

Sakområde: IT, service, säkerhet och miljö

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

Beslutsdatum: 2024-06-24
Träder i kraft: 2024-06-24
Giltighetstid: Tills vidare
Bör uppdateras före: 2027-06-24

Dokument som upphävs: SLU ua 2015.2.10-2115 Riktlinjer för informationssäkerhetsklassning; SÅK 2014-19 Instruktion för informationssäkerhetsklassning; SÅK 2015-17 Skyddsnivå utifrån informationssäkerhetsklassning; SLU.ua 2019.2.8.3-4147 Instruktion för åtkomsthantering av system.

Bilaga till: Beslut om regler för informationsklassning vid Sveriges lantbruksuniversitet.

Regler för informationsklassning vid Sveriges lantbruksuniversitet

1. Syfte och målgrupp

Detta dokument anger ramverket för att klassa och skydda information vid Sveriges lantbruksuniversitet (SLU). Dokumentet riktar sig till personer som innehar rollerna som informationsägare och systemägare vid SLU.¹

Informationsklassning innebär att värdera SLU:s information med utgångspunkt i de konsekvenser och skadeverkningar som kan uppstå om informationen inte hanteras säkert. Informationsklassning syftar till att etablera ett anpassat skydd för informationen som motsvarar dess värde och betydelse. Olika typer av information har olika värden och ska således skyddas med olika säkerhetsåtgärder. Resultatet av en informationsklassning avgör, tillsammans med en riskbedömning, vilka säkerhetsåtgärder som ska vidtas för att skydda informationen.

SLU:s information ska klassas utifrån aspekterna:

Konfidentialitet – egenskap som innebär att informationen inte röjs eller tillgängliggörs för obehöriga.

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

Tillgänglighet – egenskap som innebär att informationen är tillgänglig för behöriga när den behövs.

¹ Se vidare SLU.ua.2023.2.10-2023 Informationssäkerhetspolicy för Sveriges lantbruksuniversitet.

Föreliggande regler beskriver SLU:s informationsklassningsmodell, konsekvenskategorier för informationsklassning, grundregler för genomförande av informationsklassning, samt riktlinjer för dokumentation och återrapportering. Till reglerna hör även en kravkatalog som anger vilka informations- och it-säkerhetskrav som ska uppfyllas för SLU:s it-tjänster utifrån värderingen av informationens konfidentialitet, riktighet och tillgänglighet.

Dessa regler kompletteras av rutinen för genomförande av informationsklassning vid SLU.

2. Informationsklassningsmodell för SLU

En informationsklassningsmodell används för att bedöma de förväntade skadeverkningarna av att information röjs, förvanskas eller görs otillgänglig. SLU:s informationsklassningsmodell kategoriserar skadeverkningarna hierarkiskt i fem olika klasser utifrån aspekterna konfidentialitet, riktighet och tillgänglighet. Varje klass värderas utifrån graden av skada som kan uppstå för SLU, individer eller externa intressenter. Ju högre klass, desto högre grad av skada. SLU:s informationsklassningsmodell framgår av tabellen nedan.

Tabell 1: SLU:s informationsklassningsmodell.

Klass	Skada	KONFIDENTIALITET	RIKTIGHET	TILLGÄNGLIGHET
Säkerhets-skyddsklass	Sveriges säkerhet	Säkerhetsskyddsklassificerad information som omfattas av säkerhetsskyddslagstiftningen. Särskild hantering.	Säkerhetsskyddsklassificerad information som omfattas av säkerhetsskyddslagstiftningen. Särskild hantering.	Säkerhetsskyddsklassificerad information som omfattas av säkerhetsskyddslagstiftningen. Särskild hantering.
Klass 3	Mycket allvarlig	Mycket konfidentiell information som förväntas leda till mycket allvarlig skada för SLU, individer eller externa intressenter om den röjs eller tillgängliggörs för obehörig.	Information som förväntas leda till mycket allvarlig skada för SLU, individer eller externa intressenter om den inte är riktig och fullständig.	Information som förväntas leda till mycket allvarlig skada för SLU, individer eller externa intressenter om den inte är tillgänglig för behörig inom en timme .
Klass 2	Allvarlig	Konfidentiell information som förväntas leda till allvarlig skada för SLU, individer eller externa intressenter om den röjs eller tillgängliggörs för obehörig.	Information som förväntas leda till allvarlig skada för SLU, individer eller externa intressenter om den inte är riktig och fullständig.	Information som förväntas leda till allvarlig skada för SLU, individer eller externa intressenter om den inte är tillgänglig för behörig inom en dag .
Klass 1	Besvärande	Intern information som förväntas leda till besvärande skada för SLU, individer eller externa intressenter om den röjs eller tillgängliggörs för obehörig.	Information som förväntas leda till besvärande skada för SLU, individer eller externa intressenter om den inte är riktig och fullständig.	Information som förväntas leda till besvärande skada för SLU, individer eller externa intressenter om den inte är tillgänglig för behörig inom en vecka .
Klass 0	Ingen/ Försumbar	Öppen information som förväntas leda till ingen eller försumbar skada för SLU, individer eller externa intressenter om den röjs eller tillgängliggörs för obehörig.	Information som förväntas leda till ingen eller försumbar skada för SLU, individer eller externa intressenter om den inte är riktig och fullständig.	Information som förväntas leda till ingen eller försumbar skada för SLU, individer eller externa intressenter om den inte är tillgänglig för behörig inom en månad .

