Regiondirektören

BESLUT

Alf Jönsson
alf.jonsson@skane.se

Datum: 2018-08-27 (2020-06-02)
Dnr: 1800025

Instruktion för informationsklassificering

Syftet är att beskriva hur Region Skånes information ska klassificeras med målet att information hanteras på rätt sätt och får rätt skydd.
Instruktionen fastställer också vilka skalor och metoder som ska användas vid klassificering av information.

Härmed beslutas att

- Instruktion för informationsklassificering fastställs
- Informationssäkerhetschef har uppdraget att underhålla instruktionen och genomföra ändringar som endast innebär liten påverkan samt har uppdrag att löpande underhålla tillhörande anvisning ”Klassificera informationstillgångar”.

Alf Jönsson

Koncernkontoret
Området för säkerhet och intern miljöledning

Johan Reuterhäll
Informationssäkerhetschef
johan.reuterhall@skane.se

INSTRUKTION

Datum: 2020-06-02
Dnr: 1800025

Informationsklassificering

Syftet är att beskriva hur Region Skånes information ska klassificeras med målet att information hanteras på rätt sätt och får rätt skydd.
Instruktionen fastställer också vilka skalor och metoder som ska användas vid klassificering av information.

Till instruktionen hör anvisning ”Klassificera informationstillgångar” som ska följas vid genomförande.

Revisionshistorik

Datum	Ändring	Ansvarig
2020-06-02	Ny lagstiftning samt uppdatering av rollers benämningar	Johan Reuterhäll

Innehållsförteckning

1 Bakgrund

Informationsklassificering är en grundläggande aktivitet inom informationssäkerhetsarbetet. Informationsklassificering innebär att information klassificeras utifrån det värde den har för de verksamheter/processer som använder informationen samt de legala krav som informationen omfattas av. Informationsklassificering är en analys av vad konsekvenserna kan bli om informationen inte längre är konfidentiell, riktig eller tillgänglig.

Instruktionen ska användas för att genomföra den informationsklassificering som Regionstyrelsen beslutat om enligt ”Riktlinjer för informationssäkerhet”.

2 Syfte

Syftet med instruktionen är att beskriva hur information ska identifieras och klassificeras. Instruktionen fastställer vilka skalor och metoder som ska användas. För det praktiska genomförandet finns anvisning ”Klassificera informationstillgångar” som ska följas.

3 Mål

Målet är att Region Skånes informationstillgångar ska ges en lämplig skyddsnivå så att:

- informationen finns tillgänglig när den behövs (tillgänglighet)
- informationen är korrekt (riktighet)
- obehöriga inte får tillgång till informationen (konfidentialitet)

4 Omfattning

Instruktionen omfattar klassificering av information oavsett om informationen behandlas manuellt (analog form) eller automatiserat (digital form) och oberoende av vilken miljö informationen förekommer.

4.1 Avgränsning

Information som faller under Säkerhetsskyddslagen (SFS 2018:585) ska behandlas separat eftersom krav på hantering och utrustning ställer särskilda krav på skydd. Om information som omfattas av Säkerhetsskyddslagen identifieras vid informationsklassificering ska denna särskiljas och behandlas separat. Säkerhetsskyddschef eller informationssäkerhetschef ska i dessa fall kontaktas för vidare instruktioner. Denna typ av information är ytterst begränsad och kan röra viss information från Försvarsmakten samt exempelvis information om kritisk infrastruktur, styrsystem och säkerhetskänsliga ritningar.

5 Berörda roller

Informationsägare	Informationsägaren har ansvar för informationstillgångar och beslutar om informationshantering inom ramen för befintlig lagstiftning och interna regelverk.
Verksamhetschef	Ansvarar för den information som hanteras inom den egna verksamheten.
Verksamhetsansvarig	Avser rollen verksamhetsansvarig enligt *Verksamhetsstyrd styr- och förvaltningsmodell för IT och MT-system*.
Systemansvarig	Avser rollen systemansvarig enligt *Verksamhetsstyrd styr- och förvaltningsmodell för IT och MT-system*. Systemansvarig har huvudansvaret för att systemet uppfyller de krav som informationsägaren ställer.
Informations- och dataskyddssamordnare	Bistår med processtöd och rådgivning vid informationssäkerhetsklassificering.
Projektledare och förstudieledare	Ansvarar för att nödvändiga aktiviteter genomförs i projektet för att kraven på informationshanteringen ska tillgodoses.
Inköpsansvariga	Ansvarar för att inköpsprocessen innehåller nödvändiga aktiviteter för att omhänderta resultatet från informationsklassificeringen.

