Informationssäkerhetspolicy

För att trygga stadens informationstillgångar ska användandet av stadens information ske kontrollerat. En förutsättning för detta är att varje IT-användare känner till de krav som ställs.

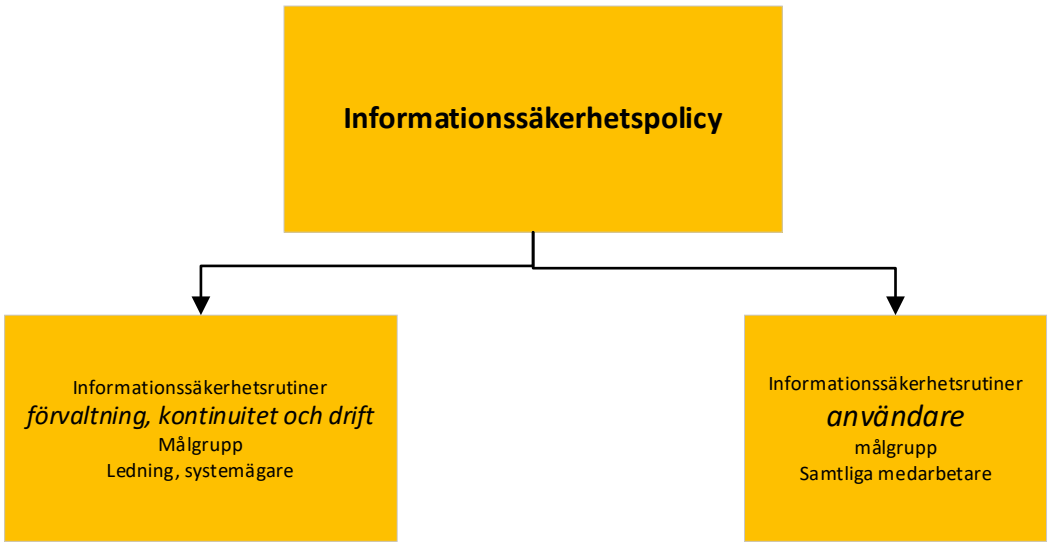
Stadens policy är att varje verksamhet ska ansvara för att informationen inom den egna verksamheten hanteras på ett tillförlitligt sätt. Policyn utgör stadens viljeyttring för att hantera stadens information på ett säkert sätt.

Denna informationssäkerhetspolicy är till för anställda och förtroendevalda i Mariehamns stad.

I denna policy inbegrips alla delar av stadens verksamheter och alla de informationstillgångar som staden äger eller hanterar.

Policyns roll i informationssäkerhetsarbetet

Informationssäkerhetspolicyn redovisar stadens viljeinriktning och mål för informationssäkerhetsarbetet. Policyn konkretiseras i informationssäkerhetsrutiner enligt nedan.



Allmänt om informationssäkerhet

Information är en av stadens viktigaste tillgångar och hanteringen av den är viktigt och en naturlig del i verksamheternas dagliga arbete. All information som staden hanterar bör vara korrekt och behöver vara tillgänglig när den behövs. Känslig information ska skyddas på rätt sätt och vid rätt tillfälle för att staden ska kunna fullgöra sitt uppdrag på ett förtroendeingivande sätt. Informationssäkerhetsarbetet ska vara långsiktigt och kontinuerligt och ska skydda stadens, invånares och användarnas information.

Mariehamns stad är beroende av information för att kunna utföra sitt uppdrag. Information kan till exempel vara text, ljud, bild, film och tal och kan förekomma i många olika former såsom tryckt eller skrivet, analogt eller digitalt, lagrat på lagringsmedia, överföras via e-post, yttras i konversationer och vara en del av någons kunskap. Personuppgifter är skyddsvärd information och vanligt förekommande.

Informationssäkerhet handlar om att skydda information så att

- Informationen alltid finns när staden behöver den (tillgänglighet)
- Informationen är korrekt och inte manipulerad eller förstörd (riktighet)
- Informationen finns tillgänglig för rätt person vid rätt tillfälle (konfidentialitet)

Strategiska mål med informationssäkerhet

Mariehamns stad bedriver långsiktigt och systematiskt informationssäkerhetsarbete och utgår från riktlinjer för etablerad standard för informationssäkerhet (ISO 27 000 serien). Informationssäkerhet är en grundförutsättning för att uppnå kvalitet och effektivitet i verksamheten.

Framgångsfaktorer

Avgörande för informationssäkerhetsarbetet är att:

- Att användare och förtroendevalda har kunskap om vilka krav som gäller
- Stadens information skyddas på en lämplig administrativ och teknisk nivå, utifrån genomförd informationssäkerhetsklassificering och riskanalyser
- Informationssäkerhetsincidenter ska följas upp och förebyggas
- Det ska finnas en gemensam, säker och väldefinierad infrastruktur för extern och intern kommunikation
- Fortlöpande riskanalyser görs för informationssystem med hög klassningsnivå
- Struktur och beredskap finns avseende informationssäkerheten
- Informationens kontinuitet garanteras med hjälp av en planerad livscykelhantering av stadens informationssystem
- Årlig översyn genomförs och ska framgå i verksamhetsplaneringen.

