DNR: SÄK 2015-17
Exp. den: 2015-11-05/AL

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

STYRANDE DOKUMENT

Sakområde: Säkerhet och informationssäkerhet

Dokumenttyp: Anvisning
Beslutsfattare: Säkerhetschef P-O Skatt
Avdelning/kansli: SLU Säkerhet
Handläggare: Informationssäkerhetschef Anette Lindberg

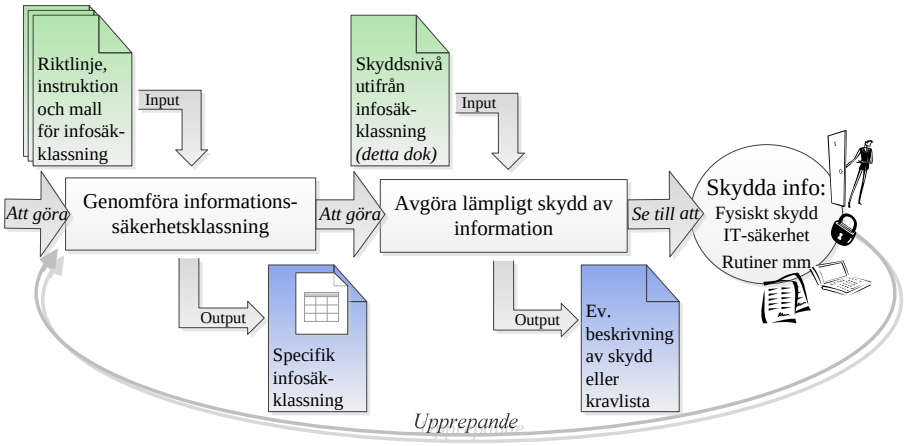
Beslutsdatum: 2015-11-05
Träder i kraft: 2015-11-05
Giltighetstid: Tills vidare
Bör uppdateras före: [Datum]

Ev dokument som upphävs: SÄK 2015-10

Bilaga till: [Dokumentnamn]

Skyddsnivå utifrån informationssäkerhetsklassning

Olika typer av information har olika informationssäkerhetsvärde för SLU utifrån kategorierna[1] konfidentialitet, riktighet och tillgänglighet. Värdet bedöms genom informationssäkerhetsklassning[2], vidare benämnd klassning. Beroende på informationens värde och därmed klassning är olika säkerhetsåtgärder lämpliga.



Figur 1. Utifrån styrande dokument (”input”) genomförs verksamhetsspecifika bedömningar (”output”), vilket ska leda till ett anpassat skydd. För att bibehålla ett bra och anpassat skydd ska processen upprepas regelbundet eller vid förändring.

[1] Konfidentialitet innebär att information inte ska avslöjas eller vara tillgänglig för obehörig.
Riktighet innebär att information inte obehörigt ändras eller modifieras, varken otillåtet, av misstag eller på grund av funktionsstörning.
Tillgänglighet innebär att information finns att tillgå ”här och nu” i förväntad utsträckning och inom önskad tid samt i framtiden, ”långtidsförvaring”.

[2] Informationssäkerhetsklassning sker genom att bedöma vilken skada/konsekvens det skulle innebära för SLU om information påverkades utifrån konfidentialitet, riktighet och tillgänglighet. Allvarligare konsekvens (från *ingen konsekvens* till *förödande skada*) ger högre klass (*klass noll* till *klass tre*).

Innehåll

Syfte och bakgrund

Syftet är att beskriva vilket skydd olika informationstyper[3] behöver för att bibehålla konfidentialitet, riktighet och eller tillgänglighet under informationens hela livscykel. Dokumentet används av t.ex. datoranvändare, informationsägare och systemägare. Kraven är ställda ur ett informationssäkerhetsperspektiv, men samma eller liknande krav kan ha sitt ursprung inom andra områden, såsom juridik, arkiv, dokumenthantering, utveckling, drift och förvaltning.

Dokumentet är en del i SLU:s ledningssystem för informationssäkerhet (LIS)[4] på strategisk/taktisk nivå, se medarbetarwebbens informationssäkerhetssidor (internt.slu.se/informationssakerhet). För den senaste utgåvan, se medarbetarwebben.

Undantag

Detta är inte en fast och exakt kravställning utan informationsägare, systemägare, verksamhetsledare, projekt eller liknande kan behöva anpassa skydd till både högre och lägre nivå utifrån speciella förutsättningar. Beslut bör dokumenteras.

All information omfattas inte av alla krav i kravlistan. Kraven varierar t.ex. om information är pappersburen eller digital, om det är original eller kopia eller om det finns motstridigheter mellan t.ex. tillgänglighet och konfidentialitet.

Information som kan komma att sekretessbeläggas utifrån Offentlighets- och sekretesslagen 15 kap 2§ hanteras i särskild ordning enligt Säkerhetskyddslagen. Kontakta SLU Säkerhet och chefsjurist.

[3] Med information avses digitalt lagrad, pappersburen och eller talad information. Typ av information kan vara artiklar, opublicerat forskningsresultat, rådata, avhandling, tentamenfrågor, examensarbete, anbud, interna rutiner, loggar, lösenord och mycket mer.

[4] Se standard SS-ISO/IEC 27001 – Ledningssystem för informationssäkerhet

Informationssäkerhetsklassning

Klassning innebär analys av *hur stor skada (konsekvens) det skulle innebära om SLU:s information inte finns tillgänglig i framtiden, om vi inte kommer åt it-system nu, om ”hemligheter” sprids eller om information förändras på ett otillbörligt sätt.*
Ju allvarligare konsekvenser desto högre klass. När klassning är genomförd, antingen centralt eller lokalt, vet man hur viktig olika informationstyper är för SLU och dess verksamheter. Hela förfaringssättet beskrivs på medarbetarwebbens informationssäkerhetssidor (internt.slu.se/informationssakerhet).

