Informationssäkerhetspolicy

Dokumentnamn	Dokumenttyp	Fastställd/upprättad	Beslutsinstans
Informationssäkerhetspolicy	Policy	2013-11-11	KF
Dokumentansvarig	**Diarienummer**		**Giltig till**
IT-chef	KS.2013.182		Tillsvidare
Dokumentinformation		**Dokumentet gäller för**	
		Samtliga nämnder i Gnesta kommun	

Innehåll

Revisionshistoria

Upprättad 20130826

Definitioner

BITS

Basnivå för Informationssäkerhet

DISA

Datorstödd informationssäkerhetsutbildning för användare

Informationssystem

Avser alla processer och system som innehåller information.

Information

Avser det innehåll eller de meddelanden som överförs vid kommunikation, oberoende av i vilken form eller miljö den förekommer.
Information finns exempelvis tryckt på papper, lagrad elektroniskt, överförs med post, e-post eller via integrationer samt visas på film eller nämns i ett samtal.

Kommunikation

Avser överföring av information mellan människor eller apparater.

Informationssäkerhet

Med informationssäkerhet avses att:

rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt
det är möjligt att spåra vem som tagit del av högt säkerhetsklassad information
informationen är och förblir riktig

Omfattning

Vad omfattas

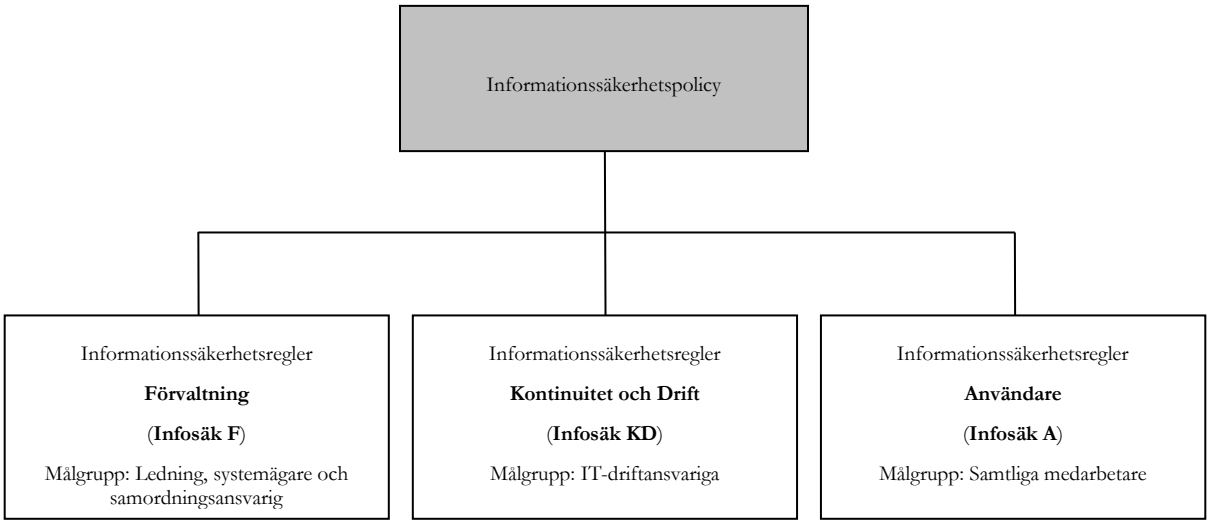
Informationssäkerheten omfattar kommunens alla informationstillgångar som finns i kommunens besittning. Exempel på informationstillgångar kan vara:

Information som finns i datorer eller på servrar
Information som skickas med e-post, chatt eller liknande
Information som finns på mobila enheter. Typ telefoner och surfplattor
Information som finns lagrad på externt media. Typ USB-minne m.m.
Information som visas på webbsidor eller via sociala medier
Information som överförs muntligt via ett samtal med telefon, direkt eller annat media
Information som finns i skriftlig form på papper

Vem omfattas

Samtliga anställda, förtroendevalda, elever inom skola/förskola/vuxenutbildning och uppdragstagare som arbetar med kommunens information omfattas av informationssäkerhetspolicyn.

Policyns roll i informationssäkerhetsarbetet



Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet. Policyn konkretiseras i informationssäkerhetsregler. Policyn är framtagen enligt BITS-konceptet från Myndigheten för samhällsskydd och beredskap.

Informationssäkerhet är den del av kommunens lednings- och kvalitetsprocess som handlar om hur verksamheten hanterar information.

Informationssäkerhetspolicyn och särskilda informationssäkerhetsregler styr kommunens arbete kring informationssäkerhet

Allmänt om informationssäkerhet och IT

Information är en av Gnesta kommuns viktigaste tillgångar.

