DNR: SÄK 2014-19
Exp. den: 2014-12-16

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

STYRANDE DOKUMENT

Sakområde: Säkerhet och informationssäkerhet

Dokumenttyp: Anvisning/Instruktion	Beslutsdatum: 2014-12-18
Beslutsfattare: Säkerhetschef	Träder i kraft: 2014-12-18
Avdelning/kansli: SLU Säkerhet	Giltighetstid: tills vidare
Handläggare: Informationssäkerhetschef	Bör uppdateras före: [Datum]

Ev dokument som upphävs: -

Bilaga till: -

Instruktion för informationssäkerhetsklassning

Syfte

Syftet med informationssäkerhetsklassning är att tydliggöra att olika typer av information har olika värde för SLU utifrån aspekterna konfidentialitet, riktighet och tillgänglighet[1], vilket också leder till olika behov av skydd.

a) Konfidentialitet innebär att information inte ska avslöjas eller vara tillgänglig för obehörig.
b) Riktighet innebär att information inte obehörigt ändras eller modifieras, varken obehörigen, av misstag eller på grund av funktionsstörning.
c) Tillgänglighet innebär att informationen finns att tillgå, dels här och nu i förväntad utsträckning och inom önskad tid men också hur länge den ska sparas i framtiden.

För att kunna hantera information på ett säkert och anpassat sätt, för att kunna kravställa eller upprätthålla säkerheten i ett it-system eller att genomföra riskbedömningar är det viktigt att veta informationens värde, dvs att informationssäkerhetsklassa.

Ansvar

Myndigheten för samhällsskydd och beredskap, MSB, uttrycker att ”en myndighet ska klassificera sin information”. Det är ägare[2] 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. Ägarskapet kan förändras över tid.

[1] Även möjligheten att säkerställa vem som haft åtkomst till information, dvs spårbarhet, kan vara viktig att ange. Se kapitel Övrigt på sid 3.
[2] Standarden SS-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. Termen ”ägare” innebär inte att personen har faktisk äganderätt till tillgången.*

Tillvägagångssätt

”Mall för informationssäkerhetsklassning” finns framtagen för registrering av klassningsresultatet och den finns på SLU Säkerhets sidor på medarbetarwebben. Använd mallen och registrera resultatet löpande under klassningen enligt beskrivning nedan. Observera att flöden för bestämmande av klass och konsekvensnivåer beskrivs på sid 5 och 9.

1. Inledning

1.1. Dokumentadministration:
Öppna ”Mall för informationssäkerhetsklassning”. Fyll i dokumenthuvudet med datum för klassning, författare, organisationstillhörighet.
Spara filen så att klassningsobjektets namn framgår.

1.2. Klassningsobjekt och Beskrivning:
Namnge vad som ska informationssäkerhetsklassas, ett så kallat klassningsobjekt. Klassningens omfattning kan vara ett projekt, hel eller del av organisation, en process ett IT-system, en databas, etc. Klassningsobjektet blir en gruppering av ett antal olika typer av information. För att underlätta förståelsen av vad som ska klassas och vad som inte ska klassas kan objektet beskrivas. Det kan vara ett projekts omfattning, en verksamhets avgränsning, ett IT-systems användningsområde etc.

1.3. Kl.datum, Ansvarig och Deltagare:
Ange när klassningen har ägt rum, vem som är ansvarig för klassningsobjektet och vilka som deltog. Ansvarig för objektet behöver inte vara närvarande men denne är troligtvis informationsägare. I de fall t.ex. förtydliganden behöver göras eller när omklassning ska genomföras är de bra att veta vilka som genomförde tidigare klassning. Komplettera med befattning och kontaktuppgifter.

2. Identifiera typ av information

Identifiera de olika typer av information[3] som finns inom klassningsobjektet och registrera dessa i kolumnen. I de fall informationen är mycket beroende av specifik hårdvara eller likande kan detta anges för att påvisa dess värde.
Det kan vara svårt att avgöra till vilken detaljeringsgrad information ska identifieras. I de fall en informationstyps värde avviker från övriga typer kan den definieras extra noga. Dessutom kan de informationstyper vars bedömning förändras över tid anges som två olika informationstyper, t.ex. publicerad och opublicerad rapport, ansökningsinformation vid ansökningstider och vid övrig tid. Dessa informationstyper används med fördel i riskbedömning.