Uppföljning och efterlevnad

Mariehamns stad ska följa upp informationssäkerhetsarbetet genom att rapportera incidenter, åtgärda informationssäkerhetsbrister samt rapportera förekommande fall till Datainspektionen. Efterlevnaden av informationssäkerhetspolicyn ska följas upp via en revision inför upprättandet av databokslutet. Förbättringsarbeten ska ske löpande.

Organisation och roller

Mariehamns stad fastställer informationssäkerhetspolicyn.

Stadsdirektören har det övergripande ansvaret för informationssäkerheten och ser till att det finns en tydlig ansvarsfördelning för att upprätthålla säkerheten.

Systemägare är den som har ansvaret för aktuellt informationssystem. Systemägaren bestämmer ändamålen för behandlingen och hanteringen av informationen, svarar för att

informationen är autentisk och tillförlitlig samt för hur den delas och hur länge den ska vara tillgänglig. Systemägaren ansvarar för att registerbeskrivningar finns och hålls uppdaterade samt ansvarar för att riskanalyser upprättas.

Systemförvaltare är systemets avancerade användare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Dataskyddsombudets roll är att regelbundet utbilda, rådgöra och granska nämndernas informationssäkerhet kopplat till dataskyddsförordningen.

Informationssäkerhetsansvarig ska på uppdrag av stadsdirektören förvalta policy och riktlinjer för informationssäkerheten samt att utbildningsmaterial för informationssäkerhet finns tillgängligt.

IT- ansvarig har det operativa ansvaret för att uppfylla de krav som verksamheterna ställer på den tekniska IT-infrastrukturen samt för den tekniska IT-säkerheten.

Användare inom Mariehamns stad ansvarar för att följa fastställda informationssäkerhetsrutiner och policy.

Informationssystem och informationsklassning

Samtliga informationssystem ska vara förtecknade och klassificerade i stadens Klassa-plattform. För verksamhetskritiska system ska en riskanalys upprättas. Klassificeringen och en eventuell riskanalys utförs av systemägaren i samråd med IT. Alla system ska minst klara den basnivå för informationssäkerhet som staden har fastställt.

Information som hanteras av stadens IT-system ska klassificeras och nivåsättas enligt sekretess, riktighet och tillgänglighet. Nivåerna avgör om systemet behöver hög eller låg skyddsnivå.

Tabell för informationssäkerhetklassning

Säkerhetsaspekt (Konsekvensnivåer)	Skyddsvärde	Riktighet	Tillgänglighet
Kravnivå (1 – 4)			
Mycket hög (4)	Information som är sekretessbelagd och inte får röjas	Information som: Enligt lagkrav ska säkras mot förändring eller förstörning. Av andra skäl än lagkrav inte får vara felaktiga	Information som ska vara åtkomlig inom högst 2 timmar.
Hög (3)	Information som kan medföra allvarliga negativa konsekvenser för staden, stadens verksamheter eller för enskild person om den röjs.	Information som kan medföra allvarliga negativa konsekvenser för staden, stadens verksamheter eller enskild person om den röjs.	Information som ska vara tillgänglig inom högst 4 timmar.
Medel (2)	Information som kan ge negativa konsekvenser för staden, stadens verksamheter eller för enskild person om den röjs.	Information som kan ge negativa konsekvenser för staden, stadens verksamheter eller enskild person om den röjs.	Information som ska vara tillgänglig inom högst 1 dygn
Basnivå (1)	Information orsakar inte negativa konsekvenser för staden, stadens verksamheter eller för enskild person om den röjs.	Information som kan ge försumbar negativa konsekvenser för staden, stadens verksamheter eller enskild person om den röjs.	Information som ska vara tillgänglig inom högst en vecka.

Informationssäkerhetsutbildning

Personal som behövs ska genomgå den utbildning som behövs för att informationssäkerheten ska upprätthållas.

Distansarbete

Regler för distansarbete finns på stadens Intranät och beskriver vad användare bör tänka på när arbete utförs på distans.

Säker e-post

Sekretessbelagd information och känsliga personuppgifter till externa parter ska skickas via stadens anvisade lösning för säker e-post. Tillgången till lösningen beställs av systemägaren.

Kontinuitetsplan

Kontinuitetsplan ska finns för stadens verksamhetskritiska system. Den beskriver hur verksamheten ska agera vid ett oförutsett driftsavbrott, återställa och uppta verksamheten.

Revidering och uppföljning

Uppföljning är en viktig och avgörande del i informationssäkerhetsarbetet för att bevaka att

- Beslutade förbättringsåtgärder är genomförda
- Regler följs
- Att policy, informationssäkerhetsinstruktioner och riskanalyser vid behov revideras

Relaterade stöddokument

Dokumentnamn
Stadens IT-användaravtal
Stadens policy för distansarbete
Stadens informationssäkerhetspolicy
Stadens informationssäkerhetsrutiner (1,2)
Informationsklassningens resultat