Gemensamma anvisningar för informationsklassning

Motala kommun

Beslutsinstans:	Kommunfullmäktige	**Diarienummer:**	11/KS 0071
Datum:	2011-08-22	**Paragraf:**	107
Reviderande instans:	Kommunstyrelsen	**Diarienummer:**	
Datum:		**Paragraf:**	
Gäller från:	**2011-08-22**		

Gemensamma anvisningar för informationsklassning

Följande anvisningar utgör bilaga till Motala kommuns Informationssäkerhetspolicy vilken är kommunens övergripande styrdokument för hantering av informationssäkerhet.

All information i Motala kommun skall klassificeras utifrån krav på skyddsvärde, riktighet och tillgänglighet. Behandling av information som innehåller personuppgifter skall anmälas till kommunens personuppgiftsombud som ger anvisningar om hur informationen får hanteras.

Informationsägare är ansvarig för informationsklassning av enskilda dokument och klassificeringen genomförs främst utifrån kriterierna skyddsvärde och riktighet.

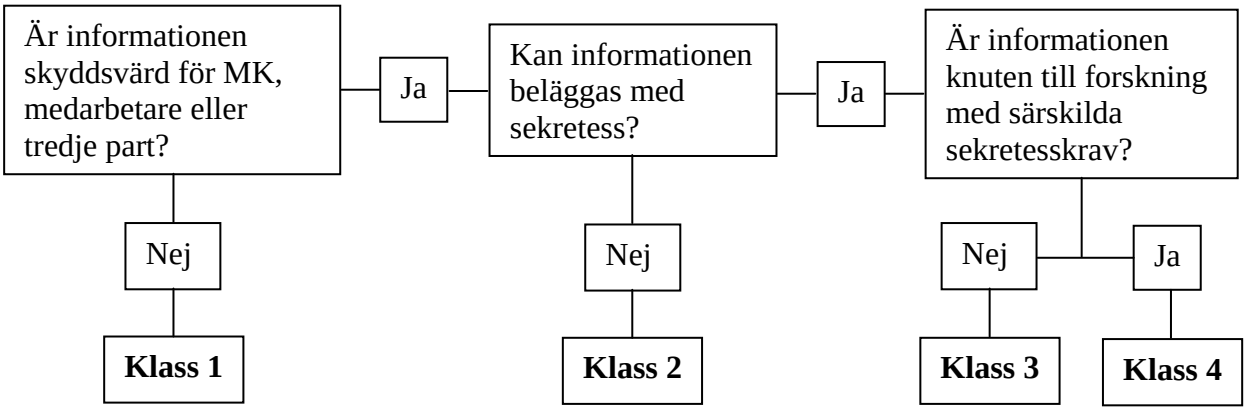
Systemägare är ansvarig för informationsklassning av hela IT-system och klassificeringen skall genomföras utifrån alla tre kriterier.

Informationsklassning

Resultatet från nedanstående tre olika klassificeringar skall utgöra det samlade kravet på skydd av och tillgänglighet till den aktuella informationen eller IT-systemet. De samlade kraven utgör grunden för hur informationsägaren skall hantera informationen och underlag för systemägarens kravställning på ett IT-system.

Skyddsvärde (sekretess)

Informationen skall vid informationsklassning bedömas utifrån kravet på skyddsvärde. Kravet på skyddsvärde klassificeras mot nedanstående fyra informationsklasser. Där informationsklass ett har lägst krav på riktighet och klass fyra högst krav på riktighet.



För information i klass 1 gäller:

- Informationen får lagras på arbetsstationens lokala hårddisk.
- Informationen får även lagras på flyttbart medium utan restriktioner.
- Informationen får överföras elektroniskt utan kryptering.
- Informationen får överföras via fax och med post, såväl internt som externt.

T.ex. information som kan spridas till en obestämd krets utan risk för negativa konsekvenser.