[3] Exempel på typ av information kan vara offentlig forskningsrapport, artiklar, opublicerat forskningsresultat, rådata, avhandlingar, bilder, studieanmälan, tentamensfrågor, examensarbete, examensbevis, projektplan, anbud, avtal, personuppgifter, interna rutiner, loggar, lösenord, information på externwebben.
Observera att här avses inte bara allmänna handlingar.
Observera även att t.ex. en databas ofta innehåller ett flertal olika informationstyper.

3. Konsekvensbedömning avseende konfidentialitet, riktighet och tillgänglighet

Information klassificeras utifrån vilka konsekvenser, dvs skada på SLU:s värden (exempelvis *allvarlig skada),* som oönskad påverkan på informationen bedöms kunna leda till utifrån konfidentialitet, tillgänglighet och riktighet. Konsekvensens, dvs den eventuella skadans, storlek leder till klass 3, 2, 1 eller 0.

3.1. Ta den första typen av information som skrivits in i tabellen och bedöm vilken konsekvens det skulle innebära för SLU om konfidentialitet förlorades. Läs igenom frågorna och följ flödet i kapitel ”Frågor och flöde för att avgöra klass (konsekvensnivå)” på sid 5 för att välja nivå på klass. Konsekvensnivåerna nämnda i flödet definieras i kapitel ”Beskrivning av konsekvensnivåer kopplat till informationssäkerhetsklass” på sid 9.

3.2. Registrera typens informationssäkerhetsklass för konfidentialitet i tabellen i formen K0, K1, K2 eller K3. Komplettera gärna bedömningen med kommentar för att kunna följa resonemanget i efterhand.

3.3. Motsvarande bedömning görs för informationstypen gällande riktighet (R0, R1, R2 eller R3), tillgänglighet på kort sikt (TK0, TK1, TK2 eller TK3) och tillgänglighet på lång sikt (TL0, TL1, TL2 eller TL3) Byt ut *konfidentialitet* mot *riktighet* och *tillgänglighet* och *K* mot *R, TK och TL* i beskrivningen på sid 9.

3.4. Varje informationstyp ska ha bedömning gällande alla aspekterna konfidentialitet, riktighet och tillgänglighet på kort och lång sikt, vilket ger kombinationer såsom exempelvis K0 R1 TK2 TL1 eller K1 R2 TK0 TL0.

4. Övrigt

Här kan typen av information beskrivas, bedömning förklaras, sekretessparagraf[4] anges, speciella spårbarhetskrav[5], tidsaspekter gällande tillgänglighet, speciella beroenden förtydligas om det antas kan vara till nytta för andra läsare eller kommande omklassningar.

5. Sammanfattning, slutsats

Här anges vilka slutsatser som dras av klassningen, speciellt viktiga informationstyper, förslag på skydd, tidsaspekter osv.

[4] Vid begäran om utlämnande av information görs en sekretessbedömning, men det är lämpligt att vid klassningstillfället göra en uppskattning av om information kan antas omfattas av sekretess.

[5] Även möjligheten att säkerställa vem som haft åtkomst till information, dvs spårbarhet, kan vara en viktig informationssäkerhetsaspekt.

Resultatet

Varje typ av information ska nu ha fått en kombination av informations-säkerhetsklasser uttryckt i Kx Rx TKx TLx. Det kan vara t.ex. Årsrapport K0R2TK1TL1.

Resultatet sparas i fil namngiven så att klassningsobjektet framgår. Kopia på resultatet ska finnas hos SLU Säkerhet. För kontaktuppgifter, se medarbetarwebben.

Resultatet ligger till grund för på vilket sätt information får hanteras, var den får lagras, om den ska krypteras, långtidsförvaras, vem som får ta del av den, vilka krav som ska ställas på specifikt IT-system etc.

