Gemensamma anvisningar för informationsklassning

Motala kommun

Beslutsinstans:	Kommunens ledningsgrupp	**Diarienummer:**	20/KS 0015
Datum:	2020-02-13	**Paragraf:**	
Reviderande instans:		**Diarienummer:**	
Datum:		**Paragraf:**	
Gäller från:	2020-03-01		

Gemensamma anvisningar för informationsklassning

Inledning

Viktig information som är åtkomlig för obehöriga, som inte är tillgänglig för behöriga när den behövs eller som inte är tillförlitlig kan innebära stora negativa konsekvenser för en verksamhet. Informationssäkerhet handlar om att skydda organisationens information så att sådana konsekvenser inte uppstår.

Följande anvisningar utgår från Motala kommuns Informationssäkerhetspolicy, 19/KS 0116, vilken är kommunens övergripande styrdokument för hantering av informationssäkerhet. Hantering av känslig information ska göras i enlighet med Offentlighets- och sekretesslag (2009:400) och personuppgifter ska hanteras i enlighet med Dataskyddsförordningen (GDPR).

Dessa anvisningar ersätter Gemensamma anvisningar för informationsklassning, 11/KS 0071. Anvisningarna behöver kompletteras med förvaltnings- och i vissa fall verksamhetsspecifika anvisningar.

Gemensamma anvisningar för informationsklassning

All information i Motala kommun ska klassificeras utifrån krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Behandling av information som innehåller personuppgifter ska registreras separat enligt anvisningar i respektive förvaltning.

Informationsägare är ansvarig för informationsklassning av enskilda dokument. Systemägare är ansvarig för informationsklassning av hela IT-system.

Informationstillgångar måste skyddas så att:

- Endast behöriga personer kan ta del av dem (konfidentialitet)
- Vi kan lita på att de är korrekta (riktighet)
- De alltid finns när vi behöver dem (tillgänglighet)
- Det ska vara möjligt att ta reda på hur och av vem informationen har hanterats (spårbarhet)

Resultatet från ovanstående fyra kriterier för klassificering ska utgöra det samlade kravet på skydd av och tillgänglighet till den aktuella informationen eller IT-systemet. De samlade kraven utgör underlag för systemägarens kravställning på ett IT-system och avgör hur informationen ska hanteras.

Klassning av information görs utifrån en matris för konsekvensbedömning, se sidan 6. Nedan finns också förenklade flödesscheman för klassning av respektive kategori. Dessa är endast tänkta som en vägledning och täcker inte in alla typer av information.

Konfidentialitet (K)

Med konfidentialitet avses informationens skyddsvärde eller känslighet. Detta bedöms utifrån den eventuella skada som kan uppstå om obehöriga kan ta del av informationen.

System som behandlar en stor mängd information måste alltid bedömas utifrån skyddsvärdet av den samlade (aggregerade) informationen i systemet. Stora mängder öppen information kan tillsammans bli känslig och därför behöva klassas högre än de enskilda dokumenten i systemet.

Krav på konfidentialitet uppfylls oftast genom behörighetsstyrning som till exempel inloggning i system eller åtkomst till dokumentskåp.

Exempel på information med krav på konfidentialitet är intern personalinformation, personuppgifter samt uppgifter som omfattas av sekretess enligt Offentlighets- och sekretesslagen (OSL).

