Alvesta kommun

Alvesta kommun

Riktlinje för informationssäkerhet

PROGRAM PLAN POLICY **RIKTLINJE**

Beslutat av:	Kommunstyrelsen § 119/2024
Beslutsdatum:	2024-09-10
Gäller från och med:	2024-09-10
Giltighetstid:	Gäller till och med 2028-12-31
Dokumentet gäller för:	Alvesta kommunkoncern
Ansvarig för uppföljning:	Kommunledningsförvaltningen
Diarienummer:	KS 2024-00310 5.5.3

Alvesta kommun Postadress: Alvesta kommun, 342 80 Alvesta · Besök: Centralplan 1, 342 80 Alvesta · Tel: 0472-150 00
E-post: kommunen@alvesta.se · Webb: alvesta.se

Alvesta kommun

Datum: 2024-09-10

Dnr: KS 2024-00310 5.5.3

Riktlinje

Alvesta kommuns styrdokument

Våra styrdokument kan vara av två huvudtyper, aktiverande och normerande. Aktiverande dokument syftar till förändring och utveckling och anger på så sätt hur vi ska agera för att nå ett visst resultat. Normerande dokument reglerar befintlig verksamhet och talar om hur vi ska förhålla oss till en given situation.

Aktiverande

Aktiverande dokument syftar till förändring och utveckling. De förklarar vad vi vill åstadkomma och utformningen av uppdraget.

Program – Anger långsiktiga ambitioner och viljeinriktningar.

Plan – Anger konkreta åtgärder, tidsramar och ansvar.

Normerande

Normerande dokument berör hur vi utför befintlig verksamhet, till skillnad från aktiverande vars uppgift är att bryta nya vägar.

Policy – Anger kommunens principer eller inriktning i en viss fråga.

Riktlinje – Anger absoluta gränser och skakrav.

Innehållsförteckning

Syfte **3**

Omfattning **3**

Informationssäkerhetsarbete **3**

Ansvar och befogenheter *3*

Ledningssystem för informationssäkerhet *4*

Informationssäkerhetsprocesser *4*

Identifiering och hantering av risker *5*

Informationsklassning *5*

Konsekvensbedömning *7*

Informationssäkerhet för medarbetare med flera **10**

Informationssäkerhet för nätverk samt informations- och kommunikationssystem **10**

Kontinuitetsplanering **10**

Syfte

Denna riktlinje konkretiserar policyn för informationssäkerhet som har antagits av kommunfullmäktige. Det övergripande målet med riktlinjen är att tillse att det operativa informationssäkerhetsarbetet bedrivs i enlighet med gällande lagstiftning och med informationssäkerhetspolicyn.

Kommunstyrelsen styr med denna riktlinje kommunens informationssäkerhetsarbete i enlighet med MSB:s rekommendationer samt med beaktande av kraven i inforationssäkerhetsstandarden ISO/ICE 27000.

I denna riktlinje avses med Alvesta kommun, hela kommunens organisation och de bolag där kommunen har ett avgörande ägarinflytande.

Omfattning

Denna riktlinje omfattar all behandling av information som tillhör Alvesta kommun oavsett format. I de fall informationen hanteras digitalt omfattas samtliga IT-miljöer. Om Alvesta kommuns information behandlas i en extern miljö ska behandlingen vara reglerad i avtal i enlighet med denna riktlinje.

Informationssäkerhetsarbete

All information som behandlas i Alvesta kommun ska vara identifierad, informationssäkerhetsklassificerad och förtecknad. Av förteckningen ska det framgå vem som är informationsägare. IT-stöd som används för att behandla och information ska vara förtecknade och informationssäkerhetsklassificerade samt ha en utsedd ägare.

Ansvar och befogenheter

Kommunstyrelsen ansvarar i enlighet med informationssäkerhetspolicyn för det strategiska arbetet med informationssäkerhet. Med detta menas bland annat att kommunstyrelsen ansvarar för vad som ska skyddas och hur en verksamhet ska avgöra lämplig skyddsnivå.

Kommunchef ansvarar för att upprätta, och vid behov revidera, tillämpningsanvisningar i form av ett ledningssystem för informationssäkerhet. Förändringar i ledningssystemet för som är av principiell beskaffenhet, det vill säga förändringar som påverkar kommunens

risker, konsekvensbedömningar, antal skyddsnivåer eller andra grundläggande strukturer i informationssäkerhetsarbetet ska beslutas av kommunstyrelsen.

