Ystads kommun

Informationssäkerhetspolicy för Ystads kommun F 17:01

Dokumentet gäller för: Ystads kommuns nämnder, kommunala bolag och kommunala förbund	Gäller fr.o.m. - t.o.m. 2017-08-01-tillsvidare	Fastställd av: Kommunfullmäktige 2017-06-14 § 102 Ersätter:	För revidering ansvarar: Kommunfullmäktige
Ärendenummer: Ks 2017/147	Ansvarig för uppdatering: IT-avdelningen, IT-chef		Tillhör Ystads kfs: Reglementen

Ystads kommun

Innehåll

Ystads kommun

Inledning

Ystads kommuns verksamhet är grundad på principer om öppenhet, personlig integritet och respekt för individen. Medborgarna ska kunna få insyn i kommunens verksamhet. De ska kunna förlita sig på att den information som kommunen lämnar samt samlar in får ett tillräckligt skydd.

Information är en av kommunens mest strategiska resurser. Alla verksamheter är beroende av tillförlitlig information. Avbrott i tillgången till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser inom hälso- och sjukvården och inom kommunens övriga ansvarsområden.

Utvecklingen med informationshantering i IT-system och nya funktionaliteter innebär förbättringar i många avseenden. Samtidigt innebär beroendet av informationssystem att sårbarheten och riskexponeringen ökar om inte säkerhetsaspekterna beaktas.

Därför arbetar Ystads kommun aktivt med informationssäkerhet. Det innebär att se till att informationstillgångar finns tillgängliga när de behövs, att de är korrekta, och att obehöriga inte får åtkomst till dem. Genom att arbeta systematiskt och långsiktigt upprätthåller vi ett tillräckligt skydd som är anpassat efter våra verksamheters förutsättningar och behov.

Informationssäkerhetsarbetet syftar till att stödja och säkerställa kommunens verksamhet. Alla medarbetare deltar i detta arbete. Informationssäkerhetsarbetet är en viktig del i kommunens övergripande arbete med intern styrning och kontroll samt riskhantering.

Denna policy beskriver de övergripande principer som ska gälla för informationssäkerhetsarbetet i Ystads kommun.

Mål

Målet för kommunens informationssäkerhetsarbete är att skydda informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för verksamheterna att uppnå sina mål.

God informationssäkerhet främjar verksamheternas funktionalitet, kvalitet och effektivitet, medborgares rättigheter och personliga integritet, förmågan att förebygga och hantera allvarliga störningar och kriser samt förtroendet för kommunens informationshantering och IT-system.

Omfattning

Informationssäkerhetspolicyn gäller för hantering av information i alla dess former i Ystads kommun, inklusive bolag och förbund och av samtliga som arbetar på uppdrag av kommunen. Det sistnämnda regleras genom avtal.

Informationssäkerhetsarbetet styrs utifrån organisationens verksamhetskrav samt gällande lagar och föreskrifter.

Regelverket består av styrande dokument som på övergripande nivå utgörs av denna policy, tillhörande riktlinjer och rutinbeskrivningar. Allt informationssäkerhetsarbete i kommunen utgår från dessa dokument.

Ystads kommun

Respektive nämnd, styrelse och bolag styr sitt informationssäkerhetsarbete inom dess verksamhetsområde genom nödvändiga processer och rutiner som behövs för att säkerställa att verksamheten uppfyller kraven på en ändamålsenlig informationssäkerhet. De styrande dokumenten på lokal nivå utformas utifrån de övergripande.

Utöver detta krävs att Ystads kommun i tillämpliga delar lever upp till gällande lagar och förordningar samt till kommunens övriga styrande dokument.

Innebörd

Informationssäkerhetsarbetet innebär att värdera all information efter sin känslighet och med hjälp av administrativa och tekniska skyddsåtgärder säkerställa att den finns tillgänglig när den behövs, att den är korrekt och att obehöriga inte kan få tillgång till den. Utöver dessa säkerhetsaspekter måste behov av spårbarhet uppfyllas – att i efterhand kunna avgöra vem som tagit del av informationen, vilka förändringar som skett och av vem dessa utförts.

Säkerhetsaspekter

Konfidentialitet (rätt person): Information får inte göras tillgänglig eller avslöjas på ett sådant sätt att den personliga integriteten eller sekretessen hotas.

