



SVENLJUNGA
KOMMUN

policy

Säkerhetspolicy för IT och elektroniskt lagrad information

Beslutat av	Kommunstyrelsen
Beslutandedatum	2023-05-08, § 66
Ansvarig	IT-chef
Revideras	Vid behov
Följas upp	Årligen



Innehållsförteckning

Inledning	3
Mål för IT-säkerhetsarbete	3
Organisation, roller och ansvar	3
Övergripande ansvar	3
Roller och ansvar	4
IT-infrastukturägare – IT-chef	4
Driftansvarig – IT-driftsledare	4
Systemägare – förvaltningens ansvar	4
Särskilt prioriterade säkerhetsområden och ansvar	5

Inledning

IT-säkerhet är en viktig del i organisationens lednings-och kvalitetsprocess som bidrar till att IT-system används på ett korrekt vis och med avsedd funktionalitet. Policyn redovisar kommunens viljeinriktning och är ett stöd för IT:s säkerhetsarbete som ämnar tydliggöra:

- Mål för IT-säkerhetsarbete
- Ansvar och roller inom IT-säkerhetsområde
- Områden som är av särskild betydelse

Mål för IT-säkerhetsarbete

- Lagar och föreskrifter följs
- Verksamhetsutvecklingsarbetet stöds
- Krishanteringsförmågan säkerställs
- Förebygga oväntade händelser i IT-systemen som kan leda till negativa konsekvenser
- Säkra en effektiv informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- Investeringar som görs och gjorts både i form av information (data) och teknisk utrustning skyddas i tillräcklig grad
- Informationen (data) ses som en tillgång och skyddas i paritet med dess värde
- All personal, som använder IT som ett arbetsredskap, ges kunskap om gällande IT-säkerhetsregler
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- Hotbilden för varje enskilt samhällsviktig IT-system analyseras fortlöpande

Organisation, roller och ansvar

Övergripande ansvar

Det övergripande ansvaret för säkerheten i organisationens IT-verksamhet vilar på kommunstyrelsen. Detta är med förutsättning att systemet finns lokalt och inom kommunens nätverk. Gällande system som befinner sig utanför kommunens nät är det respektive nämnd som ansvarar för säkerheten. Detta kan nämnderna reglera

genom serviceavtal eller dylikt. Kansli och IT-enheten utgör i dessa fall som en rådgivande funktion.

Roller och ansvar

Organisation, roller och fördelning av ansvar ska säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla IT-säkerhetspolicyns mål. Detta innebär att ett IT-system med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial eller dylikt.

IT-infrastrukturägare – IT-chef

Infrastruktursägarens roll och ansvar är att säkerställa den långsiktiga tekniska utvecklingen, att säkerheten ligger på en tillräckligt god nivå och att befintliga lagar samt föreskrifter följs.

Driftansvarig – IT-driftsledare

Driftansvarig säkerställer drift av infrastrukturen och de system som finns internt i Svenljunga kommun. Driftansvarig tillsammans med systemförvaltare ansvarar för att den löpande driften upprätthålls enligt överenskommelse. Driftansvaret kan under vissa omständigheter vara delat.

Systemägare – förvaltningens ansvar

Systemägare bär ansvaret för planering, styrning av systemförvaltningsarbetet och budgeten. Ansvaret utgår från systemägare men kan också delegeras till andra roller inom organisationen. Driftansvaret kan vara delat mellan olika roller för samma IT-system, t.ex. så att IT-enheten har ansvaret för serverdriften och systemägaren har ansvar för systemdriften tillsammans med extern leverantör.

Systemförvaltare – förvaltningens ansvar

Systemförvaltaren ansvarar för det löpande arbetet kring IT-systemet. Systemförvaltare ska samordna användning och systemförvaltning av systemet och samverka med driftansvarig och systemägare för en säker och rationell drift av IT-systemet.

Respektive förvaltning ansvarar för att samtliga IT-system och program är identifierade och förtecknade.

Den interna organisationen för IT-säkerhetsarbetet, roller, fördelning av ansvar och arbetssätt framgår av rutin för digital systemförvaltning i Svenljunga kommun.

Särskilt prioriterade säkerhetsområden och ansvar

- Behörighetsadministration
 - Systemförvaltare i respektive förvaltning.
- Behörighetsbeställning
 - Chef ansvarar för beställning medan IT-enheten utför beställningen.
- Behörighetskontroll
 - Chef och systemförvaltare i respektive förvaltning.
- Loggning och sårbarhet
 - IT-enheten för centrala system i kommunen. I övrigt förvaltningen och verksamheters ansvar genom exempelvis avtal.
- Distansarbete
 - Chefer – tillser att medarbetare hanterar information på ett säkert vis i enlighet med den exponerande informationen som kan inhämtas på Medarbetarwebben.
- Drift- och förvaltning
 - Gällande driften är detta ett centralt ansvar såtillvida systemet finns inom kommun. Förvaltning av system åvilas ägare av systemet.
- Tillträdesskydd
 - IT ansvarar för tillträdesskydd.
- Säkerhetskopiering och lagring
 - För de system som finns lokalt i kommunen ansvarar IT för säkerhetskopiering och lagring.
- Avveckling av datamedia och datakommunikation

- IT ansvarar för säker destruktion i enlighet med BLANCO-standard för de av kommunen inhandlade enheter.
 - Systemägare ansvarar för att i upphandlingsförfarandet ha rådighet över destruktionsförfarandet.
- Informationsklassning
 - Förvaltningarna ansvarar för att informationsklassningar genomförs för varje system med stöd från centralt håll i form av digitaliseringsstrateg.
- Lagring samt e-post och användning av Internet
 - IT ansvarar för lagring av e-post samt användning av internet.
 - Den enskilda medarbetaren ansvarar för att informationen gallras i enlighet med vid var tid gällande lagar och styrdokument.
- Systemförvaltarplaner
 - Systemägare tillika förvaltning eller enhetschef ansvarar för att upprätta systemförvaltarplaner lämpligtvis genom systemförvaltare. Stöd från centralt håll genom digitaliseringsstrateg.