Av informationssäkerhetspolicyn framgår respektive nämnds och bolags ansvar för informationssäkerhetsarbetet.

Ledningssystem för informationssäkerhet

Ledningssystemet för informationssäkerhet ska, tillsammans med eventuellt övriga till området hörande tillämpningsanvisningar och rutiner, konkretisera och reglera informationssäkerhetsarbetet i Alvesta kommun. Ledningssystemet sammanfattas i Alvesta kommuns informationssäkerhetshandbok.

Ledningssystemet för informationssäkerhet reglerar inte hanteringen av säkerhetsskyddsklassificerade uppgifter, det vill säga informationsklass fyra. Dessa uppgifter regleras i andra styrande dokument.

Informationssäkerhetsprocesser

För att informationssäkerhetsarbetet ska kunna bedrivas med kontinuitet och bibehållen kvalitet ska ett antal processer följas. Dessa processer ska anpassas efter Alvesta kommuns verksamhet och utformas i enlighet med tillämpliga delar i informationssäkerhetsstandarden ISO/IEC 27000.

Mot bakgrund av ovanstående ska följande processer med tillhörande anvisningar tas fram och regleras i ledningssystemet för informationssäkerhet:

- Informationsklassningsprocess – för identifiering och tilldelning av lämpligt skydd
- Riskhanteringsprocess – för identifiering av hantering av informationssäkerhetsrelaterade risker.
- Incidenthanteringsprocess - reglerar hantering och uppföljning av informationssäkerhetsrelaterade incidenter inklusive eskalering av incidenter.
- Behörighetshanteringsprocess – reglerar arbetet med tilldelning av behörigheter/åtkomst till kommunens information.

- Personalsäkerhetsprocess – för informationssäkerhetsrelaterade moment innan anställning/uppdrag, under anställning/uppdrag och vid anställningens/uppdragets avslut.

- Process för anskaffning, utveckling och avveckling av tjänster/system – avseende informationssäkerhetsrelaterade moment i arbetet med anskaffning, utveckling och avveckling av tjänster och system.

- Kontinuitetsplaneringsprocess – reglerar hur tillgång till kommunens information ska kravställas och optimeras utifrån verksamheternas behov.

- Säkerhetsmedvetandeprocess – anger hur medvetenheten om informationssäkerhet ska förmedlas och vidmakthållas.

- Uppföljningsprocess – anger hur uppföljning av informationssäkerhetsarbetet ska ske i verksamheten samt hur efterlevnaden ska säkerställas.

Identifiering och hantering av risker

Informationssäkerhetsrisker som har betydelse för informationssäkerheten i Alvesta kommuns olika verksamheter ska identifieras och dokumenteras.

Informationssäkerhetsrisker ska identifieras och analyseras kontinuerligt samt vid förändringar som har betydelse för informationssäkerheten. Eventuella risker kan identifieras vid exempelvis incidenter, uppmärksammade brister i informationssäkerhetsskyddet, omvärldsbevakning (generella hotbildstrender), anskaffning, utveckling och förändring av IT-stöd och IT-infrastrukturrevisioner med mera.

Informationsklassning

Informationsklassning ska genomföras för all den information som hanteras inom Alvesta kommun, för att informationen ska kunna tilldelas ett lämpligt skydd. Samtliga bedömningar av skyddsbehov för information ska göras enligt kommunens modell för informationsklassning. Modellen består av fem skyddsnivåer (0-4). Bedömningar av skyddsbehov ska göras utifrån informationssäkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Modellen för informationsklassning visar vilket behov av skydd en viss information har. För säkerhetsaspekten konfidentialitet gäller en direkt koppling till Offentlighet- och

sekretesslagen (OSL) och Dataskyddsförordningen. För övriga säkerhetsaspekter gäller att skyddsbehovet för informationen avgörs genom att konsekvenstabellen tillämpas *(se avsnitt konsekvenstabell).*

