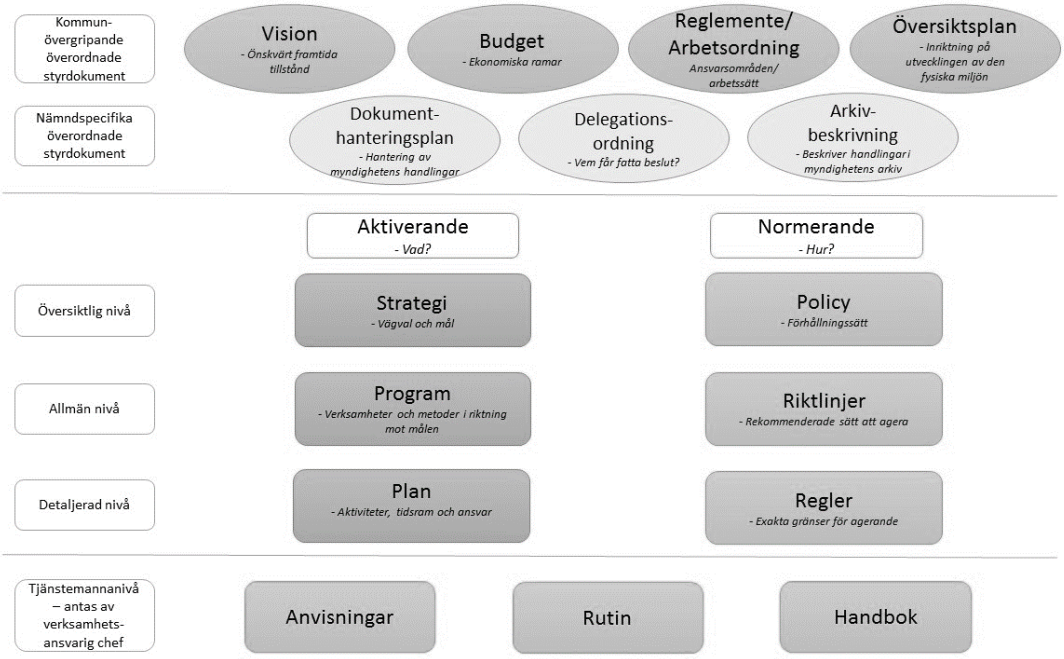
POLICY FÖR

Informationssäkerhet i Håbo kommun

HÅBO KOMMUN

Antaget av	Kommunfullmäktige
Antaget	2023-12-11, § 209
Giltighetstid	Tills vidare
Dokumentansvarig	Informationssäkerhetssamordnare

Håbo kommuns styrdokumentshierarki



Diarienummer	KS 2023/00864 nr 121646
Gäller för	Samtliga kommunala verksamheter och bolag.
Tidpunkt för aktualitetsprövning	2027-04-30

Relaterade styrdokument Policyn för informationssäkerhet kompletteras med *riktlinjer för informationssäkerhet.*

Inledning

Policy för informationssäkerhet i Håbo kommun är det övergripande styrdokument avseende kommunens informationssäkerhet. Policyn redovisar kommunens viljeinriktning och stöd för informationssäkerhetsarbetet och syftar till att klarlägga

- Varför informationssäkerhet är viktigt
- Mål och krav på informationssäkerhetsarbetet
- Organisation, ansvar och roller

Informationssäkerhetsarbetet är ett kommungemensamt ansvar som följer med verksamhetsansvaret. Alla anställda, politiker och extern personal omfattas av denna policy och har ansvar över att informationssäkerhetsbestämmelserna följs, förbättras och utvecklas.

Informationssäkerhetsarbetet ska ske kontinuerligt och främja en god informationssäkerhetskultur i hela Håbo kommun.

Policyn ska vara känd och tillgänglig i aktuell version på kommunens intranät och hemsida samt kommuniceras vid nyanställning.

Avtal och överenskommelser får inte skrivas som åsidosätter kraven i denna policy.

Syftet är att hantera och skydda kommunens information så att rättsliga och verksamhetsmässiga krav och mål på informationssäkerhet kan uppnås.

Informationssäkerhet

Informationssäkerhet ska förebygga att uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs. Informationssäkerhet ska också förebygga annan skadlig inverkan på uppgifter och informationssystem.

Informationssäkerhetsarbetet omfattar både administrativa och tekniska säkerhetsåtgärder. Dessa tre informationssäkerhetsaspekter ska ligga till grund för arbetet:

Konfidentialitet- att information inte tillgängliggörs eller röjs till obehöriga individer, enheter eller processer

Riktighet – egenskap hos information som innebär att informationen inte obehörigen, av misstag eller på grund av fel i system har förändrats.

Tillgänglighet – att informationen är nåbar när den behövs, i förväntad utsträckning och av rätt person.