Klass 3 ”Förödande eller mycket allvarlig skada”
kan innebära att SLU inte kan fullgöra en eller flera av sina primära uppgifter,
resultera i omfattande skador på SLU:s tillgångar,
resultera i stora ekonomiska förluster eller
förorsaka allvarligt negativ påverkan på enskild individs rättigheter eller liv och hälsa

Klass 2 ”Allvarlig skada”
kan innebära att SLU:s primära uppgifter kan fullföljas, men att effektiviteten är allvarligt och påtagligt reducerad,
resultera i allvarliga skador på SLU:s tillgångar,
resultera i allvarliga ekonomiska förluster eller
förorsaka allvarliga negativ påverkan på enskild individs rättigheter eller hälsa

Klass 1 ”Lindrig eller besvärande skada”
kan innebära att SLU:s primära uppgifter kan fullföljas, men att effektiviteten är påvisbart reducerad,
resultera i mindre skador på SLU:s tillgångar,
resultera i smärre ekonomiska förluster eller
förorsaka begränsad negativ påverkan på enskild individs rättigheter eller hälsa

Klass 0 ”Ingen eller försumbar skada”
medför inte någon eller endast försumbar negativ påverkan, information blir inte föremål för några särskilda skyddsåtgärder utifrån just denna specifika informationssäkerhetsaspekt.
Observera att denna klass inte renderar i några säkerhetskrav.

Den vanligaste kombinationen av klasser är K0 R1 TK1 TL1[5], dvs att information inte är konfidentiell men det finns ett värde i att den är oförändrad och tillgänglig, både nu och i framtiden. Den nivå på skydd som uppfyller den kombinationen kallas grundnivå.

Kategori / IS-klass	Konfidentialitet (K)	Riktighet (R)	Tillgänglighet kort sikt (TK)	Tillgänglighet lång sikt (TL)
Klass 3	Ovanlig	Ovanlig	Ovanlig	Ovanlig
Klass 2	Ganska ovanlig	Ganska ovanlig	Ganska ovanlig	Ganska ovanlig
Klass 1	Ganska vanlig	Vanlig	Vanlig	Vanlig
Klass 0	Vanlig	Ovanlig	Ovanlig	Ovanlig

Figur 2. Den vanligaste kombinationen av klasser är K0 R1 TK1 TL1[5], vilket visas med feta kantlinjer.

[5] Klassning sker i kategorierna konfidentialitet, riktighet, tillgänglighet på kort sikt och tillgänglighet lång sikt. Det innebär att varje informationstyp får en kombination av kategorier och klasser, t.ex. K0 R1 TK1 TL1, vilken är den vanligaste kombinationen. ”K0" betyder ”konsekvens klass 0” osv.

Skyddsnivåer – Grundnivå och tilläggsnivå

Nivåerna för skyddet är uppdelade i *grundnivå* och *tilläggsnivå*.

- Grundnivån är den kombination av säkerhetsåtgärder som är tillräcklig för att skydda den allra vanligaste kombinationen av informationssäkerhetklasser[5].
- Tilläggsnivån består av de krav som tillkommer när information placeras i någon av de högre klasserna i konfidentialitet, riktighet eller tillgänglighet (K1, K2, K3, R2, R3, TK2, TK3, TL2 eller TL3).

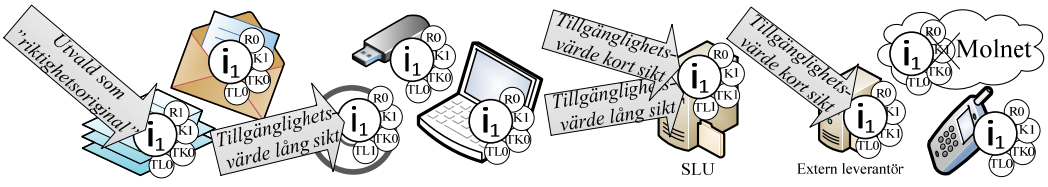
I de fall kraven på grundnivå skulle vara motstridiga kraven på tilläggsnivå har kraven på tilläggsnivån prioritet.
Observera att vid val av skydd kan skyddet behöva anpassas till både högre och lägre nivå utifrån verksamhetsspecifika aspekter. Sådant beslut bör dokumenteras.

Olika typer av information kan placeras i olika klasser. Beroende på klass så ska grundnivån och eventuellt vissa krav i tilläggsnivån uppfyllas. I exempel nedan visas att t.ex. en verksamhet hanterar fem olika typer av information. Dessa har olika värde för SLU, placeras därför i olika klasser och ska skyddas till olika nivå på olika sätt. Om all information ska skyddas på samma sätt måste det skyddas enligt den högsta nivån. Nedan visas att olika informationstyper placeras i olika klasser och därmed kräver olika skyddsnivå:

Infotyp	Infosäkklasser	Skyddsnivå
Infotyp 1	K0 R1 TK1 TL1	Grundnivå
Infotyp 2	K0 R1 TK1 TL1	Grundnivå
Infotyp 3	K0 R2 TK2 TL1	Grundnivå och Tilläggsnivå för R2 och TK2
Infotyp 4	K1 R1 TK1 TL1	Grundnivå och Tilläggsnivå för K1
Infotyp 5	*K3 R1 TK1 TL1*	*Särskild analys pga placering i klass 3*

Skydd av kopior

När krav ställs utifrån ett riktighetsperspektiv behöver inte alla informationskopior skyddas på samma sätt, utan så länge minst en utpekad informationskopia skyddas och det finns kontroll på vilken information som är den riktiga så räcker det. T.ex. måste ett originaldokument med höga riktighetskrav skickas med rekommenderad post medan en kopia kan skickas med ordinarie post om originalet eller annan kopia är säkrat.
Samma sak med tillgänglighetskrav. Om information ska finnas tillgänglig om 20 år behöver inte alla dess kopior finnas tillgängliga då. Om en databas ska finnas konstant tillgänglig behöver inte dess kopior vara tillgängliga på samma sätt.
Om däremot en informationstyp är konfidentiell så är även dess kopior det.