Omklassning

Det är viktigt att omklassning sker om informationens betydelse förändras, vilket den ofta gör över tid. T.ex. kan viss information behöva skyddas utifrån hög klass avseende konfidentialitet, K2, vid en tidpunkt för att senare vara t.ex. publicerad och inte ha några som helst krav på konfidentialitet, K0. Detsamma gäller tillgänglighet och riktighet. För att underlätta omklassningen kan det ha stor betydelse att tydliga kommentarer till varför har antecknats i övrigt-kolumnen vid det tidigare klassningstillfället.

Det kan vara lämpligt att ha informationssäkerhetsklassning som en stående punkt i verksamhetsplaneringen.

Frågor och flöde för att avgöra klass (konsekvensnivå)

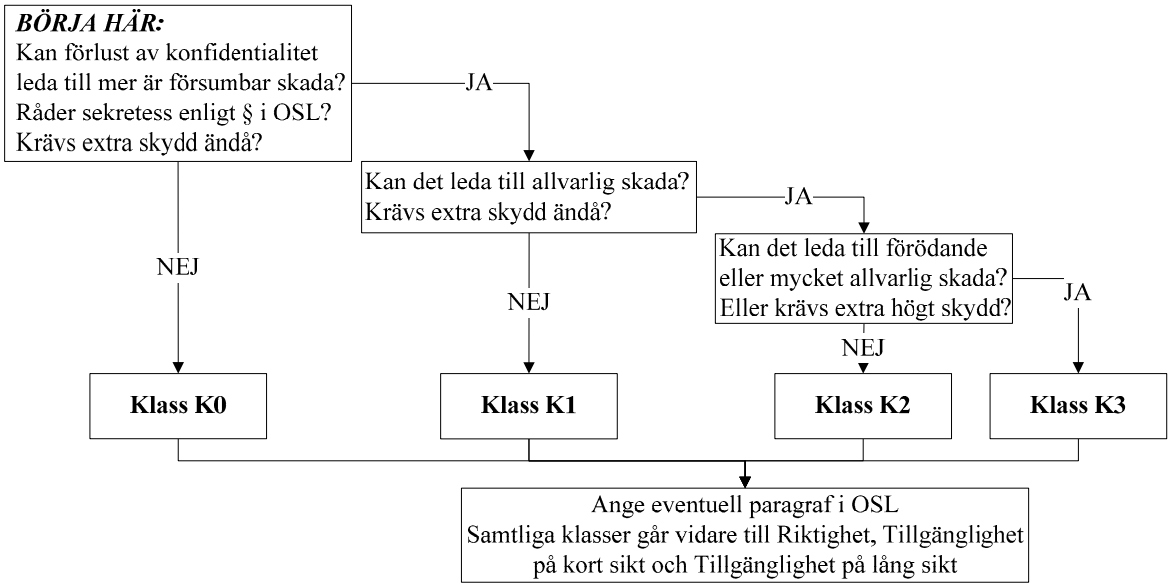
Kategori ”Konfidentialitet”

Konfidentialitet innebär att information inte ska avslöjas eller vara tillgänglig för obehörig.

För att underlätta bedömningen kan nedanstående frågor beaktas:

a) Vad innebär avslöjande utanför SLU, inom SLU, till enstaka medarbetare?
b) Vilken är det största skadan som kan uppstå?
c) Vad blir skadan utifrån ekonomi, förtroende, moral osv?
d) Bryts eventuella avtal eller lagar om informationen avslöjas?
e) Kan information komma att sekretessbeläggas[6] (t.ex. avseende skydd av utrotningshotade arter eller rikets säkerhet) enligt paragraf i Offentlighets- och Sekretesslag (2009:400) vid begäran om utlämnande[7]?
f) Kräver eventuell sekretess (t.ex. sekretess med avseende på skydd av rikets säkerhet) specifika skyddsåtgärder, såsom märkning, förvaring, kryptering, isolerat IT-system osv?

Svaren på frågorna ovan bedöms utifrån konsekvensnivåerna beskrivna på sid 9.



[6] Sekretessbelagd uppgift ska skyddas från obehörig insyn.
[7] Observera att vid begäran om utlämnande av allmän handling görs bedömning i enlighet med Tryckfrihetsförordningen och Offentlighets- och sekretesslagen (OSL) oberoende av denna klassning.