6 Ansvar för genomförande

Verksamhetschefens ansvar
Ansvaret för informationen i verksamheten följer med det delegerade verksamhetsansvaret. Verksamhetschef ansvarar för att:

- information i verksamheten skyddas i enlighet med lagkrav och interna krav
- identifiera och förteckna viktiga informationstillgångar
- identifierade informationstillgångar i den egna verksamheten klassificeras

Informationsägares ansvar
Informationsägare ansvarar för att information som denne ansvarar för är klassificerad och ges rätt skydd så att interna och legala krav på konfidentialitet, riktighet och tillgänglighet kan upprätthållas.

Systemägares ansvar
Systemägare ansvarar för IT-system. Utifrån informationsägares krav på skydd är det systemägarens ansvar att tillse att adekvata skydd finns.

7 Förteckning över viktiga informationstillgångar

Viktiga informationstillgångar ska identifieras och förtecknas. Med informationstillgång avses den information som verksamheten behöver för att utföra sina arbetsuppgifter samt den programvara, system, datorer och utrustning som krävs för hantering av informationen.

7.1 Viktiga informationstillgångar

Med viktiga informationstillgångar avses sådana som stödjer de delar av verksamheten som är samhällsviktiga eller verksamhetskritiska.

Samhällsviktiga informationstillgångar
Begreppet samhällsviktig definieras i MSB:s föreskrifter och allmänna råd om risk- och sårbarhetsanalyser[1] som en verksamhet som uppfyller minst ett av följande villkor:

1. Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
2. Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

Verksamhetskritiska informationstillgångar
Med begreppet verksamhetskritisk menas att systemet och den information systemet behandlar, helt eller delvis, är en förutsättning för verksamheten och kan vid ett bortfall eller en svår störning ensamt eller tillsammans med motsvarande händelser i andra system på kort sikt leda till att verksamheten inte kan bedrivas.

8 Genomförande

Informationsklassificering ska genomföras:

- när informationstillgång ska upphandlas
- när befintlig informationstillgång får ny funktionalitet eller har fått ändrat eller utökat användningsområde
- när antalet användare förändras påtagligt
- om informationstillgången ska behandla annan information än den ursprungliga informationsklassificeringen tog hänsyn till
- vid förändrade interna eller externa säkerhetskrav
- ny eller förändrad lagstiftning
- organisationsförändringar som påverkar informationshantering
- då det annars är påkallat

Informationsklassificering ska genomföras i så tidigt skede som möjligt för att interna och legala krav ska kunna omhändertas och vara en del av det totala beslutsunderlaget om vilket skydd informationen ska ha samt ingå i eventuella förfrågningsunderlag i samband med upphandlingar.

Syftet är att väl underbyggda beslut ska kunna fattas om vilka skyddsåtgärder som krävs. Kraven kan i vissa fall innebära hinder att utnyttja tjänster och utrustning.

[1] MSBFS 2015:5, MSBFS 2015:4, MSBFS 2016:7

9 Modell för informationsklassificering

Region Skånes modell för informationsklassificering utgår från en bedömning av konsekvenserna vid bristande konfidentialitet, riktighet och tillgänglighet.

Följande definitioner ska gälla inom Region Skåne och baseras på ”Terminologi för informationssäkerhet”, SIS-TR 50:2015.

Konfidentialitet
Informationstillgångar ska skyddas mot obehörig insyn.

Med detta menas att informationstillgången inte görs tillgänglig för eller i övrigt kommer obehöriga till del.