Figur 3. Informationstyp i_1 med klassning K1 R1 TK1 TL1 kan finnas tillgänglig på många olika ställen och därmed behöva skyddas på olika sätt.
Observera att cirkeln i figuren beskriver att skyddsbehovet är olika på olika lagringsmedia, det är inte klassningen för informationstypen som ändras.

Bilaga 1 - Sammanfattning för ”vanlig” användare

Nedan följer en sammanfattning av krav som den ”vanlige” användaren behöver förhålla sig till i de fall den hanterade information är ”normalviktig” för SLU. Kraven är en delmängd av kraven i tidigare kapitel och att betrakta som en förenkling.

Personalsäkerhet

1. Person ska ha genomgått informationssäkerhetsutbildning och förstå sitt informationssäkerhetansvar.

Hantering av tillgångar

2. **Information ska hanteras och skyddas utifrån klass. Klassning är tillsammans med riskanalys grund till informationens skyddsbehov.**
3. **Innan hantering, inklusive lagring, sker ska det säkerställas att tänkt skydd kan och får hantera valda informationstyper ur ett lag-, avtals- och lämplighetsperspektiv (personuppgifter, forskningsdata, ekonomiska uppgifter, sekretessbelagd information, ”molnet”, lagring utanför EU, synkronisering av information till olika enheter osv).**
4. Information ska hanteras så att minst två personer kan få åtkomst till den.
5. Lagringsenhet och dokumentation ska hanteras utifrån lagrad informations högsta klass, både på arbetsrummet, vid föreläsningar, under transport, vid återanvändning eller kassering osv.
6. Vid användning av lagringsmedia för information med riktighetskrav ska lagringsmedia krypteras vid extern användning.
7. Lagringsmedia ska förvaras inlåst eller under direkt uppsikt.
8. Läsbarhet av både lagringsmedia och format ska säkerställas.

Styrning av åtkomst

9. Endast behörig person ska kunna komma åt, ändra eller radera information. Gäller både digitalt lagrad, talad och pappersburen information.
10. Åtkomst till information ska begränsas, t.ex. med styrning av åtkomst, rättighetstilldelning, intrångsskydd (brandvägg) mm.
11. Person ska skydda lösenord mot obehörig åtkomst.
12. I de fall lösenord måste skrivas ner ska det förvaras inlåst.
13. Dator eller liknande, innehållande skyddsvärd information, som lämnas obevakad ska skyddas, t.ex. med lösenordsskyddad skärmsläckare, urloggning eller avstängning.

Fysisk och miljörelaterad säkerhet

14. Obevakad utrustning och information ska ha anpassat skydd, t.ex. skyddad förvaring, låst skåp eller låst rum.

Driftsäkerhet

15. Upptäckande, förebyggande och återställande skydd mot skadlig kod ska vara installerat, aktivt och uppdaterat
16. Digitalt lagrad information ska lagras på minst två digitala och två fysiska platser.
17. Säkerhetskopian ska skyddas utifrån klassning av information den innehåller.
18. Enbart behörig person ska kunna förändra information, program och eller konfiguration.

Informationssäkerhetsincidenter

19. Rapportering och hantering av informationssäkerhetsincidenter och svagheter ska ske.

Bilaga 2 - Grundnivå

Nedan listade krav ingår i grundnivån, dvs den skyddsnivå som på ett tillräcklig sätt skyddar en stor del av SLU:s informationstyper. Tilläggsnivån redovisas från sid 10 och framåt.
All information omfattas inte av alla krav. Pappersburen och digital information måste skyddas på olika sätt, där pappersburen information kan skyddas genom att låsa in den så att obehörig inte kommer åt den, ha kopior där så krävs samt skicka och destruera på korrekt sätt, medan skydd av digital information kan omfattas av dessa men också av många andra krav.
Det kan förekomma motstridigheter mellan t.ex. tillgänglighets- och konfidentialitetskrav.

Personalsäkerhet

Person ska ha genomgått informationssäkerhetsutbildning och förstå sitt informationssäkerhetansvar.

Hantering av tillgångar

Information ska hanteras och skyddas utifrån klass. Klassning är tillsammans med riskanalys grund till informationens skyddsbehov.

Innan hantering, inklusive lagring, sker ska det säkerställas att tänkt skydd kan och får hantera valda informationstyper ur ett lag-, avtals- och lämplighetsperspektiv (personuppgifter, forskningsdata, ekonomiska uppgifter, sekretessbelagd information, ”molnet”, lagring utanför EU, synkronisering av information till olika enheter osv).

Information ska hanteras så att minst två personer kan få åtkomst till den.
Lagringsenhet[6] och dokumentation ska hanteras utifrån lagrad informations högsta klass, både på arbetsrummet, vid föreläsningar, under transport, vid återanvändning eller kassering osv.
Vid användning av lagringsmedia för information med riktighetskrav ska lagringsmedia krypteras vid extern användning.
Lagringsmedia ska förvaras inlåst eller under direkt uppsikt.
Läsbarhet av både lagringsmedia och format ska säkerställas.

Styrning av åtkomst

Endast behörig person ska kunna komma åt, ändra eller radera information. Gäller både digitalt lagrad, talad och pappersburen information.
Åtkomst till information ska begränsas, t.ex. med styrning av åtkomst, rättighetstilldelning, intrångsskydd (brandvägg) mm.