Skyddsnivå	**Konfiden-tialitet**	**Riktighet**	**Tillgänglig-het**	**Spårbarhet**
4. Mycket högt skyddsbehov	Säkerhetsskyddsklassificerade uppgifter som rör Sveriges säkerhet.	Information om den inte är riktig och fullständig medför synnerligen allvarlig konsekvens för kommunen eller annan part.	Information eller funktion som om den inte ör tillgänglig medför synnerligen allvarlig konsekvens för kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför synnerligen allvarlig konsekvens för kommunen eller annan part.
3. Högt skyddsbehov	Information som omfattas av stark sekretess (omvänt skaderekvisit), absolut sekretess eller uppgift som hänför till 18 kap OSL. Alternativt avser en mycket stor mängd känsliga personuppgifter som inte omfattas av stark eller absolut sekretess. Spridning kan medföra allvarliga konsekvenser för kommunen eller annan part.	Information som om den inte är fullständig eller korrekt medför allvarlig konsekvens för kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför allvarlig konsekvens för kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför allvarlig konsekvens för kommunen eller annan part.
2. Förhöjt skyddsbehov	Information som omfattas av sekretess (”svag sekretess”) enligt OSL eller känsliga personuppgifter	Information som om den inte är korrekt eller fullständig medför en betydande konsekvens för	Information eller funktion som om den inte är tillgänglig medför betydande konsekvens för	Information eller aktivitet som om den inte är spårbar medför betydande konsekvens för

	enligt GDPR, där spridning kan medföra betydande konsekvenser för kommunen eller annan part.	kommunen eller annan part.	kommunen eller annan part.	kommunen eller annan part.
1. Grundläggande skyddsbehov	Intern information avsedd att, och utan konsekvenser, spridas till medarbetare i Alvesta kommun och till externa aktörer som har rätt till /behov av informationen.	Information som om den inte är korrekt och fullständig medför en måttlig konsekvens för kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför måttlig konsekvens för kommunen eller för annan part.	Information eller aktivitet som om den inte är spårbar medför måttlig konsekvens för kommunen eller för annan part.
0. Inget skyddsbehov	Öppen information som är avsedd att, utan konsekvenser, spridas fritt inom och utom Alvesta kommun.	Information som om den inte är riktig och fullständig medför ingen eller lindrig konsekvens för kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför ingen eller lindrig konsekvens för kommunen eller för annan part.	Information eller aktivitet som om den inte är spårbar medför ingen eller lindrig konsekvens för kommunen eller annan part.

Med annan part avses extern aktör eller medborgare.
Observera att den lägsta skyddsnivån (0-Grön) representerar öppen information som inte behöver något skydd mot insyn och som normalt inte har begränsad åtkomst. Däremot är det viktigt att informationen går att förstå, därför kan även öppen information ha ett skyddsbehov när det gäller riktighet, tillgänglighet och spårbarhet. Gränsen mellan informationsklass 0 och 1 avseende konfidentialitet bygger på om informationen är tänkt att spridas (exempelvis via intranät och webbplats).

Konsekvensbedömning

För varje konsekvensområde bedöms eventuella konsekvenser av att en viss information inte har lämpligt skydd. Vid informationsklassning ska alltså verksamheten, utifrån konsekvenstabellen, bedöma skyddsbehovet av en viss information, genom att analysera och värdera konsekvenserna av att informationen i fråga sprids/görs tillgänglig för obehörig, inte är tillgänglig, inte stämmer och inte är spårbar.

De fyra konsekvensområdena i tabellen är gemensamma för hela kommunen. För att ge stöd åt vilka konsekvenser som avses är konsekvenserna indelade i ett antal nivåer; lindrig, måttlig, betydande, allvarlig och synnerligen allvarlig konsekvens. Notera att synnerligen allvarlig konsekvens inte finns med, synnerligen allvarlig konsekvens avser konsekvenser för Sveriges säkerhet och relaterar inte till kommunen och dess verksamhet.

Utifrån den klassning som görs finns det lämpliga skyddsåtgärder kopplade till respektive informationsklass. Skyddsåtgärderna ska alltid utformas i paritet med den eventuella konsekvens som kan uppstå om konsekvensen realiseras. Det är därför viktigt att göra realistiska värderingar för att undvika att informationen får ett onödigt högt skydd, med höga kostnader som följd, eller för lågt skydd, vilket innebär en för stor riskoptimering.

Konsekvenstabell

Konsekvenstabellen innehåller fyra konsekvensområden som relaterar till skyddsnivåerna i klassningsmodellen.