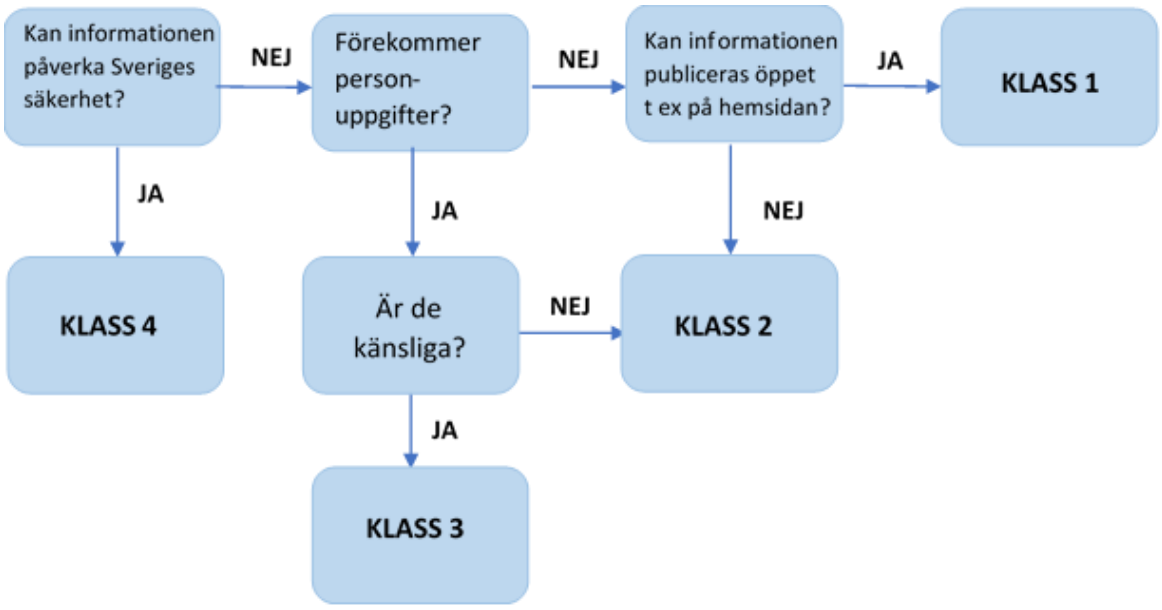

Bild 1. Förenklat flödesschema för klassning av information utifrån dess konfidentialitet.

Som *känsliga personuppgifter* klassas t ex uppgifter om politisk eller religiös övertygelse, sexuell läggning eller facklig tillhörighet. Även andra typer av personuppgifter kan vara integritetskänsliga, t ex personnummer, löneuppgifter och uppgifter om lagöverträdelser.

Riktighet (R)

Riktighet handlar om att information inte ska kunna förändras eller förvanskas. Riktigheten klassas utifrån hur viktigt det är att informationen är korrekt och hur stor skada som kan uppstå om felaktig information lämnas ut.

Krav på riktighet kan uppfyllas till exempel genom åtkomstskydd av handlingar eller system och loggar över vem som upprättat eller redigerat informationen (spårbarhet).

Information behöver vara korrekt, det är därför mycket sällsynt att information klassas som en 1:a gällande Riktighet.

Exempel på information med krav på riktighet är myndighetsbeslut, information om öppettider, kontaktuppgifter, skolbetyg och patientjournaler.

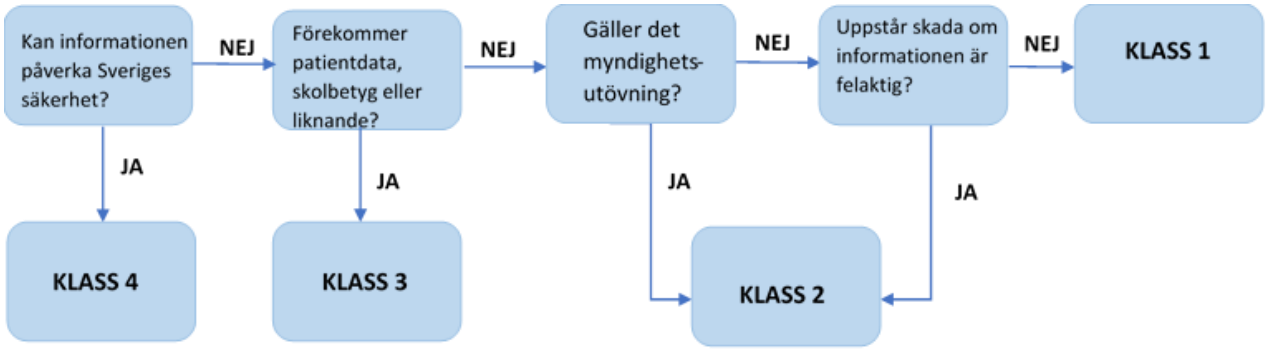

Bild 2. Förenklat flödesschema för klassning av information utifrån dess riktighet

Tillgänglighet (T)

Tillgänglighet handlar om hur länge verksamheten klarar sig utan den specifika informationen. Tillgängligheten kan påverkas av huruvida det finns alternativa informationskanaler eller kopior av dokument.