Användaridentitet ska vara unik, individuell och kunna spåras till fysisk person.
Autentisering (säkerställande av identitet) ska ske med minst lösenord.
Person ska skydda lösenord mot obehörig åtkomst.

[6] USB-minne, hårddisk, minneskort, smartphone, surfplatta, skrivare och liknande

Lösenord[7] ska vara konstruerat utifrån värdet på information det skyddar och det ska inte överföras eller lagras i klartext.
Lösenordsbyten ska ske regelbundet eller på initiativ av användare eller systemadministratör.
I de fall lösenord måste skrivas ner ska det förvaras inlåst.
Lösenord som är tillgängligt för flera personer ska undvikas i möjligaste mån, men i de fall de används ska de hållas i säkert förvar enligt särskilda rutiner.
Vid upprepade felaktiga autentiseringsförsök ska automatiska åtgärder vidtas, såsom nekad behörighet och automatisk utelåsning.

Tilldelning och förändring av vanlig och priviligierad åtkomst ska ske utifrån persons behov samt informationens klassning.
Privilegierade åtkomsträttigheter ska begränsas, styras, ej vara möjliga att tilldela sig själv samt kontrolleras.
Skilda roller för loggadministration, daglig drift och tilldelning av åtkomsträttigheter ska finnas.
Användande av roll med mycket stor åtkomst i system ska undvikas.

Åtkomsträttighet ska återkallas när åtkomst inte längre behövs.
Återkallning kan ske med tidsbegränsad åtkomsttilldelning, via identitetshanteringssystem eller manuell hantering.
Användarkonton och åtkomsträttigheter ska granskas regelbundet.

Dator eller liknande, innehållande skyddsvärd information, som lämnas obevakad ska skyddas, t.ex. med lösenordsskyddad skärmsläckare, urloggning eller avstängning.

Kryptering

När kryptering används ska funktionen vara avsedd för specifik klass, kryptonyckel ska skyddas och det ska säkerställas att information går att återställa av fler än en person alternativt finnas tillgänglig i okrypterad form.

Fysisk och miljörelaterad säkerhet

Det ska finnas fysiska avgränsningar och passerkontroll som förhindrar intrång, otillåten användning, stöld, brand och annan skada.
Obevakad utrustning och information ska ha anpassat skydd, t.ex. skyddad förvaring, låst skåp eller låst rum.
Elavbrott ska motverkas och kablar för el och kommunikation ska ha ett anpassat skydd mot avlyssning, störning och skada.

[7] Myndigheten för samhällsskydd och beredskap anser att ett starkt lösenord består av siffror, specialtecken, stora och små bokstäver och är minst 12 tecken långt.

Driftsäkerhet

Information ska vara åtkomlig under ordinarie arbetstid utan större störningar.
Avbrott ska normalt inte vara längre än fyra timmar, men kan vara under veckor vid mycket allvarliga händelser.
Återställning av system kan dröja flera veckor vid mycket allvarlig händelse.

Det ska finnas aktuell dokumentation gällande t.ex. behörighetshantering, teknisk drift, kapacitetskrav, användarstöd, supportavtal och överenskommelser.

Skydd mot skadlig kod

Upptäckande, förebyggande och återställande skydd mot skadlig kod ska vara installerat, aktivt och uppdaterat

Säkerhetskopiering och återställning

Förlorad information får inte vara äldre än 24 timmar, dvs säkerhetskopiering ska ske minst var 24:e timme.
Den ska kunna återskapas inom sju till fjorton dagar.
Information som förändrats eller förstörts ska kunna återskapas efter ett år.

Säkerhetskopiering ska utföras och testas regelbundet.
Digitalt lagrad information ska lagras på minst två digitala och två fysiska platser.
Säkerhetskopian ska skyddas utifrån klassning av information den innehåller.
Återstarts- och återställningsrutiner ska finnas.
Vid återläsning/återställning från säkerhetskopior ska dessa kontrolleras så att inte problem som förorsakade återläsningen återläses.

Spårbarhet, övervakning och larmning

Säkerhetsrelevanta händelser[8] i IT-system ska registreras tillsammans med datum, tid, identitet.
Logg ska skyddas, sparas och analyseras regelbundet eller vid behov.
Automatiska analyser av loggen ska vara möjlig
Vid fel på loggfunktionen ska behörig administratör få meddelande.
Övervakning av IT-system ska ske, t.ex. avseende drifttillståndsförändringar, strömbortfall, varningar, larm eller andra specificerade händelser

Tekniska sårbarheter

Säkerhets- och programvaruuppdateringar ska analyseras och vid behov införas.

Riktighet[9]

Enbart behörig person ska kunna förändra information, program och eller konfiguration.

[8] Exempelvis lyckad och misslyckad inloggning, förändring av åtkomsträttighet, start och stopp av loggfunktion, användning av högre rättighet, förändring av funktion för åtkomst.
[9] Riktighetskontroll kan ske på olika sätt, t.ex. genom behörighetskontroll, kryptografisk mekanism, digitala signaturer, manuella signaturer, manuell kontroll av behörig person, separering av arbetsuppgifter, rimlighet i mängd av inkommande och utgående data, kontrollsumma, formatkontroll. Verifiering kan ske t.ex. mot installationsmedia, originalinformation eller liknande.

Kommunikationssäkerhet

Information ska skyddas mot manipulation vid både extern och intern kommunikation.
Sammankoppling med andra nätverk får ske endast efter att nödvändiga säkerhetsåtgärder vidtagits.
Intrångsskydd ska förhindra obehörig åtkomst till IT-system och det ska kontrollera både inkommande och utgående informationsflöde.

Anskaffning, utveckling, test, underhåll, förvaltning och avveckling av system

Informationssäkerhet ska vara en integrerad del över hela livscykeln, även vid återanvändning och återvinning. Klassning och riskanalys är grunden för val av säkerhetsskydd.

