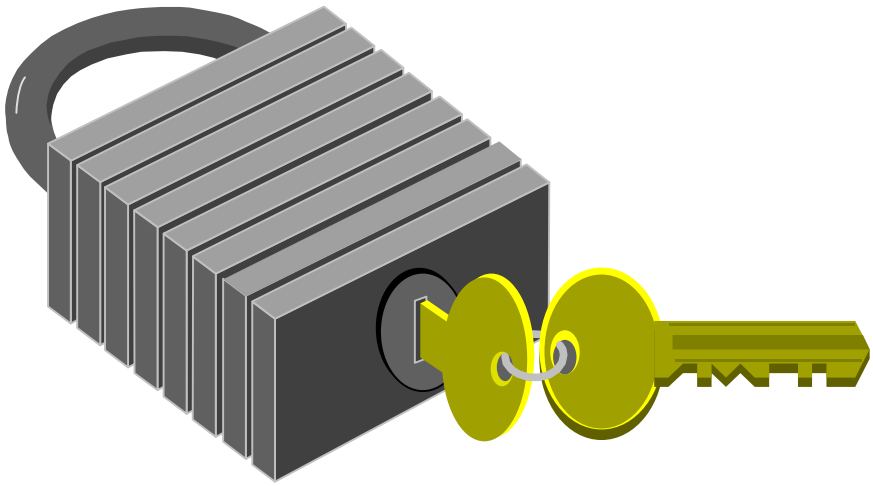
ÅRJÄNGS KOMMUNS INFORMATIONSSÄKERHETS-POLICY

(Bilaga 1)

Antagen av kommunens ledningsgrupp 2010-10-18



Innehåll

1. Informationssäkerhetspolicyns roll i informationssäkerhetsarbetet

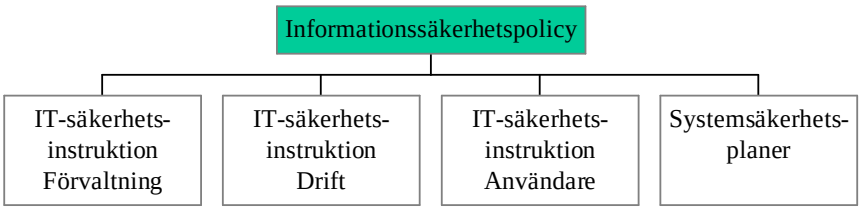
Informationssäkerhet är en del av kommunens lednings- och kvalitetsprocess som ska bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. Krisberedskapsmyndighetens rekommendationer om basnivå för Informationssäkerhet (BITS) ska gälla som ramverk för informationssäkerhetsarbetet.

Denna informationssäkerhetspolicy är en del av kommunens IT-verksamhet och redovisar kommunledningens viljeinriktning och stöd för informationssäkerhetsarbetet och syftar till att klarlägga:

- mål för Informationssäkerhetsarbetet
- organisation, ansvar och roller inom Informationssäkerhetsarbetet
- riktlinjer för områden av särskild betydelse

Policyn konkretiseras i Informationssäkerhetsinstruktionerna Förvaltning, Drift respektive Användare samt i systemsäkerhetsplaner.

Styrande dokument för Informationssäkerheten är:



Informationssäkerhetspolicyn fastställs av kommunfullmäktige. Instruktionerna för Förvaltning, Drift och Användare fastställs av kommunchefen. Systemsäkerhetsplanerna fastställs av respektive systemägare.

2. Mål för Informationssäkerhetsarbetet

2.1 Långsiktiga mål

För kommunens Informationssäkerhetsarbete ska gälla att:

- lagar och föreskrifter följs
- det stöder kommunens samlade utvecklingsarbete
- det förebygger oväntade händelser i IT-systemen som kan leda till negativa konsekvenser

- det säkrar en effektiv informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande partners, andra organisationer och tredje man
- alla investeringar både i form av information (data) och teknisk utrustning skall skyddas i tillräcklig grad
- kommunens information skall ses som en tillgång och skyddas i förhållande till dess värde
- all personal ska ges kunskap om gällande Informationssäkerhetsregler
- det skall finnas tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- hotbilden för varje enskilt samhällsviktigt/verksamhetskritiskt IT-system analyseras fortlöpande
- samtliga IT-system som finns inom kommunen ska vara identifierade och uppfylla basnivån för Informationssäkerhet enligt BITS
- för de samhällsviktiga IT-systemen ska en systemsäkerhetsplan vara upprättad i enlighet med KBM:s säkerhetsguide. Planen ska utgöra underlag för systemägarens beslut om driftgodkännande
- kostnaderna för säkerhetsåtgärder skall vara rimliga i förhållande till riskerna

