Upplands Väsby kommun

Styrdokument

Datum:
2023-05-02

Diarienummer:
KS/2022:154

Riktlinjer för klassificering av information

Kategori	Styrdokumentsuppgifter
Nivå	Kommungemensamt
Kategori	Normerande styrdokument
Antagen	Kommunstyrelsen den 29 maj 2023
Ikraftträdande	Den 1 juli 2023
Giltig till och med	Tills vidare
Ansvarig ägare	Kommundirektör

Innehåll

Styrdokument 1
Riktlinjer för klassificering av information 1
1 Styrdokumentets roll och omfattning 3
2 Begreppsförklaring 3
3 Vad är informationsklassning? 4
4 Syfte med informationsklassning 5
5 Kommunens informationssäkerhet och dess säkerhetsaspekter 5
5.1 Avgränsning 5
6 Ansvar och roller 5
6.1 Central styrning 5
6.2 Lokal styrning 6
7 Arbetssätt och metod för klassificering av information 6
7.1 Informationsklassningsprocess 7
7.2 Aggregation och inferens 8
7.3 Beroende av information från annan verksamhet 8
8 Generell informationsklassning 9
8.1 Säkerhetsaspekter 9
8.2 Modell för generell informationsklassning 9
8.3 Skyddsnivå och säkerhetsåtgärder 11
9 Klassificering av hemlig information 11
9.1 Modell för klassning av hemlig information 11
9.2 Skyddsnivå för hemlig information 12
9.3 Säkerhetsåtgärder för hemlig information 12

Versionshistorik

Versionsnummer	Datum	Författare	Version och ändringar
1.0 – KS/2022:154	2023-05-29	Niza Löfdahl	Första utgåva

1 Styrdokumentets roll och omfattning

Riktlinjer för klassificering av information fastställs av kommunstyrelsen. Styrdokumentet ska användas som ett stöd i arbete med klassificering av organisationens fysiska, muntliga och digitala information. På så sätt upprätthålls kommunens arbete med fysisk, personlig och digital informationssäkerhet i enlighet med kommunens informationssäkerhetspolicy.

Detta styrdokument ska gälla för hela organisationen.

2 Begreppsförklaring

I detta styrdokument avses med

avbrott	fysisk eller digital information som för tillfälle är oåtkomligt på grund av till exempel ett planerat fysiskt eller tekniskt underhållsarbete, angrepp, tekniskt problem eller andra typer av hinder,
hemlig information	information som innehåller säkerhetsskyddsklassificerade uppgifter enligt säkerhetsskyddslagen,
inferens	en slutsats som dras utifrån en kontext av mängder av harmlösa uppgifter. Slutsatsen kan ge en bild om verksamhetens sårbarhet eller avslöjas verksamhetens hemlighet. Ett exempel på inferens är uppgifter om Pentagons dubbelbeställningar på pizza natten innan USA:s invasion av Panama,
informationsmängd	en gruppering av information, som exempelvis i form av dokument, register, databaser eller liknande, som innehåller flera informationstyper,
informationstyp	ett visst slag av information som kan finnas lokalt inom verksamheten eller hela organisationen, som exempelvis personuppgifter (namn, adress, telefonnummer osv), belopp, m.m.,
informationstillgång	skyddsobjekt som består av information (skyddsvärd information) och resurs som hanterar/förvaltar/förvarar informationen. Informationen är den primära delen av tillgången. Resursen avser såväl manuell som it-baserad