IT-system inklusive säkerhetsfunktioner ska vara stabilt och väl testat och det ska finnas aktuell systemdokumentation.

Utvecklings- och testsystem ska vara separerade från driftsatt system för att minska risken för driftstörning eller informationssäkerhetsincident.
Säkerhetskraven gäller till stor del även utvecklings- och testmiljöerna, beroende på vilken information som används vid respektive tillfälle i respektive system.

Leverantörsrelationer

Relevanta informationssäkerhetskrav ska avtalas med leverantör och dessa ska revideras och kontrolleras efter behov.

Det ska tecknas avtal gällande leverantörens tillgång till och användning av SLU:s information. Även ansvar och roller för leverantör och SLU, eventuella revisionsrättigheter, hantering av eventuella personuppgifter ska regleras.

Informationssäkerhetsincidenter

Rapportering och hantering av informationssäkerhetsincidenter och svagheter ska ske.

Kontinuitetsplanering

Kontinuitetsplanering ska utföras, dokumenteras och utvärderas för att säkerställa den nivå av kontinuitet som krävs vid en svår situation.
Planen ska beröra vad utebliven eller bristande tillgänglighet till kritisk information innebär, kritiska återstartstider, lösningar och aktiviteter, reservrutiner, roller och ansvar.

Bilaga 3 - Tilläggsnivå (inklusive grundnivå)

Nedan visas en sammanställning över krav på både grundnivå och tilläggsnivå. Ofta räcker det att uppfylla kraven på grundnivån (för information klassad K0 R1 TK1 TL1). Ibland visar dock klassning (klasserna K1, K2, K3, R2, R3, TK2, TK3, TL2 eller TL3) att även kraven i någon eller några av kategorierna på tilläggsnivå behöver uppfyllas. Klass 0 redovisas inte eftersom det är en kravlös klass.

Kryssen visar vilka krav som ska uppfyllas för respektive klass. Det kan underlätta att titta på en kategori (K, R, TK och TL) i taget. Det finns krav som ska uppfyllas oberoende av vilken klass informationstypen placerats i (t.ex. krav pe1 som har kryss i alla rutor) och det finns krav som endast behöver uppfyllas i en eller ett fåtal klasser (t.ex. pe3 som endast tre av 12 klasser behöver uppfylla). Observera att inte alla kryss måste stämma överens i alla fyra kategorier för att kravet ska uppfyllas. T.ex. behöver inte informationstypens klassning vara K3 R3 TK3 TL3 för att krav pe3 ska uppfyllas, utan det räcker med en klass 3 i någon av kategorierna, tex K3 R1 TK1 TL1.

All information omfattas inte av alla krav. Pappersburen och digital information måste skyddas på olika sätt, där pappersburen information skyddas genom att låsa in den så att obehörig inte kommer åt den, ha kopior där så krävs samt skicka och destruera på korrekt sätt, medan skydd av digital information kan omfattas av dessa men också av många andra krav. Dessutom kan det förekomma motstridigheter mellan t.ex. tillgänglighet och konfidentialitet. Alla kopior behöver inte skyddas på samma sätt utifrån riktighets- och tillgänglighetsaspekterna. Däremot måste konfidentiell information och dess kopior skyddas så att ingen obehörig kan ta del av den, se på sid 4.

Observera återigen att skyddsnivån kan behöva anpassas till både högre och lägre nivå utifrån speciella förutsättningar. Sådana beslut bör dokumenteras.

Säkerhetskrav / **Klass**[10]	**K1**	**K2**	**K3**	**R1**	**R2**	**R3**	**TK1**	**TK2**	**TK3**	**TL1**	**TL2**	**TL3**
Personalsäkerhet												
pe1 Person ska förståelse för informationssäkerhet och för sitt ansvar gällande informationssäkerhet.	x	x	x	x	x	x	x	x	x	x	x	x
pe2 Person ska genomgå informationssäkerhetsutbildning.	x	x	x	x	x	x	x	x	x	x	x	x
pe3 Person ska genomgå särskild och återkommande informationssäkerhetsutbildning			x			x			x			x
pe4 Bakgrundskontroll ska genomföras.		x	x		x	x		x	x		x	x
pe5 Person ska underteckna ansvarsförbindelse.		x	x		x	x		x	x		x	x
Hantering av tillgångar												
ha1 Klassning ska genomföras och den är tillsammans med riskanalys grund till informationens skyddsbehov	x	x	x	x	x	x	x	x	x	x	x	x

[10] Klass 0 innebär *ingen eller försumbar skada*, klass 1 *lindrig eller besvärande skada*, klass 2 *allvarlig skada* och klass 3 *förödande eller mycket allvarlig skada* för SLU.