De långsiktiga målen skall säkerställa att kommunen kan tillhandahålla relevant information som:

- är riktig, komplett och aktuell
- efterfrågas och som kommunen har ett ansvar att tillhandahålla och bevara
- säkerställer kommunens skyldigheter enligt offentlighetsprincipen
- endast delges behöriga personer enligt bestämmelserna om sekretess

2.2 Årliga mål och aktiviteter

Informationssäkerhetsarbetet ska bedrivas så att det blir en integrerad del av kommunens normala verksamhet. **Årliga mål** för arbetet skall därför beslutas och framgå av verksamhetsplanering och budget.

För de årliga målen bör anges:

- vad som ska göras under året
- behov av resurser för arbetet, såväl personella som ekonomiska
- tidplan för arbetet
- tidpunkt och former för uppföljning, utvärdering och avrapportering
- information och utbildning till medarbetare

3. Organisation, roller och ansvar

3.1 Övergripande ansvar

Det övergripande ansvaret för säkerheten i Årjängs kommuns IT-verksamhet vilar på kommunchefen.

3.2 Roller och ansvar

Organisation, roller och fördelning av ansvar ska säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla Informationssäkerhetspolicyns mål. Detta innebär att ett IT-system med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial mm.

Samtliga informationssystem ska vara identifierade, förtecknade och det ska finnas av kommunstyrelsen utsedd systemägare för varje system. Kommunens system ska klara den basnivå för informationssäkerhet som KBM:s rekommendationer beskriver. För de samhällsviktiga informationssystemen ska en systemsäkerhetsplan vara upprättad i enlighet med KBM:s ”Basnivå för informationssäkerhet (BITS)”.

Den interna organisationen för Informationssäkerhetsarbetet, roller och fördelning av ansvar framgår av Informationssäkerhetsinstruktion Förvaltning.

4. Särskilda rutiner

Vissa områden inom området informationssäkerhet är av särskild betydelse för kommunens verksamhet. Av informationssäkerhetsinstruktionerna ska bl.a. nedanstående områden och de särskilda riktlinjer, regler och rutiner som gäller för dessa framgå enligt följande:

- Informationssäkerhetsinstruktion Förvaltning:

- Behörighetsadministration
- E-postadresser
- Loggning och spårbarhet
- Införande, utveckling och avveckling av IT-system
- Drift
- Incidenthantering
- Konsulters åtkomst till kommunens nätverk

- Informationssäkerhetsinstruktion Användare:

- Informationsklassning

- Användarens ansvar
- Behörighet och lösenord
- Arbetsplatsen
- Distansarbete
- E-post
- Internet
- Virus m.m.
- Avslutning av anställning
- Efterlevnad av instruktionen

- Informationssäkerhetsinstruktion Kontinuitet & Drift:

- System- och driftdokumentationer
- Driftsgodkännande
- Kontinuitetsplanering
- Förvaring av datamedia
- Bemanning
- Tillträdes- och brandskydd
- Elförsörjning
- Regler för säkerhetskopiering och förvaring av datamedia.

5. Kontinuitetsplanering

Av kommunens systemsäkerhetsplaner ska framgå de enskilda IT-systemens krav på avbrotts- och katastrofplanering. Kraven ska vara sammanställda i systemsäkerhetsplanen för den tekniska infrastrukturen. Se Informationssäkerhetsinstruktion Förvaltning.

6. Driftgodkännande av IT-system

Före systemägarens beslut om driftgodkännande ska en granskning göras för att kontrollera att säkerheten är tillgodosedd enligt kraven i systemsäkerhetsplanen. Beslutet dokumenteras i systemsäkerhetsplanen. Se Informationssäkerhetsinstruktion Förvaltning

7. Revidering och uppföljning

Policy, säkerhetsinstruktioner och systemsäkerhetsplaner ska löpande följas upp och vid behov revideras. Se Informationssäkerhetsinstruktion Förvaltning.