2.1. Regler för tillämpning av informationsklassningsmodellen

Information som klassas enligt SLU:s informationsklassningsmodell ska indelas i informationstyper. En informationstyp motsvarar en särskild kategori av information som definieras av informationsägaren eller av tillämpliga regelverk. Exempel på informationstyper är känsliga personuppgifter, opublicerad forskningsdata, rapporter, källkod eller loggar.

Varje informationstyp som värderas enligt informationsklassningsmodellen ska klassas utifrån samtliga tre aspekter konfidentialitet, riktighet och tillgänglighet. En informationstyp ska således tilldelas ett av värdena klass 0, klass 1, klass 2 eller klass 3 för respektive aspekt. Säkerhetsskyddsklassificerade uppgifter ska klassas enligt särskilda konsekvenskategorier och säkerhetsskyddsklasser som anges i säkerhetsskyddslagstiftningen.

Informationstyper som klassas vid SLU ska vidare grupperas i ett klassningsobjekt. Ett klassningsobjekt är en logisk och för verksamheten meningsfull del av organisationen där information skapas, lagras eller på annat sätt behandlas. Exempel på klassningsobjekt är it-tjänster, verksamhetsprocesser eller forskningsprojekt.

Mer information om tillämpningen av informationsklassningsmodellen finns i rutinen för genomförande av informationsklassning.

3. Konsekvenskategorier för informationsklassning

Som framgår av informationsklassningsmodellen klassas SLU:s information utifrån de skadeverkningar som kan uppstå för tre parter: SLU, individer eller externa intressenter. För att värdera skadeverkningarna för dessa parter om information röjs, förvanskas eller görs otillgänglig ska universitetsgemensamma konsekvenskategorier användas.

En konsekvenskategori används för att stödja bedömningen av skadeverkningarna för SLU, individer eller externa intressenter utifrån informationsklassningsmodellens klassningsnivåer. En konsekvenskategori syftar således till att utgöra en gemensam bedömningsgrund för en viss skadeverkan om information inte hanteras säkert med avseende på dess konfidentialitet, riktighet och tillgänglighet. I samband med en informationsklassning bör flera konsekvenskategorier kombineras för att göra en helhetsbedömning av skadeverkningarna om den aktuella informationstypen röjs, förvanskas eller görs otillgänglig.

I tabell 2 nedan beskrivs konsekvenskategorierna för informationsklassning vid SLU.

Tabell 2: Konsekvenskategorier för informationsklassning vid SLU.

PART	KONSEKVENSKATEGORI	SKADEVERKAN
SLU	<i>Verksamhetspåverkan</i>	Förlust av informationens konfidentialitet, riktighet eller tillgänglighet leder till <i>negativ påverkan på SLU:s förmåga att utföra sitt uppdrag</i> inom forskning, undervisning, miljöanalys eller stödverksamhet.
	<i>Förtroende</i>	Förlust av informationens konfidentialitet, riktighet eller tillgänglighet leder till <i>förtroendeskada</i> för SLU till följd av negativ publicitet och negativ allmän opinion.
	<i>Ekonomi</i>	Förlust av informationens konfidentialitet, riktighet eller tillgänglighet leder till <i>ekonomisk skada</i> för SLU i form av ökade kostnader, minskade intäkter eller skador på tillgångar.
	<i>Lagefterlevnad</i>	Förlust av informationens konfidentialitet, riktighet eller tillgänglighet leder till <i>brott eller avvikelser</i> mot för SLU tillämpliga lagar, förordningar eller föreskrifter.
Individer	<i>Liv och hälsa</i>	Förlust av informationens konfidentialitet, riktighet eller tillgänglighet leder till <i>skada på liv och hälsa</i> för SLU:s anställda, studenter, verksamma eller andra individer.
	<i>Fri- och rättigheter</i>	Förlust av informationens konfidentialitet, riktighet eller tillgänglighet leder till <i>negativ påverkan på friheter och rättigheter</i> för SLU:s anställda, studenter, verksamma eller andra individer.
Externa intressenter	<i>Skada för externa intressenter</i>	Förlust av informationens konfidentialitet, riktighet eller tillgänglighet leder till <i>skada för externa intressenter</i> (myndigheter, företag, forskningspartners) vad avser förmågan att utföra uppdrag, förtroende eller ekonomi.