För IT-system ska tillgänglighet även uttryckas i tidstermer för att påvisa i vilken utsträckning avbrott kan accepteras. Vid klassning av IT-systems tillgänglighet bör även framgå varifrån (t ex kontorsarbetsplats eller smartphone) och när (t ex kontorstid, helger) informationen behöver vara tillgänglig.

Krav på tillgänglighet kan uppfyllas till exempel genom säkerhetskopiering av data eller att viktig information finns utskriven på papper.

Exempel på system med krav på tillgänglighet är lönesystem, journalsystem för patientdata och tekniska styrsystem.

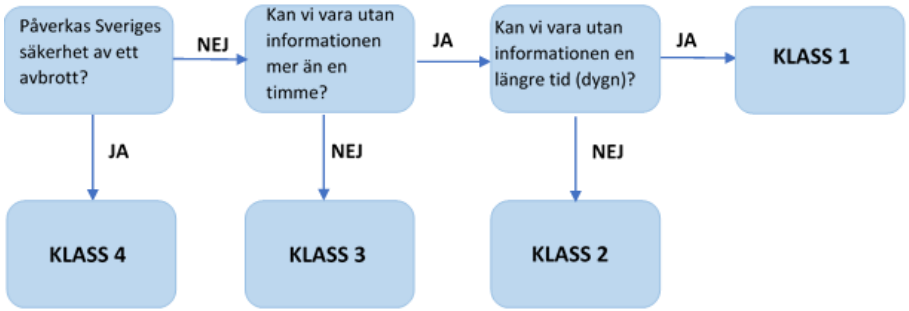

Bild 3. Förenklat flödesschema för klassning av information utifrån dess tillgänglighet

Spårbarhet (S)

Spårbarhet innebär att det i efterhand ska vara möjligt att ta reda på hur uppgifter har hanterats och av vem. Skyddsnivån avgörs av hur viktigt det är att veta vad som hänt med informationen vid förändringar av uppgifter eller i händelse av säkerhetsincidenter.

Krav på spårbarhet kan uppfyllas till exempel genom loggar över vem som tagit del av eller redigerat ett dokument, loggar i passersystem som visar vem som haft tillgång till utrymme där informationen förvaras eller genom kvittenser vid mottagande av handlingar.

Exempel på information med krav på spårbarhet är patientdata, anställningsuppgifter, myndighetsbeslut och fakturahantering.

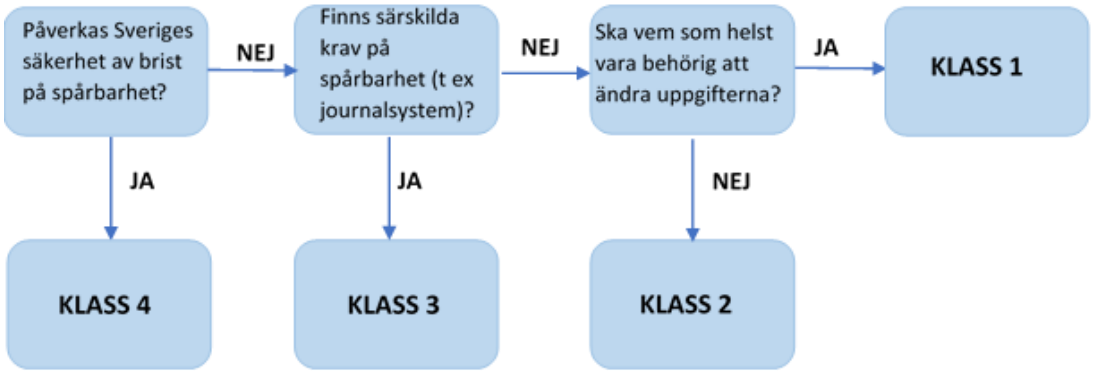

Bild 4. Förenklat flödesschema för klassning av information utifrån dess spårbarhet

Sammanställning av informationsklass

Resultatet av klassningen förs in i dokumentet med angivande av de fyra kategorierna enligt följande: K:R:T:S.