	informationshantering. Telekom och kommunikationssystem räknas som resurs,
klassningsobjekt	informationstillgångar som ska klassas vid ett specifikt tillfälle. Ett klassningsobjekt kan vara enbart information eller information och resurs som hanterar informationen. En nämnd (arkivbildare) kan också klassas som ett klassningsobjekt i vissa sammanhang,
kontor	ett tjänstorgan som arbetar med verkställande av politiska beslut. Bolag, stiftelse och sakkunniga revisorer är likställda med kontor enligt detta styrdokument,
organisation	Upplands Väsbys kommunkoncern som består av verksamheter (politiska organ) samt kontor, bolag, stiftelse och sakkunniga revisorer (tjänstorgan),
skyddsvärd information	värdefull information som behöver skyddas. Skyddsvärd information är till exempel information om hur organisationen använder it-system i en specifik verksamhet, uppgifter om enskilda medborgare, organisationens risk- och sårbarhetsanalys, vissa ritningar, vissa uppgifter som kopplas till organisationens nyckelpersoner, samt information som berör hälso- och sjukvård, dricksvatten, energiförsörjning etc. Informationsklassning är en metod som används för att identifiera skyddsbehovet för den finns informationsmängd,
verksamhet	ett politiskt organ så som kommunstyrelse och dess utskott, kommunens nämnder, bolags- och stiftelsestyrelse och kommunens förtroendevalda revisorer.

3 Vad är informationsklassning?

Informationsklassning är en arbetsprocess där organisationens information värderas. Värderingen baseras på negativa konsekvenser som kan uppkomma på grund av otillräckligt skydd för informationens konfidentialitet, riktighet och tillgänglighet. De negativa konsekvenserna kan påverka enskild persons liv och hälsa, verksamheten, annan verksamhet, miljö, grundläggande demokratiska värden eller Sveriges säkerhet.

Arbetsprocessen ska genomföras i enlighet med bestämmelser enligt kapitel 7, *Arbetssätt och metod för klassificering av information.* Klassningsaktiviteten görs utifrån organisationens klassningsmodeller i kapitel 8.2, *Modell för generell informationsklassning* och kapitel 9.1. *Modell för klassning av hemlig information.*

4 Syfte med informationsklassning

Syftet med klassificering av information är att:

- öka medvetenhet om och förståelse av negativa konsekvenser som kan uppkomma på grund av otillräckligt skydd,
- bedöma och fastställa krav på säkerhetsåtgärder som det aktuella klassningsobjektet och den aktuella informationens behöver,
- organisationens systematiska informationssäkerhetsarbete upprätthålls.

5 Kommunens informationssäkerhet och dess säkerhetsaspekter

Enligt kommunens informationssäkerhetspolicy (KS/2021:396) innebär informationssäkerhetsarbetet att skydda organisationens information i alla former. Det innebär att organisationens fysiska, muntliga och digitala information ska skyddas utifrån olika säkerhetsaspekter. Säkerhetsaspekterna enligt informationssäkerhetspolicyn består av:

- konfidentialitet,
- riktighet,
- tillgänglighet,
- spårbarhet.

5.1 Avgränsning

I enlighet med informationssäkerhetspolicyn ska spårbarhetsaspekten inte tillämpas i informationsklassningen.

6 Ansvar och roller

Ansvar och roller delas in i två nivåer enligt beskrivningen nedan.

6.1 Central styrning

Den centrala styrningen utgörs av kommunstyrelsen med kommunledningskontoret som utförare.

6.1.1 Kommunstyrelsen

Kommunstyrelsen fastställer handlingsplanen för kommunens övergripande informationssäkerhetsarbete. Handlingsplanen ska bland annat inbegripa klassificering av information som hanteras av kommunledningskontoret men som ägs av olika verksamheter inom organisationen. Ett exempel på detta är information som förekommer i ärenden för medborgare och företag samt upphandlingar.

Kommunstyrelsen fastställer även en handlingsplan för sitt informationssäkerhetsarbete som ska verkställas av kommunledningskontoret.

6.1.2 Kommunledningskontoret

Kommunledningskontoret tar fram förslag till handlingsplanerna enligt kapitel 6.1.1. Handlingsplanerna ska ses över årligen. Om det sker någon extra ordinär händelse såsom krig och kris ska handlingsplanerna ses över vid den tidpunkten.

Kontoret tar fram en sammanställning över säkerhetsåtgärder som ska tillämpas av verksamheterna.

Kommunledningskontoret tar fram en gemensam mall för själva klassningen enligt 7.1.3. *Klassning av information* och ger stöd i klassningsarbetet.