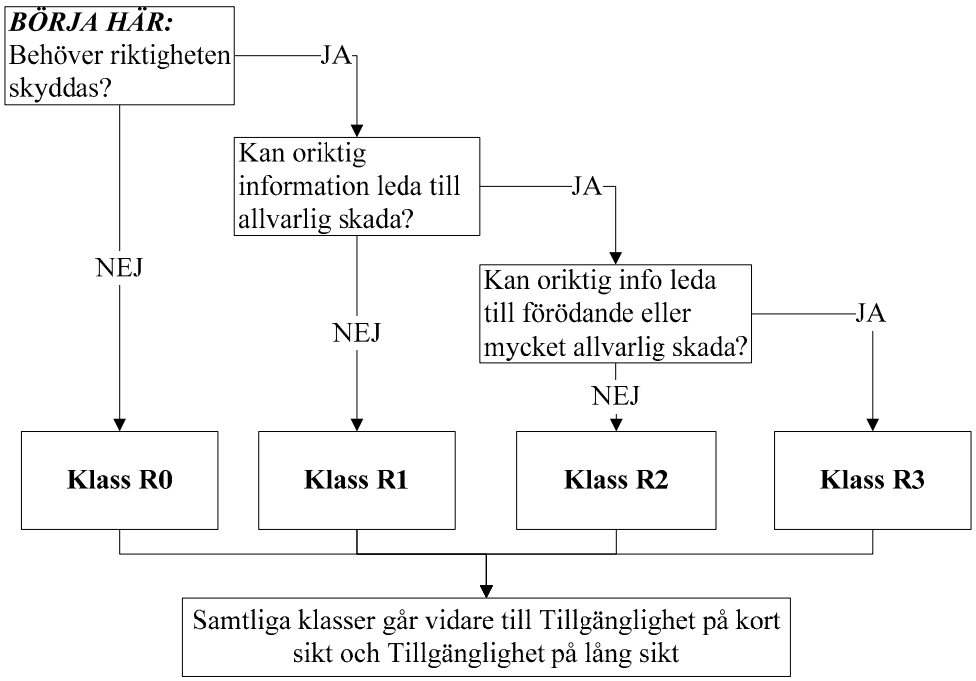
Konsekvensbedömning för kategori ”Riktighet”

Riktighet innebär att information inte obehörigt ändras eller modifieras, varken otillåten, av misstag eller på grund av funktionsstörning.

För att underlätta bedömningen kan nedanstående frågor beaktas:

a) Vad innebär det om informationen förändras på ett för SLU icke avsett sätt?
b) Finns tillämpliga lagkrav avseende riktighet?
c) Vad är det värsta som kan hända om informationen är oriktig?
d) Räcker det att informationen är tolkningsbar eller måste den vara exakt?

Svaren på frågorna ovan bedöms utifrån konsekvensnivåerna beskrivna på sid 9.



Konsekvensbedömning för kategori ”Tillgänglighet på kort sikt”