Säkerhetskrav / Klass[10]	K1	K2	K3	R1	R2	R3	TK1	TK2	TK3	TL1	TL2	TL3
ha2 Innan hantering, inklusive lagring, sker ska det säkerställas att tänkt skydd kan och får hantera valda informationstyper ur ett lag-, avtals- och lämplighetsperspektiv (överväg personuppgifter, forskningsdata, ekonomiska uppgifter, sekretessbelagd information, ”molnet”, lagring utanför EU, synkronisering av information till olika enheter osv)	x	x	x	x	x	x	x	x	x	x	x	x
ha3 Information ska hanteras så att minst två personer kan få åtkomst åt den.							x	x	x	x	x	x
ha4 Dokumentation och lagringsenheter (tex USB-minne, hårddisk, minneskort smartphone, läsplatta, skrivare och liknande) ska hanteras utifrån lagrad informations högsta klass, både på arbetsrum, vid föreläsning, under transport, vid återanvändning eller kassering osv.	x	x	x	x	x	x	x	x	x	x	x	x
ha5 Vid extern användning av extern lagringsenhet ska information krypteras.	x	x	x	x	x	x						
ha6 Lagringsmedia med konfidentiell eller originalinformation ska hållas under direkt uppsikt eller förvaras inlåst i skåp eller på arbetsrum.	x	x	x	x	x	x						
ha7 Läsbarhet av både lagringsmedia och format ska säkerställas.							x	x	x	x	x	x
ha8 Särskilda separerade skrivare ska användas för utskrift		x	x									
ha9 Kopiering är endast tillåten efter godkännande av informationsägare	x	x	x									
ha10 Information ska skickas i dubbla förslutna kuvert internt och med rekommenderad post externt. Försändelse till utlandet ska bedömas från fall till fall.	x	x			x			x			x	
ha11 Speciella sändebud ska användas vid försändelse, efter speciellt tillstånd av informationsägare		x	x		x	x		x	x		x	x
ha12 Vid förstöring av papper ska papperstugg eller kontrollerad bränning användas. Vid förstöring av digitalt lagringsmedia ska överskrivning eller mekanisk förstöring användas.	x	x	x									
ha13 Sekretessbelagd information ska hanteras i särskild ordning. Sekretessbelagd information utifrån OSL 15 kap 2§ meddelas till SLU Säkerhet och chefsjurist och hanteras enligt säkerhetsskyddslagen.	x	x	x									
Styrning av åtkomst												
åt1 Endast behörig person ska kunna komma åt, ändra eller radera information. Gäller digital, talad och pappersburen information. Informationsägare, verksamhetsledare eller liknande fattar beslut om behörighet.	x	x	x	x	x	x	x	x	x	x	x	x
åt2 Åtkomst till information ska begränsas, t.ex. med styrning av åtkomst, rättighetstilldelning, intrångsskydd (brandvägg) mm.	x	x	x	x	x	x	x	x	x	x	x	x
åt3 Användaridentitet ska vara unik och individuell. Utifrån spårbarhetsaspekt ska inte användaridentiteten återanvändas av annan person och inte heller raderas. Användarkonton ska vara spårbara till fysisk person.	x	x	x	x	x	x	x	x	x	x	x	x
åt4 Förinställda eller onödiga användarkonton ska blockeras eller förses med nytt lösenord		x	x		x	x		x	x		x	x

Säkerhetskrav / Klass[10]	K1	K2	K3	R1	R2	R3	TK1	TK2	TK3	TL1	TL2	TL3
åt5 Autentisering (säkerställande av identitet) ska ske vid inloggning till skyddsvärd information och det ska ske med minst lösenord. Person ska skydda lösenordet mot obehörig åtkomst.	x	x	x	x	x	x	x	x	x	x	x	x
åt6 Stark autentisering t.ex. två-faktorsautentisering ska användas.		x	x		x	x		x	x		x	x
åt7 Lösenord ska vara konstruerat utifrån värdet på information det skyddar (*MSB: ett starkt lösenord består av siffror, specialtecken, stora och små bokstäver och är minst 12 tecken långt*), lösenordsbyten ska ske regelbundet eller på initiativ av användare eller systemadministratör.	x	x	x	x	x	x	x	x	x	x	x	x
åt8 Lösenord ska ej överförs eller lagras i klartext	x	x	x	x	x	x	x	x	x	x	x	x
åt9 I de fall lösenord måste skrivas ner ska det förvaras inlåst	x	x	x	x	x	x	x	x	x	x	x	x
åt10 Lösenord som är tillgängligt för flera personer ska undvikas i möjligaste mån, men i de fall de används ska de hållas i säkert förvar enligt särskilda rutiner	x	x	x	x	x	x	x	x	x	x	x	x
åt11 Vid upprepade felaktiga autentiseringsförsök ska automatiska åtgärder vidtas, såsom nekad behörighet och automatisk utelåsning	x	x	x	x	x	x	x	x	x	x	x	x
åt12 Session ska brytas vid låsning eller spärrning av autentiseringsfunktion om riktighet och tillgänglighet så tillåter.		x	x		x	x		x	x		x	x
åt13 System ska meddela behörig administratör vid upprepande felaktiga autentiseringsförsök		x	x		x	x		x	x		x	x
åt14 Tilldelning och förändring av vanlig och priviligierad åtkomst ska ske utifrån persons behov samt informationens klassning	x	x	x	x	x	x	x	x	x	x	x	x
åt15 Privilegierad åtkomsträttighet ska begränsas, styras, ej vara möjliga att tilldela sig själv samt kontrolleras.	x	x	x	x	x	x	x	x	x	x	x	x
åt16 Skilda roller för loggadministration, daglig drift och tilldelning av åtkomsträttigheter ska finnas. Användande av roll med mycket stor åtkomst i system ska undvikas.	x	x	x	x	x	x	x	x	x	x	x	x
åt17 Identitetsadministration samt tilldelning av åtkomstsrättigheter ska inte utföras av samma person.		x	x		x	x		x	x		x	x
åt18 Åtkomsträttighet ska återkallas när åtkomst inte längre behövs. Återkallning kan ske med tidsbegränsad åtkomsttilldelning, via identitetshanteringssystem eller manuell hantering.	x	x	x	x	x	x	x	x	x	x	x	x
åt19 Användarkonton och åtkomsträttigheter ska granskas regelbundet	x	x	x	x	x	x	x	x	x	x	x	x
åt20 Dator eller liknande, innehållande skyddsvärd information, som lämnas obevakad ska skyddas, t.ex. med lösenordsskyddad skärmsläckare, urloggning eller avstängning.	x	x	x	x	x	x	x	x	x	x	x	x
åt21 Nedkoppling vid inaktivitet, begränsad uppkopplingstid, speciell lösning för fjärråtkomst ska ske.		x	x		x	x		x	x		x	x
åt22 Om obehörig har tagit del av information ska detta anmälas till verksamhetschef, säkerhetschef och vid sekretessbelagd information även chefsjurist		x	x									