Kommunledningskontoret tar fram en gemensam mall för handlingsplan för informationssäkerhetsarbete. Kontoret ska också ge stöd till verksamheterna i framtagande av handlingsplaner.

Kommunledningskontoret genomför klassningsprocessen avseende personuppgifter i samverkan med samtliga verksamheter. Eftersom denna informationstyp förekommer i alla verksamheter inom organisationen, ska alla personuppgiftsansvariga medverka i detta arbete.

6.2 Lokal styrning

Den lokala styrningen består av politiska organ så som nämnder, utskott, bolags- och stiftelsestyrelse och kommunens förtroendevalda revisorer, samt tjänstorgan.

6.2.1 Nämnder, utskott, bolags- och stiftelsestyrelse och kommunens förtroendevalda revisorer

Varje verksamhet fastställer en handlingsplan för sitt informationssäkerhetsarbete. En beskrivning av klassificeringen av verksamhetens information ska framgå av handlingsplanen.

6.2.2 Kontor, bolag, stiftelse och sakkunniga revisorer

Det lokala tjänstorganet tar fram ett förslag till handlingsplan enligt 6.2.1. samt genomför klassificering av information i enlighet med detta styrdokument. Handlingsplanen ska ses över årligen. Om det sker någon extra ordinär händelse såsom krig och kris ska handlingsplanerna ses över vid den tidpunkten.

Med stöd av kommunledningskontoret genomför kontor, bolag, stiftelse och sakkunniga revisorer informationsklassning för den verksamheten som den tillhör. Kontoret, bolaget, stiftelsen och sakkunniga revisorerna tar också fram tidsramen för att kunna bedöma konsekvensnivåer för verksamhetens information tillgänglighet.

7 Arbetssätt och metod för klassificering av information

Informationsklassningsarbetet ska genomföras i enlighet med processbeskrivningen i detta kapitel. En bedömning av aggregation, inferens och beroende av information från annan verksamhet ska göras under processens gång. Detta beskrivs närmare i kapitel 7.2 *Aggregation och inferens* samt kapitel 7.3 *Beroende av information från annan verksamhet.*

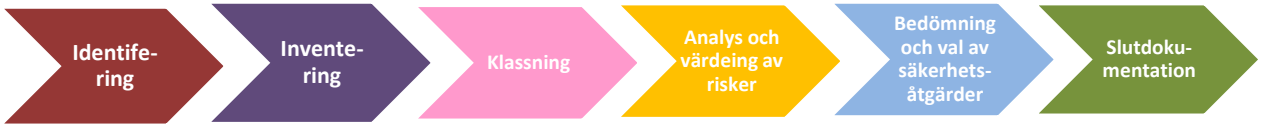
Klassningsarbetet genomförs med stöd av ett standardiserat verktyg för informationsklassning som fastställs av kommunledningskontoret.

7.1 Informationsklassningsprocess

Informationsklassningsprocessen ska genomföras i workshop, där deltagare med olika kompentenser och perspektiv deltar.

Arbetet ska ledas av en workshopledare som har kompetens inom informationsklassning. Verksamheten avgör vilka som ska delta därutöver.

Informationsklassningsprocessen består av sex olika aktiviteter enligt modellen nedan. De sex aktivisterna ska genomföras i olika steg efter varandra i enlighet med modellen.



Modell för arbetsprocess för informationsklassning

7.1.1 Identifiering

I denna aktivitet identifieras och beskrivas klassningsobjektet och informationen som ska ingå i klassningen. Resursen som hanteras informationen ska också identifieras och beskrivas. Vid detta tillfälle ska också legala och interna krav gällande informationssäkerhet, och som är relevanta för verksamheten, identifieras.

Identifieringsaktiviteten ska dokumenteras. Resultatet ska användas som underlag i inventeringsaktiviteten.