Motala

DOKUMENTHANTERINGSPLAN

PERSONALHANDLINGAR

Anställning

Handling (benämning, beskrivning)	Sortering och förvaringssätt	Gallras/ bevaras	Anmärkning	Info-klassning K:R:T:S
			Sekretess förekommer enligt: 25 kap. 1 § OSL Företagshälsovård 39 kap. 1 §§ OSL Personalsocial verksamhet 39 kap. 5 a § OSL Urvalstester	
Rekrytering:				
- behovsanalys	W-katalog	3 år		1:2:1:2
- kravprofil	W-katalog	3 år		1:2:1:2
- platsannons	Offentliga Jobb (OJ)	3 år		1:2:1:2
- ansökningshandlingar, ej erhållen tjänst	OJ	3 år efter tillsättning	Pappersansökningar gallras efter inskanning	3:3:1:2
- ansökningshandlingar, erhållen tjänst	Personalakt	Bevaras	Bevaras i personalakt	3:3:1:2
- ansökningshandlingar, spontanansökningar	-	Vid inaktualitet		3:3:1:2
- meddelanden som skickas till sökande , tex om avbruten ansökningsprocess	OJ	3 år		2:2:1:2
- bekräftelsebrev	OJ	-	Utgående till ansökande	2:2:1:2
- sammanställning av sökande	OJ	3 år efter tillsättning		2:2:1:2
- självskattningsanalyser, svarsgraf	Thomas	Bevaras	Skrivs ut och bevaras i personakt	3:3:1:2
- självskattningsanalyser, enskilda svar samt utdata	Thomas	Vid inaktualitet	Exempelvis intervjufrågor och rapporter av tillfällig karaktär	3:3:1:2
- protokoll från fackliga förhandlingar		Bevaras		2:2:1:2
- utdrag ur belastningsregister	Personalakt	Bevaras	Begärs in av personer som i sin anställning har kontakt med barn. Vill berörd person ha tillbaka registerutdraget tas en kopia. Utdraget sorteras in i personalakt.	3:3:1:2

Exempel på angivande av informationsklassning i dokumenthanteringsplan.

Nivåer för klassning och särskilda instruktioner för hantering av information i respektive nivå

Informationsklassning görs genom en konsekvensbedömning utifrån ovanstående kategorier. Konsekvensen bedöms, i varje enskild kategori, med hjälp av en skala med fyra nivåer där ett innebär lägst och fyra innebär högst konsekvens. Se matris för konsekvensbedömning på sidan 6.

Större delen av den information som kommunen hanterar kan placeras i klass 1-3. I klass 4 placeras endast information som omfattas av säkerhetsskydd, dvs uppgifter som kan beläggas med försvarssekretess enligt OSL 15 kap 2 §.

Information kan klassas på olika nivåer i olika kategorier och ska hanteras utifrån den högsta klassificeringen. Det samma gäller för IT-system som ska klassas utifrån den högst klassade information som hanteras i systemet.

Klass 1 – Ingen skyddsnivå krävs

I klass 1 placeras information där förlust av någon av kategorierna konfidentialitet/riktighet/tillgänglighet/spårbarhet inte medför någon negativ påverkan på Motala kommun eller tredje part.

Informationen får försändas med fax, post eller e-post utan begränsningar.

Klass 2 – grundläggande skyddsnivå

I klass 2 placeras information där förlust av någon av kategorierna konfidentialitet/riktighet/tillgänglighet/spårbarhet medför måttlig negativ påverkan på Motala kommun eller tredje part.