Säkerhetskrav / Klass[10]	K1	K2	K3	R1	R2	R3	TK1	TK2	TK3	TL1	TL2	TL3
Kryptering												
kr1 När kryptering används ska den vara avsedd för specifik informationssäkerhetsklass	x	x	x	x	x	x						
kr2 Kryptonyckelhantering och skydd av kryptonyckel måste ske så att inte information röjs eller riktighet påverkas	x	x	x	x	x	x						
kr3 När kryptering används ska det säkerställas att information går att återställa av fler än en person alternativt finnas i okrypterad form							x	x	x	x	x	x
Fysisk och miljörelaterad säkerhet												
fy1 Det ska finnas fysiska avgränsningar och passerkontroll som förhindrar intrång, otillåten användning, stöld, brand och annan skada.	x	x	x	x	x	x	x	x	x	x	x	x
fy2 Obevakad utrustning och information ska ha anpassat skydd, t.ex. skyddad förvaring, låst skåp eller låst rum.	x	x	x	x	x	x	x	x	x	x	x	x
fy3 Elavbrott ska motverkas				x	x	x	x	x	x			
fy4 Kablar för elförsörjning och kommunikation ska ha anpassat skydd mot avlyssning, störning och skada	x	x	x	x	x	x	x	x	x			
Driftsäkerhet												
dr1 Information ska vara åtkomlig under ordinarie arbetstid utan större störningar. Avbrott ska normalt inte vara längre än fyra timmar, men kan vara under veckor vid mycket allvarliga händelser. Återställning av system kan dröja flera veckor vid mycket allvarlig händelse.							x					
dr2 Information ska vara åtkomlig dygnet runt utan större störningar. Avbrott ska normalt inte vara längre än en timme, men kan vara upp till ett dygn vid mycket allvarliga händelser. Återställning av system kan dröja ett dygn vid mycket allvarlig händelse.								x				
dr3 Information ska vara åtkomlig dygnet runt med endast mindre störningar Avbrott ska normalt inte vara längre än några minuter, inte ens vid mycket allvarliga händelser. Återställning av system ska ske direkt även vid mycket allvarlig händelse.									x			
dr4 Det ska vara redundanta system med funktion för automatisk failover på geografiskt åtskilda platser, även försörjningssystem och kommunikationsmöjligheter.									x			
dr5 Det ska finnas aktuell dokumentation gällande t.ex. behörighetshantering, teknisk drift, kapacitetskrav, användarstöd, supportavtal och överenskommelser. Vid behov ska driftjournal föras där förändringar och händelser som påverkar driftsituationen noteras.	x	x	x	x	x	x	x	x	x	x	x	x

Säkerhetskrav / Klass[10]		K1	K2	K3	R1	R2	R3	TK1	TK2	TK3	TL1	TL2	TL3
dr6	Uppdelning av arbetsmoment (dualitet) görs där behov finns för att minska risk för misstag eller avsiktligt missbruk.		x	x		x	x		x	x		x	x
dr7	Onödiga tjänster, protokoll och programvaror ska tas bort eller inaktiveras.		x	x		x	x		x	x		x	x
Skydd mot skadlig kod													
ssk1	Upptäckande, förebyggande och återställande skydd mot skadlig kod ska vara installerat, aktivt och uppdaterat	x	x	x	x	x	x	x	x	x	x	x	x
Säkerhetskopiering och återställning													
sk1	*Förlorad information får inte vara äldre än 24 timmar (dvs säkerhetskopiering ska ske minst var 24:e timme), den ska kunna återskapas inom sju till fjorton dagar och information som förändrats eller förstörts ska kunna återskapas efter ett år*							x					
sk2	*Förlorad information får inte vara äldre än 8 timmar (dvs säkerhetskopiering ska ske minst var 8:e timme), den ska kunna återskapas inom en till sju dagar. Information som förändrats eller förstörts ska kunna återskapas efter ett år*								x				
sk3	*Förlorad information får inte vara äldre än 4 timmar (dvs säkerhetskopiering ska ske minst var 4:e timme), den ska kunna återskapas inom 24 timmar och information som förändrats eller förstörts ska kunna återskapas efter ett år*									x			
sk4	Säkerhetskopiering ska utföras och testas regelbundet				x	x	x	x	x	x	x	x	x
sk5	Digital information ska lagras på minst två digitala och två fysiska platser.				x	x	x	x	x	x	x	x	x
sk6	Säkerhetskopian ska skyddas på samma sätt som den information den innehåller	x	x	x	x	x	x	x	x	x	x	x	x
sk7	Återstarts- och återställningsrutiner ska finnas.				x	x	x	x	x	x	x	x	x
sk8	Vid återläsning/återställning från säkerhetskopior ska dessa kontrolleras så att inte problem som förorsakade återläsningen återläses				x	x	x						
Spårbarhet, övervakning och larmning													
sp1	Säkerhetsrelevanta händelser (t.ex. förändringar av åtkomsträttigheter, förändringar av funktion för åtkomst, start och stopp av loggfunktion, användning av högre rättigheter, lyckade och misslyckade inloggningar) i IT-system ska registreras tillsammans med datum, tid, identitet.	x	x	x	x	x	x	x	x	x	x	x	x
sp2	Åtkomst till, förändring, radering, export av information inklusive utskrift från system ska loggas		x	x		x	x		x	x		x	x
sp3	Konfigurationsförändringar i system ska loggas		x	x		x	x		x	x		x	x
sp4	Loggen ska skyddas, sparas och analyseras regelbundet eller vid behov.	x	x	x	x	x	x	x	x	x	x	x	x
sp5	Loggen får inte raderas eller skrivas över till följd av fel eller manipulation förrän den är sparad		x	x		x	x		x	x		x	x