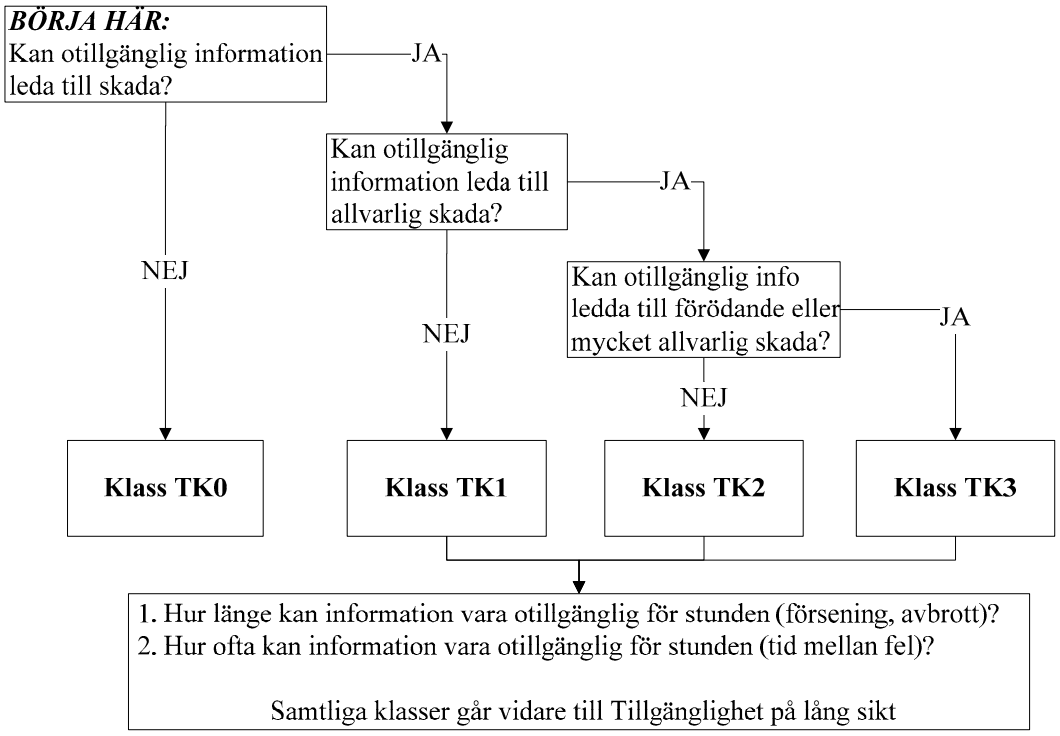
Tillgänglighet på kort sikt innebär att informationen finns att tillgå ”här och nu” i förväntad utsträckning och inom önskad tid.

För att underlätta bedömningen kan nedanstående frågor beaktas:

a) Hur långa avbrott tål SLU? Måste informationen vara tillgänglig konstant, inom en timme, en dag, en vecka, en månad eller räcker det med ett år?
b) Vad innebär kortare avbrott dagligen eller veckovis?
c) Vad innebär det om informationen blir tillgänglig betydligt långsammare än tänkt?
d) Behöver informationen vara tillgänglig via internet, på gemensam server, via löstagbart media?
e) Förändras tillgänglighetskravet över olika återkommande perioder och över tid?

Tidsaspekterna ovan kommer inte hanteras i klassningen pga att det skulle medföra alltför många klassningsnivåer. Tidsaspekterna måste hanteras på annat sätt, t.ex. genom krav på IT-system, säkerhetskopiering, lagring osv.

Svaren på frågorna ovan bedöms utifrån konsekvensnivåerna beskrivna på sid 9.



Konsekvensbedömning för kategori ”Tillgänglighet på lång sikt”

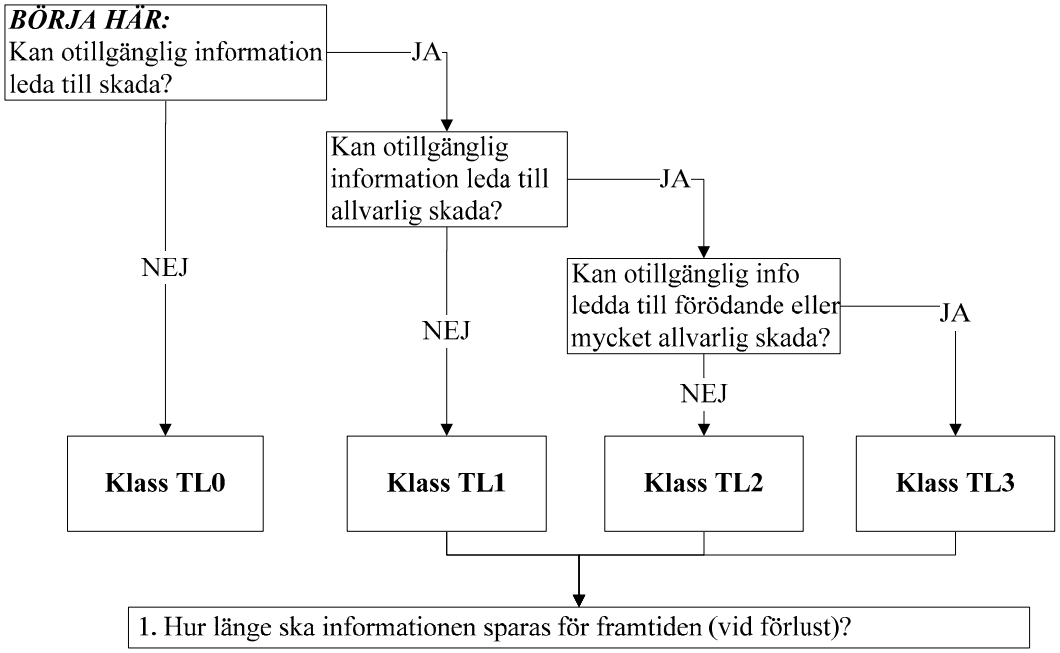
Tillgänglighet på lång sikt innebär hur viktigt det är att informationen finns tillgänglig i framtiden (”långtidsförvaring”).