7.1.2 Inventering

Informationsmängder och informationstyper ska inventeras och beskrivas. In- och utdata samt arbetsprocesser för lagring av data ska också inventeras och beskrivas. Därutöver ska arbetsgruppen inventera om en del av informationsmängderna har bevarats i olika former och lagringsenheter. Exempelvis inkomna pappersansökningar med samma innehåll som har bevarats båda i pappers- och digitalt format. Ett annat exempel är inkomna elektroniska ansökningar med samma innehåll som har bevarats i olika it-system/stöd.

Resultatet från inventeringen ska dokumenteras och användas som underlag i klassningsaktiviteten.

7.1.3 Klassning av information

Vid klassningsaktiviteten ska konsekvens- och skyddsnivåer fastställas. Informationen ska ses som den primära informationstillgången och resursen ska ses som den sekundära informationstillgången.

Bedömningen av konsekvens- och skyddsnivåer ska göras i enlighet med bestämmelser enligt kapitel 8.2, *Modell för generell informationsklassning* och kapitel 9.1, *Modell för klassning av hemlig information*.

Resultatet från klassningen ska dokumenteras och användas som underlag i aktiviteten ”*Analys och värdering av risker”*.

7.1.4 Analys och värdering av risker

I dokumentationen av analysen och riskbedömningen ska det framgå:

- vilka risker som kan förekomma på grund av ett bristande skydd,
- vilka risker som kan medföra stora negativa konsekvenser,
- hur hög sannolikheten är att riskerna kan inträffa och
- vilka risker är högprioriterade.

Resultatet från denna aktivitet ska användas som underlag i aktiviteten ”*Bedömning och val av säkerhetsåtgärder”.*

7.1.5 Bedömning och val av säkerhetsåtgärder

Den färdigställda analysen och värderingen av risker och sannolikheter är fundamentet i bedömningen och valet av säkerhetsåtgärder. Säkerhetsåtgärderna ska motsvara behovet av de ingående informationsmängdernas högsta klassning och som därmed även ger tillräckligt skydd för de informationsmängder med lägre klassning.

Resultatet från denna aktivitet ska ingå i slutdokumentationen enligt kapitel 7.1.6.

7.1.6 Slutdokumentation

Slutresultatet från hela informationsklassningsprocessen ska dokumenteras. Denna dokumentation ska användas som underlag till framtida klassificering av det aktuella klassningsobjektet och den aktuella informationen.

Slutdokumentationen ska också användas som underlag för att avgöra vilken resurs som kan hantera den aktuella informationen. Framförallt kan slutresultatet användas som underlag till kravspecifikation vid upphandling av it-system/stöd.

7.2 Aggregation och inferens

Harmlös information kan vara känslig om den ackumuleras och aggregeras med annan information.

Antagonister, kriminella, terrorister, främmande makt eller annan typ av verksamhet kan utnyttja mängder av harmlösa uppgifter för att dra slutsatser som kan användas i angreppssyfte.

Därför ska en bedömning av aggregation och inferens göras under klassningsprocessens gång. På så sätt har informationen tillräckligt skydd.

7.3 Beroende av information från annan verksamhet

Information som skapas och samlas i en verksamhet kan nyttas av annan verksamhet inom organisationen. Ett exempel på detta är geodata.

Därför ska en bedömning av verksamhetens beroende av information från annan verksamhet göras under klassningsprocessens gång.

8 Generell informationsklassning

Generell informationsklassning ska genomföras. Om det framkommer i detta klassningsarbete att verksamheten hanterar information som omfattas av säkerhetsskyddslagen, ska informationen klassas enligt klassningsmollen i kapitel 9.1, *Modell för klassificering av hemlig information*.

8.1 Säkerhetsaspekter

Den generella klassningen utförs utifrån de tre säkerhetsaspekterna som beskrivs i kapitel 5, *Kommunens informationssäkerhet och dess säkerhetsaspekter*. Tabellen nedan (tabell 1) är en sammanställning över säkerhetsaspekterna och förklaringar av organisationens syfte med informationssäkerhetsarbete.