För information i klass 2 gäller:

- Informationen skall i första hand lagras på en fristående server och ej på arbetsstationens lokala hårddisk. Servern skall vara placerad i ett godkänt serverrum.
- Informationen får även lagras på flyttbart medium utan restriktioner.
- Informationen får överföras elektroniskt utan kryptering.
- Informationen får faxas under förutsättning att mottagarkontroll genomförs.
- Vid försändning med internpost skall förslutet kuvert användas. Extern posthantering får användas.
- Datamedia, som innehåller information i klass 2, ska vid transport/förvaring utanför verksamhetens lokaler alltid vara kontinuerligt övervakad eller krypterad.

T.ex. intern myndighetsinformation som inte kan beläggas med sekretess enligt sekretesslagen.

För information i klass 3 gäller:

- Informationen skall lagras på en fristående server i ett skyddat nät[1]. Servern skall vara placerad i ett godkänt serverrum.
- Informationen får i undantagsfall lagras på en arbetsstation under förutsättning att hela lagringsmediet är krypterat och att IT-systemet inte delar ut resurser. Informationen får lagras på flyttbart medium under förutsättning att hela lagringsmediet är krypterat samt att det hålls inlåst när det inte används.[2]

  Dessa medium får ej lämnas utan uppsikt och ej förflyttas utanför MK:s lokaler såvida det inte skickas till annan behörig mottagare. All elektronisk överföring av informationen skall vara krypterad.
- Informationen får ej faxas och vid försändning externt skall postbefordran med REK och mottagningsbevis alternativt bud användas. Vid försändning med internpost skall dubbla förslutna kuvert användas.
- Vid byte av hårddisk skall den utbytta hårddisken förstöras mekaniskt alternativt skrivas över enligt standard DoD 5520-22.M, med ett av MK tillhandahållet överskrivningsprogram så att lagrad information inte kan återskapas. Destruktionsintyg respektive signerad anteckning om överskrivning skall arkiveras.

T.ex. information som kan beläggas med sekretess enligt sekretesslagen.

---

[1] Ett skyddat nät har regler för inkommande och utgående trafik. Nätet kan skyddas med t ex brandväggar.

[2] Med arbetsstation avses både stationära och bärbara persondatorer.
Exempelvis CD/DVD/diskett/USB-minne/handdator/löstagbar hårddisk/band.
För säkerhetskopior/backup gäller särskilda rutiner

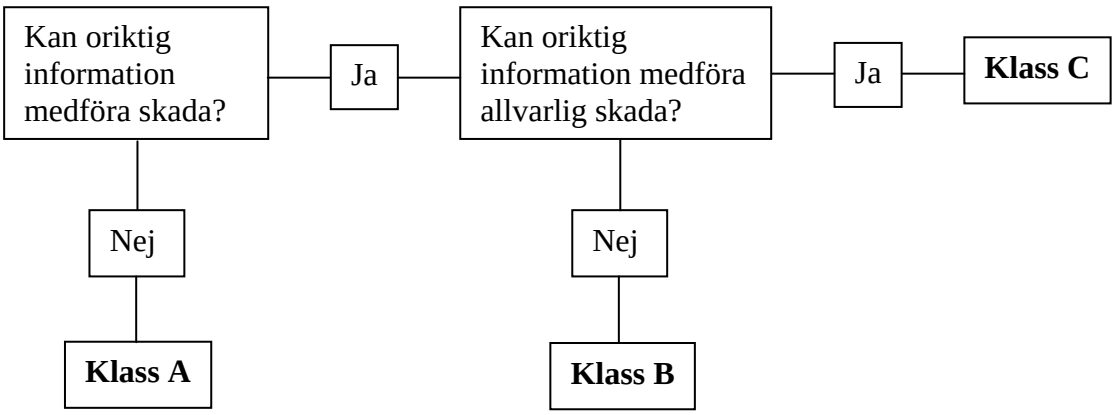
För information i klass 4 gäller:

- Informationen skall lagras på fristående server i isolerat nät[3] och ej på arbetsstationens lokala hårddisk. Servern skall vara placerad, separat inlåst, i ett godkänt serverrum.
- I de fall då server ej finns att tillgå skall informationen lagras på en krypterad separat hårddisk som när den inte nyttjas skall förvaras i säkerhetsskåp av klass SS 3492. Bärbar dator låses in på motsvarande sätt då den inte används.
- Informationen får lagras på annat flyttbart medium under förutsättning att hela lagringsmediet är krypterat samt att det förvaras inlåst i säkerhetsskåp av klass SS3492 när det inte används. Det flyttbara mediet får ej lämnas utan uppsikt och ej förflyttas utanför MK:s lokaler såvida det inte skickas till annan behörig mottagare.
- All elektronisk överföring av informationen skall vara krypterad.
- Informationen får inte faxas och vid försändning externt skall postbefordran med REK och mottagningsbevis alternativt bud användas. Informationen får inte sändas med internpost.
- Vid byte av hårddisk skall den utbytta hårddisken förstöras mekaniskt så att lagrad information inte kan återskapas. Destruktionsintyget skall arkiveras.

T.ex. information knuten till uppdragsforskning med särskilda sekretesskrav, information enligt sekretesslagen 2:1 (förhållande till främmande makt) och 2:2 (försvarssekretess)

Riktighet

Informationen skall vid informationsklassning bedömas utifrån kravet på riktighet, det vill säga skydd mot oavsiktlig eller avsiktlig förvanskning. Kravet på riktighet klassificeras mot nedanstående tre informationsklasser. Där informationsklass A har lägst krav på riktighet och klass C högst krav på riktighet.



För information i klass A gäller:
Inga krav ställs på verifiering av riktigheten i informationen eller skydd mot förvanskning av informationen.

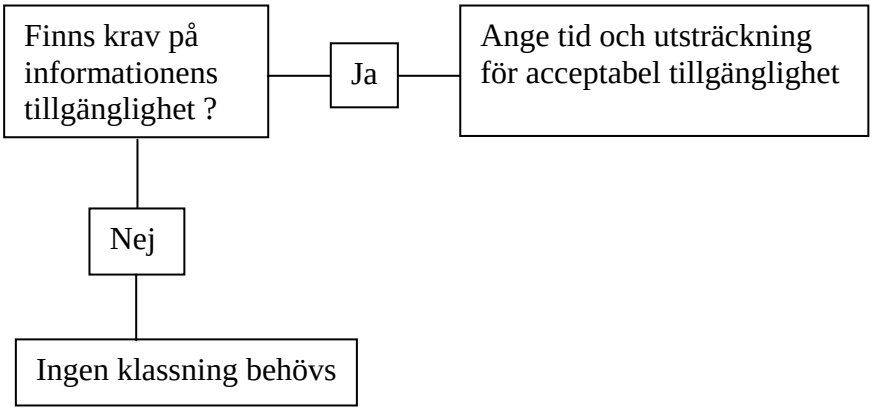
[3] Ett isolerat nät är helt fristående och inte kopplat till Internet eller andra nätverk.

För information i klass B gäller:
Informationen skall vara spårbar och riktigheten skall kunna verifieras t.ex. genom signering.
T.ex. information som ingår i myndighetsutövning, information för vilken lagrum ställer krav på riktighet, webbinformation och dylikt.

För information i klass C gäller:
Varje inmatning (transaktion) eller förändring av information skall vara spårbar och riktigheten skall kunna verifieras för varje inmatning eller förändring av information. Informationen skall förses med ett högt skydd mot oavsiktlig eller avsiktlig förändring och får endast hanteras i ett skyddat nät med ett anpassat behörighetskontrollsystem.
T.ex. Information i IT-system med särskilda krav på riktighet såsom ekonomiadministrativa system, IT-system för kritiska processer i verksamheten, IT-system som behandlar personuppgifter.

Tillgänglighet

Kravet på tillgänglighet skall uttryckas i tidstermer och i vilken utsträckning avbrott kan accepteras.



Vid framtagandet av kraven skall följande frågeställningar belysas:

- Hur länge skall informationen finnas tillgänglig?
- Hur många timmar per dygn skall informationen vara tillgänglig?
- Vad är längsta acceptabla avbrott?
- Vilket antal avbrott per tidsenhet kan accepteras?
- Varifrån skall informationen vara tillgänglig?

Referenser

Informationssäkerhetspolicy, 11/KS 0071, § 107
Rutiner för hantering av elektronisk post, KS 2009-04-21, § 121, reviderade 2010-04-08