Riktighet (rätt information): Informationen får inte förändras eller gå förlorad, av misstag, genom inverkan av obehörig eller på grund av tekniskt fel.

Tillgänglighet (rätt tid och plats): Informationen ska kunna användas i förväntad utsträckning, inom önskad tid och på rätt plats.

Spårbarhet: Händelser i informationsbehandlingen ska kunna spåras.

Skyddet av informationstillgångar och informationssystem ska vara utformat så att verksamhetens krav på dessa säkerhetsaspekter uppfylls. Detta gäller även när kommunens information eller informationssystem hanteras av extern part.

Skyddsåtgärder

För att hitta relevant skyddsnivå utifrån dessa fyra aspekter ska vi arbeta utifrån nedanstående principer:

- Vi ska arbeta med informationsklassificering där all information klassificeras samt att handlingar och dokument märks.

- All information ska ha en ägare. Informationsägaren ansvarar för att klassificera informationen och ställa de säkerhetskrav som krävs för informationshantering.

- Alla informationssystem ska ha en systemägare som ansvarar för att säkerhetskraven på systemet uppfylls.

Ystads kommun

- Omvärlden förändras. Därför ska vi, utifrån återkommande risk- och sårbarhetsanalyser och inträffade incidenter, vidta nödvändiga åtgärder för att se till att vår information har rätt skydd.

- Vi ska ställa säkerhetskrav inför upphandling, utveckling, användning och avveckling av informationssystem och vi ska följa upp de krav vi ställt.

- Vi ska arbeta med kontinuitetsplanering och ha beredskap för avbrott. Våra kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av katastrofsituationer, störningar och avbrott.

- Alla anställda ska veta vad det egna ansvaret omfattar och ha god kunskap om vilka säkerhetsregler som gäller. Detsamma gäller när tillfällig eller extern personal anlitas.

- Det är viktigt att alla har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka informationssäkerheten.

- Skyddsåtgärder skall vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en alltför liten säkerhet kan medföra.

- Kontinuerlig uppföljning ska ske mot fastställda regler.

Ansvar

Kommunfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för kommunen.

Kommunstyrelsen ansvarar för att kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerheten utarbetas och hålls aktuella. Kommunstyrelsen ansvarar också för samordningen av informationssäkerhetsarbetet i kommunen och ska därför årligen fastställa en övergripande handlingsplan för informationssäkerhetsarbetet.

Kommundirektören har kommunstyrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt. Kommundirektören ansvarar för att övergripande tillämpnings-anvisningar utarbetas och hålls aktuella i enlighet med policy och riktlinjer.

Informationssäkerhetsansvarig verkställer samordningen av informationssäkerhetsarbetet inom kommunen och förvaltar denna policy, de tillhörande riktlinjerna och tillämpningsanvisningarna samt den övergripande handlingsplanen för informationssäkerhet.

Varje nämnd och styrelse är ansvarig för informationssäkerheten inom sitt verksamhetsområde och ska därför i enlighet med tillämpningsanvisningar anta verksamhetsnära styrdokument för informationssäkerhet.
Det åligger även varje nämnd och styrelse att årligen planlägga och löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Ystads kommun

Förvaltningschef/VD ska säkerställa att all informationshantering inom den egna verksamheten sker i enlighet med denna policy samt tillhörande riktlinjer och tillämpningsanvisningar för informationssäkerhet.

Informationssäkerhetssamordnare ska utses inom varje förvaltning och bolag och ges i ansvar att samordna och följa upp det för organisationen och verksamheten gemensamma informationssäkerhetsarbetet.

Varje anställd ansvarar för att uppställda säkerhetsregler följs samt att störningar och fel i informationssystem, utrustningar och informationsinnehåll rapporteras enligt fastställda rutiner.

Informationssäkerhetsrådets uppgift är att främja, stödja, samordna och följa upp kommunens informationssäkerhetsarbete på en övergripande nivå.

Uppföljning och revidering

Uppföljning och revidering av denna policy ska ske regelbundet. I samband med revidering ska tillhörande riktlinjer och tillämpningsanvisningar samt handlingsplanen för informationssäkerhet revideras på motsvarande sätt.