Riktighet
Informationstillgångar ska skyddas mot oönskad förändring.

Med detta menas att informationstillgången, vare sig obehörigen, av misstag eller på grund av funktionsstörning förändras.

Tillgänglighet
Informationstillgångar ska kunna användas av behörig person vid rätt tillfälle.

Med detta menas att informationstillgångar ska vara tillgängliga för behöriga användare i förväntad utsträckning och inom önskad tidsrymd.

9.1 Konsekvensnivåer och beskrivningar

Tabell 1 är den skala som information i Region Skåne ska klassificeras efter. Informationsklassificering ska göras utifrån de tre säkerhetsaspekterna konfidentialitet (K), riktighet (R) och tillgänglighet (T). Skalan används vid bedömning av alla tre faktorerna.

Nivåbestämningen ska utgå från de konsekvenser som obehörig åtkomst, bristande riktighet och bristande tillgänglighet ger upphov till. Att placera uppgifter felaktigt i en lägre informationssäkerhetsklass, t.ex. för att underlätta hantering, kan leda till att uppgifterna inte får det skydd som de behöver eller till att lagstiftning inte följs. På motsvarande sätt kan en placering i en för hög informationssäkerhetsklass medföra omotiverat höga kostnader och onödiga hinder för verksamheten.

9.2 Bedömningsaspekter

Vid informationsklassificering ska det tas ställning till vilka konsekvenserna blir utifrån olika aspekter som bedöms som relevanta. Dessa aspekter är förutom de övergripande konsekvenserna, ”Invånare/medarbetare”, Verksamhet/process”, ”Ekonomi” och ”Förtroende”.

Tabell 1 - Skala med konsekvensbeskrivning

Nivå/ Skala	Bedömning	Beskrivning	
1	Ingen/ Försumbar	**a) Övergripande** Ingen/försumbar skada för verksamheten/Region Skåne, annan myndighet eller enskilda fysiska eller juridiska personer.	**b) Invånare/Medarbetare** Ingen eller försumbar påverkan på liv, hälsa, rättigheter. **c) Verksamhet/Process** Ingen eller försumbar negativ effekt på verksamhetens/Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter. **d) Ekonomi** Ingen märkbar skadekostnad för verksamheten/ Region Skåne. **e) Förtroende** Ingen/försumbar förtroendeskada för verksamheten/Region Skåne.
2	Måttlig	**a) Övergripande** Måttlig skada för verksamheten/Region Skåne, annan myndighet eller enskilda fysiska eller juridiska personer. (Kan hanteras i det löpande arbetet.)	**b) Invånare/Medarbetare** Viss påverkan på liv, hälsa, rättigheter. **c) Verksamhet/Process** Viss negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter. **d) Ekonomi** Viss skadekostnad för verksamheten/Region Skåne. **e) Förtroende** Måttlig förtroendeskada för verksamheten/RS.
3	Betydande/ allvarlig	**a) Övergripande** Betydande/allvarlig skada för verksamheten/Region Skåne, annan myndighet eller enskilda fysiska eller juridiska personer.	**b) Invånare/Medarbetare** Stor påverkan på liv, hälsa, rättigheter. **c) Verksamhet/Process** Betydande negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter. **d) Ekonomi** Betydande skadekostnad för verksamheten/Region Skåne. **e) Förtroende** Betydande/allvarlig förtroendeskada för verksamheten/Region Skåne.
4	Mycket allvarlig/ katastrof	**a) Övergripande** Mycket allvarlig/ katastrofal skada, skada för rikets säkerhet för verksamheten/Region Skåne, annan myndighet eller enskilda fysiska eller juridiska personer om den inträffar.	**b) Invånare/Medarbetare** Mycket stor påverkan på liv, hälsa, rättigheter (skadade eller dödsfall). **c) Verksamhet/Process** Mycket stor negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter. **d) Ekonomi** Mycket stor skadekostnad för verksamheten/Region Skåne. **e) Förtroende** Mycket allvarlig/katastrofal förtroendeskada för verksamheten/Region Skåne.