



Informationssäkerhetspolicy

Dokumentnamn Informationssäkerhetspolicy		Dokumenttyp Policy	Omfattning Koncernövergripande
Dokumentägare Kommundirektör/vd Ludvika kommun stadshus AB	Dokumentansvarig Säkerhetschef	Publicering Intranät	
Författningsstöd			
Beslutad 2024-05-13, § 61	Bör revideras senast 2027	Beslutsinstans Fullmäktige	Diarienummer KS2023/328
Beslutade revideringar	Vad revideringen avsett		Diarienummer vid revideringen

Styrdokumentstyper i Ludvika kommun

Utöver styrdokumentstyperna nedan finns det i Ludvika kommun lagbundna styrdokument som inte följer denna terminologi. Namn och beslutsinstans för de styrdokument som styrs istället av gällande lagstiftning.

Dokumenttyp	Definition	Beslutas av	Giltighet	Uppföljning
Policy	Anger kommunens förhållningssätt till något. Långsiktig och övergripande.	Kommunfullmäktige	Tillsvidare	Minst en gång per mandatperiod
Strategi	Hjälper att göra vägval och prioriteringar. Kan innehålla mål och uppdrag.	Kommunstyrelsen eller respektive nämnd	Tillsvidare	Minst en gång per mandatperiod
Riktlinjer	Innehåller konkreta beskrivningar av vad som ska göras och hur det ska göras.	Kommunstyrelsen eller respektive nämnd	Tillsvidare eller beslutad period	Minst en gång per mandatperiod eller då riktlinjen upphör att gälla
Regler	Ska vara konkreta och sätta tydliga gränser.	Fullmäktige, kommunstyrelsen eller respektive nämnd	Tillsvidare eller beslutad period.	Minst en gång per mandatperiod eller då reglerna upphör att gälla

1 Inledning

Denna policy gäller för informationssäkerhetsarbetet i Ludvika kommun. Området informationssäkerhet omfattar hela organisationens verksamhet och all information, oavsett om den finns i digitala system eller på papper. Alla kommunens verksamheter, nämnder, styrelser, förtroendevalda och uppdragstagare omfattas av policyn.

Informationssäkerhetspolicyn är ett övergripande dokument som visar kommunens övergripande mål för informationssäkerhetsarbetet.

2 Informationssäkerhet

Information finns och hanteras i alla kommunens verksamheter och berör allt kommunen gör. Informationen rör exempelvis personal och deltagare i våra verksamheter, våra tjänster, vår ekonomi och det omgivande samhället med medborgare, företag och föreningar. Information blir därför en av våra viktigaste och känsligaste tillgångar.

En god informationssäkerhet handlar om att skapa och upprätthålla lämpligt och proportionerligt skydd av informationen i alla dess former. Det kan vara till exempel text, ljud, bild eller film. Skyddet ska upprätthållas oavsett hur informationen lagras, bearbetas eller kommuniceras.

Arbetet med informationssäkerhet ska därför harmonisera med gällande standarder fastställda av internationella standardiseringsorganet ISO. I förekommande fall kompletteras arbetet med instruktioner i enlighet med aktuell lagstiftning samt Myndigheten för samhällsskydd och beredskaps vägledningar.

Det är viktigt att belysa att informationssäkerhet inte begränsas till säkerhet i IT-system.

Informationssäkerhet ska ge skydd utifrån fyra grundprinciper:

- **Konfidentialitet**
Att informationen skyddas mot obehörig insyn.
- **Riktighet**
Att informationen skyddas mot oönskad förändring.
- **Tillgänglighet**
Att informationen finns tillgänglig när den behövs.
- **Spårbarhet**
Att viktiga händelser i systemen kan spåras vid tillfällen när andra delar i informationssäkerheten visar tecken på skadlig påverkan

3 Syfte

Policyn ska bidra till och vara grund för kommunens skydd mot förlust av information och oavsiktlig eller obehörig förändring av den. Syftet är också att säkra tillgängligheten av informationen för behöriga användare när den behövs.

4 Mål

Målen för ett aktivt och systematiskt informationssäkerhetsarbete är att:

- Upprätta och upprätthålla ett högt förtroende hos medborgarna samt skydda den personliga integriteten.
- Informationshanteringen ska vara förutsägbar, trygg och likformig i kommunens och bolagens verksamheter.
- Säkerställa att informationen har proportionerlig skyddsnivå och att rätt information finns tillgänglig för rätt person vid rätt tillfälle.
- Förhindra och minimera effekter av störningar och skador samt skydda informationen och system mot bedömda hot.
- All personal uppmärksammar och rapporterar händelser som kan påverka säkerheten för kommunens information.
- Vara ett stöd i effektivisering och utveckling av kommunens och bolagens digitalisering.
- Informationssäkerhet ska vara en integrerad del av det dagliga säkerhets- och arbetsmiljöarbetet.

5 Ansvar

Ansvar för ledning, samordning och utveckling av informationssäkerhetsarbetet ligger hos kommunstyrelsen. Respektive nämnd och styrelse är informationsägare inom eget verksamhetsområde.

Ansvar för informationssäkerhetsarbetet följer i grunden det ordinarie verksamhetsansvaret. Det gäller från ledning till enskild medarbetare.

Kommunens säkerhetsenhet och övriga som arbetar specifikt med säkerhet, IT-säkerhet eller andra relaterade frågor relaterade till informationssäkerhet fungerar som stöd till kommunens verksamheter att fullfölja ansvaret för informationssäkerheten.

Roller och ansvar beskrivs utförligt i riktlinjer för informationssäkerhet.

6 Uppföljning och förbättringar

Respektive nämnd eller styrelse ska följa upp informationssäkerhetsarbetet inom den egna verksamheten och identifiera, analysera och vid behov utföra åtgärder för att förbättra informationssäkerheten.

Säkerhetschef ska i syfte att förbättra ledningssystemet för informationssäkerhet i början av varje år, rapportera föregående års läge och status gällande informationssäkerhet till kommundirektören och kommunstyrelsen. Särskilda skäl som exempelvis allvarliga incidenter, brister eller behov kan motivera ytterligare rapporteringar.