



Informationssäkerhetspolicy för Östhammars kommun

Innehållsförteckning

1. Fastställande.....	4
2. Policyns roll i informationssäkerhetsarbetet	4
3. Allmänt om informationssäkerhet	4
4. Mål.....	5
5. Roller och ansvar	5
6. Generella krav	6
6.1. Kommunens informationssystem	6
6.2. Informationssäkerhetsutbildning	6
7. Revidering och uppföljning.....	7

Versionshantering

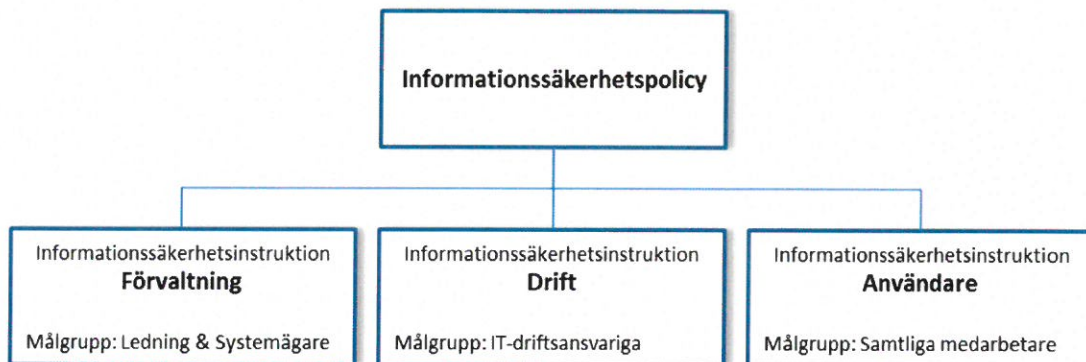
Datum	Ändrat av	Ändringsinformation	Version
2016-04-26	Dan Malmberg Jansson	Första utkast – på remiss till IT-rådet för yttrande	0.1
2016-05-17	Dan Malmberg Jansson	Komplettering efter remissvar, bl.a. avsnitt 6.6 e-post	1.0

1. Fastställande

Informationssäkerhetspolicy fastställs av Kommunfullmäktige och revideras varje mandatperiod. Informationssäkerhetsinstruktioner revideras årligen och fastställs av kommunstyrelsen.

2. Policyns roll i informationssäkerhetsarbetet

Informationssäkerhet är den del i kommunens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Informationssäkerhetspolicy och särskilda informationssäkerhetsinstruktioner styr informationssäkerhetsarbetet i Östhammars kommun.



Informationssäkerhetspolicy redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet. Policyn konkretiseras i respektive informationssäkerhetsinstruktion.

3. Allmänt om informationssäkerhet

Information är en av våra viktigaste tillgångar och hanteringen av den är en viktig del i arbetet med kommunens risk- och sårbarhetsanalys.

Utgångspunkter i vårt arbete med informationssäkerhet är:

- Lagar, förordningar och föreskrifter
- Kommunens egna krav
- Avtal

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar Östhammars kommuns informationstillgångar utan undantag.

Med informationssäkerhet avses:

- att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt
- att informationen är och förblir riktig

Informationssäkerheten är en integrerad del av vår verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar. Alla verksamheter inom Östhammars kommun är bundna av denna informationssäkerhetspolicy, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Den som använder våra informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för disciplinära åtgärder

4. Mål

Målet med Östhammars kommuns informationssäkerhetsarbete är:

- att samtlig personal har kunskap om gällande informationssäkerhetsregler
- att informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- att ingångna avtal är kända och följs
- att krishanteringsförmågan upprätthålls
- att alla investeringar både i form av information och teknisk utrustning har skydd i tillräcklig grad
- att det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- att hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet fortlöpande analyseras och hanteras
- att händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs
- att årliga mål för informationssäkerhetsarbetet beslutas gemensamt i kommunens IT-råd, och beskrivs i *Informationssäkerhetsobjektets* förvaltningsplan (PM3).

För de årliga målen anges:

- vad som ska göras under året och hur
- tidplan
- behov av personella och ekonomiska resurser
- när och hur uppföljning, utvärdering och avrapportering ska ske
- när och hur våra medarbetare ska informeras och utbildas.

5. Roller och ansvar

Informationssäkerhetsansvarig: Har det operativa ansvaret för samordning av informationssäkerhetsarbetet. (Tills vidare ligger detta ansvar på IT-chef)

Systemägare: Ansvarar för att det/de informationssystem denne har ägandeskap för, uppfyller de krav på informationssäkerhet som Östhammars kommun ställer.

Systemförvaltare: Ansvarar för den dagliga användningen av informationssystemen.

IT-chef: ansvarar för att uppfylla kommunens kontinuitetsplan för IT-stödet.

Beskrivning av roller och ansvar framgår av **Informationssäkerhetsinstruktion - Förvaltning**

6. Generella krav

6.1. Kommunens informationssystem

Samtliga informationssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare. Alla informationssystem ska minst klara den basnivå för informationssäkerhet som Östhammars kommun beslutat.

Vissa informationssystem är en förutsättning för att kunna bedriva vår verksamhet. För dessa ska en riskanalys upprättas med stöd av kommunens verktyg för analys av informationssäkerhet. Analysen ska utgöra underlag för driftgodkännande.

6.2. Informationssäkerhetsutbildning

All personal ska regelbundet få den utbildning som behövs för att informationssäkerheten ska upprätthållas.

6.3. Informationsklassning

Information som hanteras inom Östhammars kommun ska klassificeras med avseende på sekretess, riktighet och tillgänglighet enligt framtagen klassningsmodell.

6.4. Distansarbete

För att personalen ska kunna arbeta effektivt ska möjlighet finnas att arbeta mobilt eller stationärt på distans. Förutsättningar och restriktioner för detta ska dokumenteras.

6.5. Användning av Internet

Vid användning av Internet exponeras kommunens namn. Bland annat av detta skäl är det därför av vikt att lägga restriktioner på vilka hemsidor som får besökas. Hemsidor med exempelvis rasistiskt, våldsinriktat eller sexuellt innehåll får inte besökas. Undantag från detta kan beviljas av chef om informationen på sådana sidor kan ha relevans för arbetsuppgifterna.

6.6. E-post

Vid användning av e-post gäller samma lagar och regler som för pappershandlingar när det gäller vad som är allmän handling samt registrering, diarieföring och arkivering.

Enligt Tryckfrihetsförordningen är en handling allmän om den är inkommen till eller upprättad hos kommunen. Inkorgens register över inkomna e-postmeddelanden räknas också som allmän handling.

Känslig och/eller sekretessbelagd information får endast skickas som säker e-post.

6.7. Kontinuitetsplanering

Kontinuitetsplaneringen är av central betydelse för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. En kontinuitetsplan ska finnas för driften av IT-verksamheten baserad på de olika informationssystemens samlade krav och vara integrerade med Östhammars kommuns gemensamma kontinuitetsplan.

7. Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att:

- Beslutade åtgärder är genomförda
- Årliga mål är uppfyllda
- Regler och riktlinjer efterföljs
- Policy, säkerhetsinstruktioner och riskanalyser vid behov revideras.