Säkerhetsaspekt	**Förklaring**
Konfidentialitet	Att information ska skyddas från obehörig åtkomst
Riktighet	Att information ska skyddas från förvanskning och förstörelse, samt att informationen är korrekt och relevant för den process som den ska stödja
Tillgänglighet	Att information ska vara lättåtkomlig och sökbar för behörig person i den bestämda utsträckning och tidsramen

Tabell 1 – säkerhetsaspekter för generell informationsklassning

8.2 Modell för generell informationsklassning

Klassningsmodellen och koderna enligt tabell 2 ska användas vid generell informationsklassning.

Säkerhetsaspekt **Konsekvensnivå** **Skyddsnivå**	**Konfidentialitet (K)**	**Riktighet (R)**	**Tillgänglighet (T)**
Sveriges säkerhet **Säkerhetsskydd**	K4. Information som omfattas av säkerhetsskyddslagen (hemlig information) har en särskild rutin enligt kapitel 9		
Allvarlig konsekvens **Hög skyddsnivå**	K3	R3	T3

Säkerhetsaspekt Konsekvensnivå Skyddsnivå	Konfidentialitet (K)	Riktighet (R)	Tillgänglighet (T)
Betydande konsekvens **Utökad skyddsnivå**	K2	R2	T2
Ringa konsekvens **Grundläggande skyddsnivå**	K1	R1	T1
Ingen konsekvens **inget skydd - öppen**	K0	Inte tillämpligt. Det finns alltid krav på riktighet	Inte tillämpligt. Det finns alltid krav på tillgänglighet

Tabell 2 – modell för generell informationsklassning

Se nedan förklaringar av koderna enligt tabell 2.

- ***Konfidentialitet (K)***
  - **K0**: information som kan spridas inom och utom organisationen *utan risk för negativa konsekvenser* för enskild persons liv och hälsa, verksamheten, annan verksamhet, miljö eller grundläggande demokratiska värden.
  - **K1**: information som vid obehörig spridning *medför ringa negativa konsekvenser* för enskild persons liv och hälsa, verksamheten, annan verksamhet, miljö eller grundläggande demokratiska värden.
  - **K2:** information som vid obehörig spridning *medför betydande negativa konsekvenser* för enskild persons liv och hälsa, verksamheten, annan verksamhet, miljö eller grundläggande demokratiska värden.
  - **K3:** information som vid obehörig spridning *medför allvarliga negativa konsekvenser* för enskild persons liv och hälsa, verksamheten, annan verksamhet, miljö eller grundläggande demokratiska värden.
  - **K4:** information som innehåller säkerhetsskyddsklassificerade uppgifter (hemliga uppgifter) enligt säkerhetsskyddslagen. Informationen ska klassas i enlighet med bestämmelser i kapitel 9.1, *Modell för klassning av hemlig information*.
- ***Riktighet (R)***
  - **R1**: information som vid obehörig förvanskning, förstörelse eller att informationen inte är korrekt och relevant för den process som den ska stödja, *medför ringa negativa* konsekvenser för enskild persons liv och hälsa, verksamheten, annan verksamhet, miljö eller grundläggande demokratiska värden.
  - **R2**: information som vid obehörig förvanskning, förstörelse eller att informationen inte är korrekt och relevant för den process som den ska stödja, *medför betydande negativa konsekvenser* för enskild persons liv och hälsa, verksamheten, annan verksamhet, miljö eller grundläggande demokratiska värden.
  - **R3**: information som vid obehörig förvanskning, förstörelse eller att informationen inte är korrekt och relevant för den process som den ska stödja, *medför allvarliga negativa konsekvenser* för enskild persons liv och hälsa,

verksamheten, annan verksamhet, miljö eller grundläggande demokratiska värden.

- ***Tillgänglighet (T)***

  Varje verksamhet ska bestämma om tidsramen som verksamheten klarar av och kan utföra sina arbetsuppgifter/uppdrag vid avbrott.