Informationen får faxas under förutsättning att mottagarkontroll genomförs. Extern och intern posthantering får användas utan begränsning. Om informationen innehåller personuppgifter ska en bedömning av integritetskänslighet göras innan informationen får skickas med e-post.

Klass 3 – utökad skyddsnivå

I klass 3 placeras information där förlust av någon av kategorierna konfidentialitet/riktighet/tillgänglighet/spårbarhet medför betydande negativ påverkan på Motala kommun eller tredje part.

Informationen får inte faxas och vid extern försändelse ska REK- eller värdepost med mottagningsbevis användas. Vid försändning med internpost ska förslutet innerkuvert användas. Elektronisk överföring av informationen måste krypteras.

Klass 4 – mycket hög skyddsnivå

I klass 4 placeras information där förlust av någon av kategorierna konfidentialitet/riktighet/tillgänglighet/spårbarhet medför skada för Sveriges säkerhet.

Information som klassificeras som 4, oavsett kategori, måste hanteras enligt särskilda instruktioner för hantering av säkerhetsskyddsklassificerade uppgifter.

Informationen får inte faxas och extern försändelse måste ske i säkerhetskuvert med REK- eller värdepost med mottagningsbevis. Informationen får inte skickas med internposten. För elektronisk överföring krävs särskild kryptering (signalskydd).

Matris för konsekvensbedömning

	Konfidentialitet	**Riktighet**	**Tillgänglighet**	**Spårbarhet**
4 Allvarlig	Röjande av informationen medför skada för Sveriges säkerhet. *I klass fyra återfinns säkerhetsskydds-klassificerade uppgifter, företrädesvis uppgifter som omfattas av sekretess enligt OSL 15 kap 2 §.*	Uppgifter som ändras obehörigen medför skada för Sveriges säkerhet. *I klass fyra återfinns säkerhetsskydds-klassificerade uppgifter, företrädesvis uppgifter som omfattas av sekretess enligt OSL 15 kap 2 §.*	Avbrott medför skada för Sveriges säkerhet. *I klass fyra återfinns säkerhetsskydds-klassificerade uppgifter, företrädesvis uppgifter som omfattas av sekretess enligt OSL 15 kap 2 §.*	Avsaknad av spårbarhet medför skada för Sveriges säkerhet. *I klass fyra återfinns säkerhetsskydds-klassificerade uppgifter, företrädesvis uppgifter som omfattas av sekretess enligt OSL 15 kap 2 §.*
3 Kännbar	Förlust av konfidentialitet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex känsliga personuppgifter eller information som kan beläggas med sekretess enligt OSL.*	Förlust av riktighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex journalsystem för patientdata eller system för skolbetyg.*	Förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex journalsystem för patientdata etc där avbrott på mer än en timme innebär betydande negativa konsekvenser för verksamheten.*	Förlust av spårbarhet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex journalsystem för patientdata*
2 Lindrig	Förlust av konfidentialitet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex personuppgifter eller intern information som kan publiceras, eventuellt med inloggningskrav, på intranätet.*	Förlust av riktighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex information för myndighetsutövning eller information med lagkrav på riktighet.*	Förlust av tillgänglighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex informations-system som kan vara otillgängliga i några timmar utan direkt negativ inverkan på verksamheten*	Förlust av spårbarhet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex information för myndighetsutövning*
1 Försumbar	Förlust av konfidentialitet medför inte någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex information som kan publiceras på kommunens hemsida.*	Förlust av riktighet medför inte någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex information som enkelt kan återställas.*	Förlust av tillgänglighet medför inte någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. *T ex informations-system som kan vara otillgängliga i flera dygn utan konsekvens.*	Förlust av spårbarhet medför inte någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.

En mer utförlig version av matrisen återfinns i arbetsmaterialet för informationsklassning som finns på extranätet tillsammans med mallar för informationssäkerhetsarbetet.

Referenser

Offentlighets- och sekretesslag (2009:400)

Dataskyddsförordningen (GDPR)

Informationssäkerhetspolicy (19/KS 0116)