-1368

Riktlinjer för informationssäkerhet vid SLU

Sveriges lantbruksuniversitets huvuduppgift är att genom högkvalitativ forskning, utbildning och fortlöpande miljöanalys bidra till god livskvalitet och en ökad tillväxt, både i Sverige och i världen. Viktiga förutsättningar och tillgångar för den uppgiften är bland annat information[1] i olika former[2], vilka ska skyddas på ett anpassat sätt.

Myndigheten för samhällsskydd och beredskap, MSB, föreskriver i Föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10) att en myndighet ska bedriva sitt informationssäkerhetsarbete enligt de svenska standarderna SS-ISO/IEC 27001 och SS-ISO/IEC 27002 och upprätta styrande dokument inom informationssäkerhetsområdet. Dessa riktlinjer är en del i det arbetet och ingår i SLU:s ledningssystem för informationssäkerhet på strategisk/taktisk nivå.

Målet med informationssäkerhet är att säkerställa att rätt person, enhet eller process har tillgång till rätt information vid rätt tillfälle[3]:

- Konfidentialitet - egenskapen att information inte tillgängliggörs eller avslöjas för obehörig
- Riktighet - egenskapen att skydda exaktheten och fullständigheten gällande tillgångar
- Tillgänglighet - egenskapen att vara åtkomlig och användbar vid begäran av behörig

[1] T.ex. forskningsrapport, artikel, opublicerade forskningsresultat, rådata, avhandling, examensarbete, examensbevis, tentamenfrågor, journal, instruktion, projektplan, avtal, verifikation, personuppgift, rutiner, lösenord, logg.
[2] Avser såväl talad som digital och skriven information.
[3] Även möjlighet att säkerställa vem som haft åtkomst till information, dvs spårbarhet, är viktig.

Informationssäkerhet är en kombination av administrativ och teknisk säkerhet, där fysisk- och IT-säkerhet ingår i den tekniska säkerheten. Säkerhetslösningar anpassas till hur viktig och skyddsvärd informationen bedöms vara för verksamheten, vilket varierar för olika typer av information. Bedömningen sker genom informationssäkerhetsklassning och riskhantering. På så sätt uppnås en anpassad skyddsnivå för information. Informationssäkerhetsarbete ska bedrivas aktivt och förebyggande men också avhjälpande med åtgärder vid akuta händelser för att minska ev. skadors omfattning.

Riktlinjerna lyder under SLU:s säkerhetspolicy och kompletteras med anvisningar och instruktioner inom olika områden, t.ex. informationssäkerhetsklassning, riskhantering, åtkomststyrning, incidenthantering och kontinuitetsplanering, som beskriver på vilket sätt informationssäkerhet ska upprätthållas. Riktlinjerna och de kompletterande dokumenten är en anpassning till gällande lagar, förordningar, regler, standarder samt till SLU:s säkerhetspolicy och best practice.

Ansvar och roller

Rektor

Rektor har det övergripande informationssäkerhetsansvaret vid SLU men delegerar ansvar och mandat till respektive funktioner i SLU:s organisation enligt delegationsordning.

Säkerhetschef

Genom SLU:s säkerhetsorganisation ansvarar säkerhetschefen för stöd i informationssäkerhetsarbetet i form av planering, samordning, kravställning, uppföljning etc till hela SLU, d.v.s. till såväl verksamheter som verksamhetsansvariga och systemägare. Säkerhetsorganisationen ansvar även för samordning med kravställande myndigheter liksom för hantering av fysiskt skydd och att utreda informationssäkerhetsincidenter.

Chef för verksamhet

Prefekt eller motsvarande chef för verksamhet har ansvar för informationssäkerheten inom sitt ansvarsområde. Ansvaret innebär att hantera informationssäkerheten utifrån sin kunskap om både verksamhet och informationens värde. Värdet bedöms utifrån informationssäkerhetsklassning och riskhantering, vilka även ligger till grund för kontinuitetsplanering som också ska genomföras. Som stöd inom informationssäkerhetsarbetet generellt liksom för specifika delar finns säkerhetsorganisationen.

Informationsägare

Informationsägaren har ansvar för att information informationssäkerhetsklassas och skyddas. Informationsägare är ofta den verksamhetsansvarige vars verksamhet har skapat informationen, fattat beslut om den alternativt tagit över ansvaret för den.

Det kan vara prefekt eller motsvarande chef men det kan också vara delegerat. Ägarskapet kan förändras över tid.

Systemägare

Systemägaren har ansvar för att lämplig skyddsnivå kravställs utifrån övergripande regler och systemspecifik riskbedömning, att säkerheten införs och bibehålls i systemets alla skeenden, att kontinuitetsplanering av verksamhetskritiska system sker och att relevant information gällande säkerhetsnivå i systemet finns tillgänglig. Systemägaren kan och bör söka samråd med säkerhetsorganisationen i sådana frågor.

IT-avdelningen

IT-avdelningen ansvarar för det operativa IT-säkerhetsarbetet, vilket innebär val, införande och distribution av it-säkerhetslösningar, övervakning av datatrafik, rapportering och vidtagande av akuta åtgärder vid intrång i SLU:s olika IT-system, missbruk av IT-resurser och liknande.

Samtliga vid SLU

Alla inom SLU:s verksamhet har eget ansvar för att upprätthålla informationssäkerheten och följa gällande riktlinjer, instruktioner och anvisningar. Det innebär t.ex. att hålla sig uppdaterad gällande informationssäkerhetsregler och att rapportera incidenter till säkerhetsorganisationen. Varje individs kunskap och agerande är mycket viktig för att upprätthålla informationssäkerheten.

Omfattning

Dessa riktlinjer omfattar samtliga SLU:s medarbetare, studenter och övriga inom samtliga SLU:s verksamheter.