  - **T1**: information som kan tillåtas vara otillgänglig och får gå förlorad under den tidsramen som verksamheten har bestämt. Om informationen inte är tillgänglig inom den givna tidsramen *medför ringa negativa konsekvenser* för enskild persons liv och hälsa, verksamheten, andra verksamheter, miljö eller grundläggande demokratiska värden.
  - **T2:** information som kan tillåtas vara otillgänglig och får gå förlorad under den tidsramen som verksamheten har bestämt. Om informationen inte är tillgänglig inom den givna tidsramen *medför betydande negativa konsekvenser* för enskild persons liv och hälsa, verksamheten, andra verksamheter, miljö eller grundläggande demokratiska värden.
  - **T3:** informationen som ingår i kritisk verksamhet. Informationen kan tillåtas vara otillgänglig under den tidsramen som verksamheten har bestämt och får inte gå förlorad. Om informationen inte är tillgänglig inom den givna tidsramen *medför allvarliga negativa konsekvens* för enskild persons liv och hälsa, verksamheten, andra verksamheter, miljö eller grundläggande demokratiska värden.

8.3 Skyddsnivå och säkerhetsåtgärder

Skyddsnivån för den aktuella informationen ska bedömas utifrån konsekvensnivån som har identifierats. Säkerhetsåtgärder som tillämpas ska motsvara det behov som behövs för informationen.

9 Klassificering av hemlig information

Säkerhetsklassificerade uppgifter ska klassas enligt bestämmelser i detta kapitel.

9.1 Modell för klassning av hemlig information

Säkerhetsskyddsklassificerade uppgifter ska klassas i olika säkerhetsskyddsklasser enligt tabell 3 som baseras på säkerhetsskyddslagen. Säkerhetsklasserna bedöms utifrån skada för Sveriges säkerhet som kan uppkomma genom ett röjande av hemliga uppgifter. För att säkerställa tillräckligt skydd för hemlig information ska säkerhetsåtgärder bedömas utifrån informationens konfidentialitet, riktighet och tillgänglighet. Detta beskrivs mer i kapitel 9.3, *Säkerhetsåtgärder för hemlig information*.

Säkerhetsskyddsklass	Skadenivå	Konsekvens
Kvalificerat hemlig	Synnerlig allvarlig skada	Ett röjande av hemliga uppgifter till obehöriga kan medföra synnerlig allvarlig skada för Sveriges säkerhet
Hemligt	Allvarlig skada	Ett röjande av hemliga uppgifter till obehöriga kan medföra

		allvarlig skada för Sveriges säkerhet
Konfidentiell	Inte obetydlig skada	Ett röjande av hemliga uppgifter till obehöriga kan medföra betydlig skada för Sveriges säkerhet
Begränsat hemlig	Endast ringa skada	Ett röjande av hemliga uppgifter till obehöriga kan medföra endast ringa skada för Sveriges säkerhet

Tabell 3 – modell för klassificering av hemlig information

9.2 Skyddsnivå för hemlig information

Skyddsnivåer enligt tabell 4 ska tillämpas på alla tänkbara resurser och metoder som hanterar organisationens säkerhetsskyddsklassificerade uppgifter.

Skyddsnivå	Säkerhetsskyddsklass
3 – Högsta skyddsnivå för hemlig information	För information som klassas som kvalificerat hemlig
2 – Utökad skyddsnivå för hemlig information	För information som klassas som konfidentiell eller hemlig
1 – Lägsta skyddsnivå för hemlig information	För information som klassas som begränsat hemlig

Tabell 4 – skyddsnivå för hemlig information

9.3 Säkerhetsåtgärder för hemlig information

Säkerhetsåtgärder för hemlig information ska ge tillräckligt skydd för informationens konfidentialitet, riktighet och tillgänglighet. Säkerhetsåtgärderna ska:

1. skyddas informationen från obehörigt röjande, förvanskning, manipulering, förstörelse samt vara tillgänglig för behörig person inom den bestämda utsträckningen och tidsramen,
2. vara korrekt och relevant för den process som den stödja,
3. förebygga skadlig inverkan i övrigt på uppgifter och informationssystem.

Säkerhetsåtgärderna är främst riktade mot spioneri, sabotage eller annan typ av verksamhet som han hota Sveriges säkerhet.