Konsekvenskategorierna är kopplade till informationsklassningsmodellens klassningsnivåer enligt tabell 3 nedan. Varje klassningsnivå i tabellen innehåller en beskrivning av hur skadeverkningarna på respektive nivå kan tolkas eller mätas utifrån konsekvenskategorierna. Beskrivningarna av skadeverkningarna representerar på så sätt en nedbrytning av informationsklassningsmodellens schema över vad som utgör ingen eller försumbar skada (klass 0), besvärande skada (klass 1), allvarlig skada (klass 2) eller mycket allvarlig skada (klass 3). Vid informationsklassning bör tabellen användas som en referenstabell för att värdera i vilken klass som en viss informationstyp ska placeras för respektive aspekt konfidentialitet, riktighet och tillgänglighet.

Tabell 3: Konsekvenskategorier för informationsklassning utifrån klassningsnivåer.

KONSEKVENSKATEGORI	KLASS 0	KLASS 1	KLASS 2	KLASS 3
<i>Verksamhetspåverkan</i>	<ul style="list-style-type: none"> Ingen eller försumbar negativ påverkan på SLU:s förmåga att utföra sitt uppdrag. Inga förlorade arbetstimmar och/eller extra övertidstimmar till följd av negativ påverkan på SLU:s verksamhet. 	<ul style="list-style-type: none"> Besvärande negativ påverkan på SLU:s förmåga att utföra sitt uppdrag. En till några förlorade arbetstimmar och/eller extra övertidstimmar till följd av negativ påverkan på SLU:s verksamhet. 	<ul style="list-style-type: none"> Allvarlig negativ påverkan på SLU:s förmåga att utföra sitt uppdrag. Flera förlorade arbetstimmar och/eller extra övertidstimmar till följd av negativ påverkan på SLU:s verksamhet. 	<ul style="list-style-type: none"> Mycket allvarlig negativ påverkan på SLU:s förmåga att utföra sitt uppdrag. Många förlorade arbetstimmar och/eller extra övertidstimmar till följd av negativ påverkan på SLU:s verksamhet.
<i>Förtroende</i>	<ul style="list-style-type: none"> Ingen eller försumbar förtroendskada för SLU. Inga individer och/eller organisationer förlorar förtroendet för SLU. 	<ul style="list-style-type: none"> Besvärande förtroendskada för SLU. En till några individer och/eller organisationer förlorar förtroendet för SLU. 	<ul style="list-style-type: none"> Allvarlig förtroendskada för SLU. Flera individer och/eller organisationer förlorar förtroendet för SLU. 	<ul style="list-style-type: none"> Mycket allvarlig förtroendskada för SLU. Många individer och/eller organisationer förlorar förtroendet för SLU.
<i>Ekonomi</i>	<ul style="list-style-type: none"> Ingen eller försumbar ekonomisk skada åsamkas SLU (under 10 000 SEK). 	<ul style="list-style-type: none"> Besvärande ekonomisk skada åsamkas en eller flera avdelningar, fakulteter eller motsvarande vid SLU (över 10 000 SEK och under 100 000 SEK). 	<ul style="list-style-type: none"> Allvarlig ekonomisk skada åsamkas en eller flera avdelningar, fakulteter eller motsvarande vid SLU (över 100 000 SEK och under 1 000 000 SEK). 	<ul style="list-style-type: none"> Mycket allvarlig ekonomisk skada åsamkas en eller flera avdelningar, fakulteter eller motsvarande vid SLU (över 1 000 000 SEK).