1. Grundläggande mål för informationssäkerhetsarbetet

Medborgare och intressenters förtroende	• Informationssäkerhetsarbetet ska bidra till att medborgare och andra intressenter ska känna sig trygga vid informationsutbyte med kommunen och vår förmåga att hantera personuppgifter

Verksamhetens informationssäkerhet	• Informationssäkerhetsarbetet ska bedrivas systematiskt och utgå från den etablerade standardserien SS-ISO/IEC 27000. Målet är att införa ett ledningssystem för informationssäkerhet (LIS). • Arbetet ska innefatta mätbara uppföljningar enligt metodiken planera, genomföra, följa upp och åtgärda utifrån en årlig verksamhetsplan som följer verksamhetens övriga processer. • Samtliga anställda inom kommunens verksamhet ska ha kännedom och kunskap om aktuellt regelverk beträffande informationssäkerhet och ges möjlighet till grundläggande utbildning. • Grunden för ett systematiskt arbete ska resultera i en god informationssäkerhetskultur som är anpassad efter verksamhetens förutsättningar och behov. • Det systematiska informationssäkerhetsarbetet ska minst omfatta informationsklassificering, risk- och sårbarhetsanalys, incidenthantering, kontinuitetsplaner samt uppföljning, åtgärder och återkoppling. • Oväntade händelser i IT-systemen som kan leda till negativa konsekvenser ska minimeras och förebyggas. • Utifrån återkommande risk- och sårbarhetsanalyser och inträffade incidenter, ska nödvändiga åtgärder vidtas för att säkerställa att vår information har rätt skydd. Information ska skyddas utifrån sitt värde och de negativa konsekvenser en otillräcklig säkerhet kan komma att medföra.
Lag och författning	• Uppfylla de krav som ställs på informationssäkerheten i lagar, förordningar och föreskrifter. • Genom omvärldsbevakning säkerställa att vi följer informationssäkerhetskrav i system och verksamhet.
Krishantering	• Genom ett förebyggande och proaktivt informationssäkerhetsarbete ha en god förmåga att kunna upprätthålla våra kritiska verksamheter på för kommunen acceptabel nivå då incidenter, allvarliga störningar och kriser inträffar. Arbetet ska dokumenteras så att förbättringsåtgärder kan säkerställas.

Uppföljning	• Kommunstyrelsen/ledningen ska minst en gång per år informera sig om hur arbetet med informationssäkerhetsarbetet går.

2. Roller och ansvar

Nedan anges några övergripande roller som beslutar kring informationssäkerhet i kommunen. För att ta del av övriga roller och ansvarområden på detaljnivå läs *Riktlinjer för informationssäkerhet.*

2.1. Kommunfullmäktige

- Beslutar om Informationssäkerhetspolicy för Håbo kommun.

2.2. Kommunstyrelsen

- Beslutar om *Riktlinjer för informationssäkerhet*.

- Har det yttersta ansvaret för att informationssäkerhetsarbetet bedrivs, utvecklas och samordnas enligt kommunens Informationssäkerhetspolicy.

- Ska tillse att verksamheterna och ledningen erhåller funktioner, resurser och befogenheter för att kunna bedriva ett systematiskt och kontinuerligt informationssäkerhetsarbete.

- Ska informera sig om status på organisationens informationssäkerhetsarbete.

2.3. Kommundirektören

- Har det övergripande operativa ansvaret för informationssäkerheten.

2.4. Nämnder och bolagsstyrelser

- Vidtar de åtgärder som krävs för att upprätthålla en robust, säker och tillförlitlig informationshantering och tillser att policyn med riktlinjer följs.

2.5. Förvaltningschefer och Verksamhetsansvariga

- Ska planera, upprätta, följa upp och arbeta efter verksamhetsnära rutiner för informationssäkerhet inom det egna verksamhetsområdet. Verksamheterna själva har ansvar för att klassificera och värdera sin information.

- Ska utse informationsägare och tillse att medarbetare har tillräcklig kunskap om informationssäkerhet inom sitt verksamhetsområde.

3. Definition

Informationstillgång - Information och informationsbehandlande resurser som är av värde för en organisation. Informationstillgångar kan vara av fysisk eller logisk karaktär, eller bådadera. Till exempel: Information, datorer, tjänster, programvaror och personalen och dess kompetens.

Ledningssystem för informationssäkerhet - Del av organisationens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta,

införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet

Informationssystem - System som används för att samla in, lagra bearbeta och distribuera information för ett givet ändamål.

Informationsklassificering- Informationsklassificering är en metod som hjälper verksamheten att välja rätt åtgärder för att skydda information utifrån sitt värde.

Informationsägare - Roll som innebär ett utpekat ansvar för information inom ett eller flera verksamhetsområden och hanteras inom den egna verksamheten.