Utgångspunkter i kommunens säkerhets- och policyarbete inom informationsteknologi är:

- Lagar, förordningar och föreskrifter
- Krav uppsatta av Gnesta kommun
- Avtal
- Överenskommelse
- Öka effektiviteten genom rätt IT-stöd i förvaltningarna
- Ge bättre förutsättningar för ledning, styrning, uppföljning, utvärdering och resursfördelning

Hanteringen av informationen är en viktig del i risk- och sårbarhetsanalyser.

Överordnade chefer har rätt att, efter skriftlig begäran till IT-enheten få tillgång till information, inklusive e-post och hemkataloger.

Informationssäkerhet är en integrerad del av vår verksamhet. Samtliga chefer ansvarar för att all sin personal är väl insatta i informationssäkerhetspolicyn och efterlever denna. Alla som hanterar informationstillgångar ansvarar för att upprätthålla informationssäkerheten.

Samtliga som omfattas av denna policy ska vara uppmärksamma på, och rapportera händelser som kan påverka säkerheten för kommunens informationstillgångar. Rapportering ska ske till systemägaren som i sin tur rapporterar till informationssäkerhetssamordnaren inom organisationen.

Lokala avvikelser från denna policy inom organisationen är tillåtet, dock reglerar denna policy en miniminivå på informationssäkerheten.

Disciplinära åtgärder i enlighet med arbetsrätten eller motsvarande kan vidtas mot den som använder informationstillgångarna på ett sätt som strider mot informationssäkerhetspolicyn.

Mål

Att ha ett säkert informationsflöde med rätt skydd för informationen så att den är:

- Säkrad mot förlust
- Säkrad mot skada
- Säkrad mot sabotage
- Säkrad mot stöld
- Säkerhetsställd gällande riktighet
- Säkrad mot otillbörlig åtkomst

Dessa mål hanteras och följs upp i respektive verksamheters verksamhetsplan.

Ansvar

Kommunstyrelsen har det övergripande ansvaret för informationssäkerheten.

Informationssäkerhetssamordnaren har det operativa ansvaret för samordning av informationssäkerhetsarbetet.

Varje nämnd utser systemägare för informationssystem inom nämndens ansvarsområde.

Systemägare bör vara den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer. Systemägare utser även systemförvaltare för respektive informationssystem.

Beskrivning av roller och ansvar framgår av Infosäk F1.

Generella krav

Kommunens informationssystem

Samtliga informationssystem ska vara identifierade och förtecknade på central plats.

Informationssystem som är av vikt, viktigheten beslutas av systemägare, ska genomgå en riskanalys. Riskanalysen genomförs med stöd av kommunens verktyg för analys av informationssäkerhet (BITS Plus). Underlaget från riskanalysen ska ligga till grund för driftnivå av informationssystemen.

Informationssäkerhetsutbildning

All personal ska regelbundet genomgå utbildning i informationssäkerhet för att informationssäkerheten ska upprätthållas.

Informationsklassning

Information som hanteras på myndigheten ska klassificeras med avseende på sekretess, riktighet och tillgänglighet enligt kommunens klassningsmodell i Infosäk A2.

Internet

Förutsättningar och restriktioner för användandet av Internet dokumenteras i Säkerhetsinstruktion för användare.

E-post

Förutsättningar och restriktioner för användandet av e-post dokumenteras i Säkerhetsinstruktion för användare.

---

1 Informationssäkerhetsregler Förvaltning

2 Informationssäkerhetsregler för Användare.

Kontinuitetsplanering

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

Revidering

Revideringstid av informationssäkerhetspolicy och underdokument

Informationssäkerhetspolicyn ska revideras vid revidering av framtidsplanen
Informationssäkerhetsreglerna revideras vid behov eller vid förändringar i informationssäkerhetspolicyn som påverkar informationssäkerhetsreglerna.

Revideringsansvar

IT-chef är revisionsansvarig för informationssäkerhetspolicyn med underliggande dokument.

Beslutsinstans och referensgrupper

Informationssäkerhetspolicyn beslutas av Kommunfullmäktige, Informationssäkerhetsreglerna beslutas av IT-chef på delegation från kommunsfullmäktige.

Revidering och uppföljning

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

Beslutade åtgärder är genomförda
Årliga mål är uppfyllda
Policy följs
Att policy, säkerhetsinstruktioner och riskanalyser vid behov revideras

Referenser

Gnesta kommuns styrdokument och policys

http://insidan.gnesta.int/arkiv/styrdokument.4.380bcbd109b01945498000531.html