<p><i>Lagefterlevnad</i></p>	<ul style="list-style-type: none"> • Inga brott eller avvikelser mot tillämpliga regelverk. • Inga sanktionsavgifter, förelägganden, reprimander eller motsvarande utfärdas mot SLU. 	<ul style="list-style-type: none"> • Brott eller avvikelser mot tillämpliga regelverk med besvärande konsekvenser för SLU. • Låga sanktionsavgifter (under 100 000 SEK) utfärdas mot SLU. • Reprimand eller motsvarande utfärdas mot SLU. 	<ul style="list-style-type: none"> • Brott eller avvikelser mot tillämpliga regelverk med allvarliga konsekvenser för SLU. • Höga sanktionsavgifter (över 100 000 SEK och under 1 000 000 SEK) utfärdas mot SLU. • Föreläggande utfärdas mot SLU. 	<ul style="list-style-type: none"> • Brott eller avvikelser mot tillämpliga regelverk med mycket allvarliga konsekvenser för SLU. • Mycket höga sanktionsavgifter (över 1 000 000 SEK) utfärdas mot SLU. • Föreläggande med vite och/eller förbud utfärdas mot SLU.
<p><i>Liv och hälsa</i></p>	<ul style="list-style-type: none"> • Ingen eller försumbar skada på individers fysiska eller mentala hälsa. 	<ul style="list-style-type: none"> • Besvärande skada på individers fysiska eller mentala hälsa i form av mindre och tillfällig skada. 	<ul style="list-style-type: none"> • Allvarlig skada på individers fysiska eller mentala hälsa i form av permanent men icke-livshotande skada. 	<ul style="list-style-type: none"> • Mycket allvarlig skada på individers fysiska eller mentala hälsa i form av permanent, livshotande eller dödlig skada.
<p><i>Fri- och rättigheter</i></p>	<ul style="list-style-type: none"> • Ingen eller försumbar fysisk, materiell eller immateriell skada på individers fri- och rättigheter till följd av bristfällig hantering av personuppgifter. 	<ul style="list-style-type: none"> • Besvärande fysisk, materiell eller immateriell skada på individers fri- och rättigheter till följd av bristfällig hantering av personuppgifter. 	<ul style="list-style-type: none"> • Allvarlig fysisk, materiell eller immateriell skada på individers fri- och rättigheter till följd av bristfällig hantering av personuppgifter. 	<ul style="list-style-type: none"> • Mycket allvarlig fysisk, materiell eller immateriell skada på individers fri- och rättigheter till följd av bristfällig hantering av personuppgifter.
<p><i>Skada för externa intressenter</i></p>	<ul style="list-style-type: none"> • Ingen eller försumbar skada för externa intressenter (myndigheter, företag, forskningspartners) vad avser förmågan att utföra uppdrag, förtroende eller ekonomi. 	<ul style="list-style-type: none"> • Besvärande skada för externa intressenter (myndigheter, företag, forskningspartners) vad avser förmågan att utföra uppdrag, förtroende eller ekonomi. 	<ul style="list-style-type: none"> • Allvarlig skada för externa intressenter (myndigheter, företag, forskningspartners) vad avser förmågan att utföra uppdrag, förtroende eller ekonomi. 	<ul style="list-style-type: none"> • Mycket allvarlig skada för externa intressenter (myndigheter, företag, forskningspartners) vad avser förmågan att utföra uppdrag, förtroende eller ekonomi.

4. Genomförande av informationsklassning

En informationsklassning ska genomföras i samband med anskaffning, utveckling eller vid större förändring av en it-tjänst. En informationsklassning ska upprättas och därefter underhållas över tid för varje nytt projekt och/eller undersökning inom forskning och miljöanalys. I enlighet med SLU:s informationssäkerhetspolicy ansvarar informationsägaren för att klassa informationen. Om informationen har klassats av annan person än informationsägaren ska informationsägaren granska och godkänna den genomförda informationsklassningen. En genomförd informationsklassning bör ses över en gång per år.

5. Kravkatalog för informations- och it-säkerhetskrav

Av bilaga 1 framgår SLU:s kravkatalog för informations- och it-säkerhetskrav. Kravkatalogen omfattar krav på it-tjänster vid SLU utifrån resultatet av en genomförd informationsklassning. Systemägaren ansvarar för uppfyllnad av kraven i enlighet med SLU:s informationssäkerhetspolicy. Stöd i arbetet med kravuppfyllnad kan ges av Säkerhetsenheten och IT-avdelningen.

I de fall då den informationstyp som klassas inte hanteras i it-tjänster, t.ex. då information behandlas analogt eller muntligt, ska anpassade säkerhetsåtgärder vidtas som motsvarar informationstypens klassningsnivå. Samråd om val av säkerhetsåtgärder bör sökas med Säkerhetsenheten.

6. Dokumentation och återrapportering

En informationsklassning ska dokumenteras i en av Säkerhetsenheten anvisad mall. Informationsägaren är dokumentägare för den genomförda informationsklassningen. Informationsägaren ska tillhandahålla en kopia av den genomförda informationsklassningen till Säkerhetsenheten.

Kravuppfyllnad enligt kravkatalogen för informations- och it-säkerhetskrav ska återrapporteras till Säkerhetsenheten av systemägaren för it-tjänsten.

7. Bilagor

Bilaga 1: Kravkatalog för informations- och it-säkerhetskrav vid Sveriges lantbruksuniversitet.