Finnvedens samordningsförbund

Informationssäkerhetspolicy

Följande policy har upprättats för Finnvedens Samordningsförbund (nedan kallat ”förbundet”). Policyn är fastställd av styrelsen den 2 september 2019.

MÅL OCH SYFTE

Det är förbundets mål att skydda information och vårt kontor mot hot och skapa ett effektivt skydd genom att säkerställa följande:

- ***Integritet***; Informationen ska skyddas så att den inte av misstag eller avsiktligt görs tillgänglig för obehöriga personer eller används på otillåtet sätt.
- ***Tillgänglighet;*** Informationen kommer att vara tillgänglig för behöriga användare enligt deras behov och förväntad form och i önskad utsträckning enligt säkerhetspolicyn.
- ***Noggrannhet***; Informationen måste vara korrekt i den meningen att den skyddas mot oavsiktlig eller avsiktlig korruption.
- ***Kunskap;*** Att policyn är välkänd och förståelig för anställda och att alla anställda och andra berörda har kännedom om informationssäkerhetsreglerna.
- ***Hot;*** Hot mot enskilda informationssystem som är viktiga för verksamheten analyseras kontinuerligt.
- ***Förebyggande;*** Regelbundna risk- och sårbarhetsbedömningar och motsvarande förbättringsåtgärder. Kontinuerlig förbättring av säkerhetsprocesser för att matcha förbundets behov.
- ***Användarvänlighet***; Att säkerhetsåtgärder är möjliga att utföra.
- ***Resurser;*** Medel behöver finnas som möjliggör den efterfrågade säkerhetsnivån

Syftet med en informationssäkerhetspolicy är att säkerställa att informationen inom förbundet och framförallt hanteringen av informationen sköts på bästa sätt, med de förutsättningar förbundet har. En del av detta är att utföra risk- och sårbarhetsanalyser för att minimera risken att information hanteras fel eller kommer i orätta händer.

Ansvar

Ledningen

Förbundets styrelse har övergripande ansvaret för informationssäkerheten. Förbundschef är IT-säkerhetsansvarig och ansvarar för säkerhetsdokument, metoder samt processer. Förbundschef ansvarar för att årligen revidera och se över säkerhetsarbetet samt lyfta till styrelsen om informationssäkerhetspolicyn behöver revideras.

Förbundschefens ansvar innebär att:

- Årligen upprätta en risk- och sårbarhetsanalys.
- Rapportera analysen till styrelsen på nästkommande möte.
- Undersöka och rapportera alla allvarliga säkerhetsincidenter.
- Stödja och ge råd till övriga berörda i frågor som rör IT-säkerhet.
- Ha god kunskap om säkerhetsbestämmelserna i den verksamhet förbundet har.

Anställda

Alla anställda är skyldiga att ta del av Informationssäkerhetspolicyn och följa förbundets säkerhetsinstruktioner.

Anställda ska rapportera problem, hot eller åtgärder som strider mot denna policy eller andra säkerhetsanvisningar.

Även processutvecklare i förbundet och externa konsulter måste följa förbundets Informationssäkerhetspolicy.

Så länge förbundet köper tjänster av Samordningsförbundet Södra Vätterbygden ska de berörda anställda även följa detta förbunds informationssäkerhetspolicy. Säkerhetsarbetet sker då parallellt för de båda förbunden.

Systembeskrivning och ansvar

Informationssystem

Vilka informationssystem som används i förbundet och vilka som har access/behörighet i dem skiftar över tid. Separat lista med informationssystem, behörigheter och riskanalys med kommentarer uppdateras löpande.

Användning av internet

Vid användning av internet exponeras förbundets namn. Risk finns också att virus kan angripa förbundets datorer om man medvetet eller av misstag kommunicerar med hemsidor som besöks. Bland annat av dessa skäl är det viktigt med restriktioner på vilka hemsidor som får besökas. Hemsidor med rasistiskt, våldsinriktat eller sexuellt innehåll får inte besökas.

E-post

Sekretessbelagd information eller information av känslig karaktär kopplat till enskild individ får inte skickas via e-post.

Regelbunden gallring av e-post görs i enlighet med förbundets ”Rutinbeskrivning Mejl”. Formell e-post sparas minst ett år, övrig e-post tre månader.

Foton och film

Foton eller film från aktiviteter i förbundet eller förbundsfinansierad verksamhet får bara publiceras med skriftligt samtycke från identifierbara personer. Foton på anställda i förbundet, styrelse och beredningsgrupp kan publiceras utifrån laglig grund Allmänt intresse.

Rapportering av incidenter

Incidenter vad gäller informationssäkerheten rapporteras till förbundschef.

Personuppgiftsincidenter enligt GDPR rapporteras i särskilt system, skapat för detta ändamål. Vidare rapportering till Datainspektionen sker i enlighet med lagstiftningen.

Jag intygar härmed att jag tagit del av denna Informationssäkerhetspolicy.

Datum:

Namn:

_____

Underskrift