Konsekvenstabell för informationssäkerhet				
	Konsekvensnivå			
Konsekvens-område	**0 Grön Lindriga** konsekvenser kan resultera i	**1 Gul Måttliga** konsekvenser kan resultera i	**2 Orange Betydande** konsekvenser kan resultera i	**3 Röd Allvarliga** konsekvenser kan resultera i
Liv och hälsa	Enskilda personer påverkas inte eller kan uppleva få besvärligheter som de bör kunna övervinna utan problem	Enskilda personer kan drabbas av betydande besvär men som bör kunna övervinnas trots vissa svårigheter, (exempelvis enstaka personuppgifter som inte är känsliga kan spridas)	Enskilda personer kan uppleva konsekvenser, såsom stora fysiska eller psykiska besvär eller stor ekonomisk påverkan som de bör kunna övervinna även om det måste ske med reella och allvarliga svårigheter, (exempelvis obehörig spridning	Enskilda personers liv och fysiska eller psykiska hälsa äventyras på ett sätt som är oåterkalleligt sätt eller som inte kan övervinnas av den enskilda eller får mycket stora ekonomiska konsekvenser (exempelvis genom att känsliga personuppgifter sprids till en stor krets obehöriga,

			av personuppgifter i stor omfattning)	skyddade personuppgifter tillgängliggörs eller enskilda riskerar att drabbas av personlig konkurs)
Ändamålsenlig och effektiv verksamhet	Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Ingen eller mycket begränsad ekonomisk förlust.	Andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär med endast mindre påverkan. Endast försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation Verksamheten drabbas av en mindre kostnad motsvarande mellan 5-10 % av årsbudgeten för verksamhetsgrenen.	Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder), samhällsviktiga funktioner i egen eller annan organisation påverkas i liten utsträckning. Verksamheten drabbas av stor ekonomisk förlust motsvarande mellan 10-20 % av årsbudget för verksamhetsgrenen.	Samhällsviktiga funktioner i egen eller annan organisation påverkas. Verksamheten drabbas av en ekonomisk förlust som motsvarar att verksamheten behöver läggas ned eller väsentligen drivas på annat sätt.
Förtroende/varumärke	Lite negativ uppmärksamhet	Enstaka missnöjda individer som uttalar sig i sociala medier, eller en notis i lokalmedia	Minskat förtroende genom nyheter i både riks- och lokalmedia och i organiserade grupperingar i sociala medier, (missnöjet är dock begränsat till enskilda händelser eller enskilda personers agerande	Minskat förtroende exempelvis genom ihållande drev i rikstäckande medier eller av organiserade grupperingar i sociala medier. Inte endast enskilda personer i organisationen pekas ut, utan även organisationens

				grundläggande kultur.
Regelefterlevnad	Inga svårigheter för verksamheten att nå målen	Verksamheten har inte några större svårigheter att nå målen. Kortsiktigt avsteg från lagstiftning, externa rekommendationer, interna styrdokument samt övriga regelverk	Verksamheten kan med besvär fullfölja sina uppdrag. Brott mot lagstiftning, externa rekommendationer, interna styrdokument samt övriga regelverk. Möjligt med skadeståndskrav	Det är stora svårigheter för organisationens verksamhet att fullfölja uppdragen. Brott mot lagstiftning, externa rekommendationer samt övriga regelverk. Böter, vite eller fängelsestraff

Informationssäkerhet för medarbetare med flera

Det operativa arbetet med informationssäkerhet ska genomföras i alla verksamheter. Samtliga medarbetare och förtroendevalda ska följa riktlinjen och ledningssystem för informationssäkerhet. Vissa leverantörer och konsulter ska i berörda delar också följa denna riktlinje och ledningssystem för informationssäkerhet.

Informationssäkerhet för nätverk samt informations- och kommunikationssystem

Nätverk samt information- och kommunikationssystem som lagrar och behandlar information tillhörande Alvesta kommun ska förses med lämpligt skydd för att uppfylla kraven på informationssäkerhet. Skydden ska omfattas såväl organisatoriska rutiner som tekniskt skydd.

Kontinuitetsplanering

Det ska finnas kontinuitetsplanering den verksamhet som har beroenden till verksamhetskritisk information och till IT-stöd i vilka verksamhetskritisk information behandlas.