För att underlätta bedömningen kan nedanstående frågor beaktas:

a) Vad innebär det om information som är en vecka, en månad, ett år, tjugo år gammal inte går att göra tillgänglig igen?
b) Förändras tillgänglighetskravet över olika återkommande perioder och över tid?

Även här måste tidsaspekterna ovan hanteras t.ex. genom krav på IT-system, säkerhetskopiering, lagring osv.

Svaren på frågorna ovan bedöms utifrån konsekvensnivåerna beskrivna på sid 4.



Beskrivning av konsekvensnivåer kopplat till informationssäkerhetsklass

Klass 3 (K3, R3, TL3 eller TK3)

Konsekvensnivå ”Förödande eller mycket allvarlig skada”

Kan förslust av konfidentialitet leda till förödande eller mycket allvarlig skada, dvs, kan det

a) innebära att SLU inte kan fullgöra en eller flera av sina primära uppgifter?
b) resultera i omfattande skador på SLU:s tillgångar?
c) resultera i stora ekonomiska förluster?
d) det förorsaka allvarligt negativ påverkan på enskild individs rättigheter eller liv och hälsa?

Om svaret är ”ja” blir informationssäkerhetsklassen K3, gå vidare till riktighet och tillgänglighet. Om svaret är ”nej”, gå vidare till nästa konsekvensnivå, dvs nästa lägre klass.

Klass 2 (K2, R2, TL2 eller TK2)

Konsekvensnivå ”Allvarlig skada”

Kan förslust av konfidentialitet leda till allvarlig skada, dvs kan det

a) innebära att SLU:s primära uppgifter kan fullföljas, men att effektiviteten är allvarligt och påtagligt reducerad
b) resultera i allvarliga skador på SLU:s tillgångar
c) resultera i allvarliga ekonomiska förluster
d) förorsaka allvarliga negativ påverkan på enskild individs rättigheter eller hälsa

Om svaret är ”ja” blir informationssäkerhetsklassen K2, gå vidare till riktighet och tillgänglighet. Om svaret är ”nej”, gå vidare till nästa konsekvensnivå.

Klass 1 (K1, R1, TL1 eller TK1)

Konsekvensnivå ”Lindrig eller besvärande skada”

Kan förslust av konfidentialitet leda till lindrig eller besvärande skada, dvs kan det

a) innebära att SLU:s primära uppgifter kan fullföljas, men att effektiviteten är påvisbart reducerad
b) resultera i mindre skador på SLU:s tillgångar
c) resultera i smärre ekonomiska förluster
d) förorsaka begränsad negativ påverkan på enskild individs rättigheter eller hälsa

Om svaret är ”ja” blir informationssäkerhetsklassen K1, gå vidare till riktighet och tillgänglighet. Om svaret är ”nej”, gå vidare till nästa konsekvensnivå.

Klass 0 (K0, R0, TL0 eller TK0)

Konsekvensnivå ”Ingen eller försumbar skada”

Kan förslust av konfidentialitet leda till ingen eller försumbar skada, dvs

a) medför inte någon eller endast försumbar negativ påverkan
b) informationen blir inte föremål för några särskilda skyddsåtgärder utifrån just denna specifika informationssäkerhetsaspekt

Om svaret är ”ja” blir informationssäkerhetsklassen K0, gå vidare till riktighet och tillgänglighet.