Säkerhetskrav / Klass[10]	K1	K2	K3	R1	R2	R3	TK1	TK2	TK3	TL1	TL2	TL3
sp6 Loggarna från system ska sparas på central plats och de ska analyseras minst månadsvis.		x	x		x	x		x	x		x	x
sp7 Automatiska analyser av loggen ska vara möjlig				x	x	x	x	x	x	x	x	x
sp8 Loggningsfunktionen ska meddela behörig administratör vid t.ex. fel på loggning, vid för stor fyllnadsgrad i logg, kommunikationsproblem inom loggning eller om loggen skrivs över.	x	x	x	x	x	x	x	x	x	x	x	x
sp9 Loggning övervakas och automatisk omstart sker vid fel. Alternativt försätts system i säkert tillstånd om riktighet och tillgänglighet så tillåter.			x			x			x			x
sp10 Övervakning av it-system ska ske, t.ex. avseende drifttillståndsförändringar, strömbortfall, varningar, larm eller andra specificerade händelser		x	x	x	x	x	x	x	x		x	x
sp11 Det ska vara gemensam och kontrollerad tid i system för att säkerställa t.ex. loggfunktion.					x	x		x	x		x	x
Tekniska sårbarheter												
så1 Säkerhets- och programvaruuppdateringar ska analyseras och vid behov införas.	x	x	x	x	x	x	x	x	x	x	x	x
så2 Systemförändringar ska ske i mycket kontrollerad ordning		x	x		x	x		x	x		x	x
Riktighet												
ri1 Enbart behörig ska kunna förändra information, program och eller konfigurationer med riktighetskrav.				x	x	x						
ri2 Riktighetskontroll ska ske med minst två kontrollfunktioner. Det kan vara kryptografisk mekanism, digital signatur, manuell signatur, manuell kontroll utförd av behörig person, separation of duties (dualitet, minst två personer måste samverka), rimlighet i mängd av inkommande och utgående data, kontrollsumma, formatkontroll. Verifikation kan ske t.ex. mot installationsmedia, originalinformation eller liknande.					x	x						
ri3 Kontroll av riktighet ska ske med minst två kontrollfunktioner vid varje förändring av information eller med intervall som analys av riktighetsvärdet visar.						x						
Kommunikationssäkerhet												
ko1 Information ska skyddas mot manipulation vid både extern och intern kommunikation				x	x	x						
ko2 Sammankoppling med andra nätverk får ske endast efter att nödvändiga säkerhetsåtgärder vidtagits.	x	x	x	x	x	x	x	x	x	x	x	x
ko3 Konfidentiell information ska skyddas mot obehörig insyn vid både extern och intern kommunikation.	x	x	x									
ko4 Intrångsskydd ska förhindra obehörig åtkomst till IT-system och det ska kontrollera både inkommande och utgående informationsflöde	x	x	x	x	x	x	x	x	x	x	x	x
ko5 Information ska sändas och lagras krypterad efter särskild krypteringsutredning.		x	x		x	x						

Säkerhetskrav / Klass[10]	K1	K2	K3	R1	R2	R3	TK1	TK2	TK3	TL1	TL2	TL3
Anskaffning, utveckling, test, underhåll, förvaltning och avveckling av system												
an1 Informationssäkerhet ska vara en integrerad del av it-system över hela livscykeln, även vid återanvändning och återvinning. Klassning och riskanalys är grunden för val av säkerhetsskydd.	x	x	x	x	x	x	x	x	x	x	x	x
an2 It-system inklusive säkerhetsfunktioner ska vara stabilt och väl testat och det ska finnas aktuell dokumentation som beskriver systemet.	x	x	x	x	x	x	x	x	x	x	x	x
an3 Utvecklings- och testsystem ska vara separerade från driftsatt system för att minska risken för driftstörning eller informationssäkerhetincident. Säkerhetskraven gäller till stor del även utvecklings- och testsystem, beroende på vilken information som används vid respektive tillfälle i respektive system.	x	x	x	x	x	x	x	x	x	x	x	x
an4 Data ska skyddas. Vid test och utveckling kan anpassad data behöva användas.	x	x	x									
Leverantörsrelationer												
le1 Relevanta informationssäkerhetskrav ska avtalas med leverantör och dessa ska revideras och kontrolleras efter behov.	x	x	x	x	x	x	x	x	x	x	x	x
le2 Det ska tecknas avtal gällande leverantörens tillgång till och användning av SLU:s information. Även ansvar och roller för leverantör och SLU, eventuella revisionsrättigheter, hantering av eventuella personuppgifter ska regleras	x	x	x	x	x	x	x	x	x	x	x	x
Informationssäkerhetsincidenter												
in1 Rapportering och hantering av informationssäkerhetsincidenter och svagheter ska ske.	x	x	x	x	x	x	x	x	x	x	x	x
Kontinuitetsplanering												
kon1 Kontinuitetsplanering ska utföras, dokumenteras och utvärderas för att säkerställa den nivå av kontinuitet som krävs vid en svår situation. Planen ska beröra vad utebliven eller bristande tillgänglighet till kritisk information innebär, kritiska återstartstider, lösningar och aktiviteter, reservrutiner, roller och ansvar.							x	x	x	x	x	x
Övrigt												
ö1 I de fall information placeras i någon av de allra högsta klasserna (K3, R3, TK3 eller TL3) ska särskild analys av lämpligt skydd genomföras (kan vara separerade nät, kontrollerade systemförändringar, kontroll av varje förändring, aktiv verifiering av processer, larm, kontrollsummor, krypterad information, säkerhetsgodkända värdeskåp, tillstånd, särskild destruktion, säkerhetsprövningar mm). SLU Säkerhet, IT-avdelningen och eller chefsjuristen ska rådfrågas.			x			x			x			x