DNR SLU ua 2015.2.10-2115
Exp. den: 2015-05-18 / AL

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

STYRANDE DOKUMENT

Sakområde: Säkerhet och informationssäkerhet

Dokumenttyp: Riktlinjer	Beslutsdatum: 2013-02-04
Beslutsfattare: Rektor	Träder i kraft: 2015-05-18
Avdelning/kansli: Avdelningen för infrastruktur	Giltighetstid: Tills vidare
Handläggare: Anette Lindberg, CISO	Bör uppdateras före:

Ev dokument som upphävs: Bilaga till DNR SLU ua 2013.02.10-650

Bilaga till: Beslut Riktlinjer för informationssäkerhetsklassning, DNR SLU ua 2013.2.10-650

Riktlinjer för informationssäkerhetsklassning

Syfte och bakgrund

Syftet med informationssäkerhetsklassning är att tydliggöra att olika typer av information har olika värde för verksamheten och att informationen därmed måste skyddas på olika nivåer (skyddsnivåer).

Myndigheten för samhällsskydd och beredskap, MSB, föreskriver[1] i 4§ Föreskrifter (MSBFS 2009:10) om statliga myndigheters informationssäkerhet att en myndighet ska klassificera sin information med utgångspunkt i krav på:

- Konfidentialitet[2] - egenskapen att information inte tillgängliggörs eller avslöjas till obehöriga individer, enheter, eller processer
- Riktighet[2] - egenskapen att skydda exaktheten och fullständigheten gällande tillgångar
- Tillgänglighet[2] - egenskapen att vara åtkomlig och användbar vid begäran av en behörig enhet

SLU:s riktlinjer baseras på MSB:s guide ”Modell för klassificering av information” och är en del i SLU:s ledningssystem för informationssäkerhet på strategisk/taktisk nivån enligt ISO/IEC 27001.

Det ska noteras att det även finns andra typer av klassning av information, t.ex. ur arkivredovisningens (RA-FS 2008:4) perspektiv, som inte behandlas i dessa riktlinjer för informationssäkerhetsklassning.

[1] MSB föreskriver med stöd av 34 § Förordning (2006:942) om krisberedskap och höjd beredskap.
[2] Definition enligt ISO/IEC 27001 Ledningssystem för informationssäkerhet, vilken är den kravstandard som anges i Föreskrifter (MSBFS 2009:10) om statliga myndigheters informationssäkerhet.

Vad ska informationssäkerhetsklassas?

MSB föreskriver att ”en myndighet ska klassificera sin information”. SLU:s information kommer att grupperas i så kallade klassningsobjekt. Klassningsobjekt kan, beroende på vad som är lämpligast, vara hel eller del av organisation, ett projekt, ett IT-system, en databas, en process etc. Varje klassningsobjekt består av ett antal olika typer av information.

Ansvar

Det är ägare[3] av information som är ansvarig för att informationen informationssäkerhetsklassas. Ägare är ofta den verksamhetsansvarige vars verksamhet har skapat informationen, fattat beslut om den alternativt tagit över ansvaret för den. Det kan vara dekan, prefekt, forskningsledare, universitetsdirektör, avdelningschef, enhetschef, funktionschef eller motsvarande beroende på aktuell delgering. Ägarskapet kan förändras över tid.

Konsekvensbedömning

Information ska klassas utifrån vilka konsekvenser som oönskad påverkan på informationen bedöms leda till ur aspekterna konfidentialitet, riktighet och tillgänglighet. Ju större konsekvens desto högre klass. Observera att bedömningen kan bli exempelvis hög klass, dvs stor konsekvens, i tillgänglighet och låg i konfidentialitet. Varje typ av information får tre bedömningar, en ur varje aspekt konfidentialitet, riktighet och tillgänglighet.

Resultat

Resultatet av bedömningen visar till vilken grad verksamheten kan drabbas om konfidentialitet, riktighet eller tillgänglighet påverkas. Utifrån denna bedömning skyddas informationen i olika nivåer, t.ex. gällande hantering, förvaring, dokumentation, förstärkt inloggning, uppkoppling, mailhantering och digital lagring av information. Det kan få stora konsekvenser för verksamheten om informationen skyddas till för låg nivå liksom det är kostsamt att skydda information till högsta nivå.

[3] Standarden ISO/IEC 27001:2005 Ledningssystem för informationssäkerhet uttrycker: Termen ”ägare” avser en person eller enhet som har ett uttalat ledningsansvar för att styra produktion, utveckling, underhåll, användning och säkerhet avseende dessa tillgångar.

Omklassning

Det är viktigt att en förnyad bedömning görs när informationens betydelse för verksamheten förändras, vilket den ofta gör över tid. Viss information kan behöva skyddas utifrån hög klass avseende konfidentialitet vid en tidpunkt för att senare vara t.ex. publicerad och inte ha några som helst krav på konfidentialitet. Detsamma gäller tillgänglighet och riktighet.

Tillvägagångssätt och dokumentation

Tillvägagångssättet vid informationssäkerhetsklassning beskrivs i ”Instruktion för informationssäkerhetsklassning”, fastställd av SLU:s säkerhetschef.

Resultatet av informationssäkerhetsklassning dokumenteras i ”Mall för informationssäkerhetsklassning”, fastställd av SLU:s säkerhetschef. Resultatet ska sparas hos både den ansvarige för den klassade informationen och hos SLU Säkerhet. I de fall klassingen är till nytta för andra verksamheter inom SLU bör resultatet delas med dessa.

Stöd vid informationssäkerhetsklassning finns att få hos SLU Säkerhet.

Ovan nämnda dokument samt kontaktuppgifter finns tillgänglig på SLU Säkerhets sidor på medarbetarwebben.