SÖDERKÖPING.SE

Dokumentansvarig;	Dok.nr./	Dokumentnamn;	
Administrativ chef	SOC-2020-00070	Riktlinje verksamhetssystem socialförvaltningen	
Upprättad/reviderad av; Marita Aronsson, verksamhetsutvecklare		**Upprättad/reviderad dat;** 2020-09-02 2021-12-08,2022-07-05	**Revideras;** 2022-12-08 **Sida;** 1 av 4

Riktlinje verksamhetssystem socialförvaltningen

Syfte
Syftet med dokumentet är att ha en tydlig riktlinje för förvaltning, administration och uppföljning av våra verksamhetssystem för att säkerställa god kvalitet och informationssäkerhet.

Riktlinjen utgår från kommunens IT-plan och Informationssäkerhetsplaner

Ansvarig i verksamheten
Det övergripande ansvar för socialförvaltningens system finns under den administrativa chefen med verksamhetsutvecklaren som systemansvarig för verksamhetssystemen.

Styrande dokument från IT och information
IT-plan 2018-2022
Informationssäkerhetsplan 2018-2022
Informationssäkerhetsinstruktion användare 2018-2022 version 2.pdf
Informationssäkerhetsinstruktion förvaltning och drift 2018-2022

Stödjande dokument Socialförvaltningen
Systemsammanställning socialförvaltningen
Checklista vid årlig uppföljning av system och digitala verktyg

Ansvarsfördelning

Syftet med kommunens IT plan är att tydliggöra övergripande principer och förhållningssätt avseende IT inom kommunen samt definiera kommunens plan framåt. Det övergripande och strategiska ansvaret för IT-säkerheten ägs av kommunstyrelsen. IT-kontoret ansvarar för drift av underliggande system, affärssystem och infrastruktur. Kontoret ansvarar också för support, administration och inköp av IT-utrustning till samtliga verksamheter inom kommunen.

Respektive nämnd är systemägare till de affärssystem som brukas inom verksamheten. Systemägaransvaret och organisation av systemförvaltning delegeras till förvaltningschef. Förvaltningschef ansvarar för att IT samordnas inom sin verksamhet samt att resurser finns för att verkställa och driva IT på ett effektivt och säkert sätt.

Säkerhetsansvaret följer linjeorganisationen vilket innebär att var och en som är ansvarig för någon del av verksamheten även ansvarar för att IT-säkerheten efterlevs inom sitt område.

Detta dokument ska tydliggöra förvaltningens organisation samt ansvar för IT-säkerheten kring våra verksamhetssystem

Nya system, digitala tjänster och verktyg

Samtliga nya system ska godkännas av IT-chef i samråd med beställande nämnd (ägare) innan inköp och driftsättning.

Innan ett nytt förvaltningsövergripande system ska upphandlas/avtalas ska en projektplan utformas i samråd med IT och verksamhetsutvecklare, en systemsäkerhetsanalys ska genomföras med hjälp av KLASSA som ligger till grund för fortsatt kravspecifikation.

Innan ett lokalt system digitalt verktyg eller tjänst ska köpas in av verksamheterna ska verksamhetsutvecklare kontaktas för att tillsammans med verksamheten och IT-enheten säkerställas säkerhet, åtkomst och anpassning mot vår IT miljö och befintliga verktyg och tjänster.

Organisation för förvaltning av verksamhetssystem och digitala tjänster

Alla verksamhetens system ska ha en förvaltningsplan med syfte och mål, roller för systemadministration samt rutiner för behörigheter och åtkomst, uppföljning och kontroller, loggning och incidentrapportering.

Roller som alltid måste finnas för varje system är systemansvarig och systemförvaltare eller systemadministratör. Önskvärt är att det även finns en organisation av piloter/ombud för de större systemen på respektive enhet.

Systemägare

Systemägaren har det fulla ekonomiska och funktionella ansvaret för ett system samt ansvarar dessutom för systemets utveckling och eventuella avveckling**.** Socialnämnden är systemägare och ansvarar även för informationen i förvaltningens system. Nämnden har delegerat till förvaltningschefen (administrative chef) att svara för systemets funktionalitet och finansiering. Denne utser/tillsätter i sin tur funktioner som systemansvarig och systemförvaltare.

Systemansvarig

Systemansvarig har ett övergripande ansvar för systemet och upprättar tillsammans med ansvarig chef och systemförvaltare/administratör en förvaltningsplan med organisation för respektive system/tjänst/verktyg samt ett årshjul för kontroller och uppföljning. Planerad utveckling av system och digitala tjänster ska finnas i förvaltningens gemensamt framtagna utvecklingsplan.

Systemansvarig har även en kontrollfunktion att förvaltning och administration av systemen efterlevs enligt upprättad systemdokumentation och genomför årliga uppföljningar av respektive system och tjänst.

Systemansvaret återfinns hos administrativ chef eller av denne utsedd funktion.

Systemförvaltare

De förvaltningsövergripande systemen har en eller flera systemförvaltare under den administrative chefens ansvar.

Systemförvaltaren har det operativa/dagliga ansvaret för systemets administration och leverantörskontakter. Systemförvaltaren är ansvarig för uppdateringar, konfigurationer och inställningar samt felsökning och tester i systemet. Systemförvaltaren har ett ansvar för övergripande/gemensamma processer och rutiner, utbildningar samt loggar.

Systemadministratör

För system, tjänster och verktyg som används av en specifik verksamhet eller enhet ska en systemadministratör finnas. Systemadministratören har kontakt mot leverantören, administrerar det dagliga användandet och support av systemet. Systemadministratören administrerar behörigheter, kopplar ihop enheter och appar och ansvarar för lokala rutiner och utbildningar. Systemadministratör utses av ansvarig enhetschef i verksamheten.

Pilot/ombud

Piloten/ombudet är en person med god kunskap om hur systemet används i det dagliga arbetet. Piloten är en länk mellan central förvaltning och verksamheten och ska kunna stötta systemförvaltaren i processen samt förmedla ut nyheter och utbilda sina medarbetare.

En pilot finns lokalt på enheten där systemet används och utses av ansvarig chef.

Förvaltningsgemensamma verksamhetssystem

Verksamhetssystemen för Treserva, TES och LOK lednings och kvalitetssystem används av flera verksamheter, inklusive privata utförare och har en central systemförvaltning.

Det är den administrative chefens ansvar att det finns resurser till detta samt att se till att kommunens informationssäkerhetsplan följs för dessa system.

Verksamheternas specifika system

Verksamhetssystem som inte är centrala, utan används av ett verksamhetsområde eller en enhet ska även förvaltas och administreras på respektive verksamhet.

Det är enhetschefens ansvar att tillhandahålla resurser till detta samt att se till att kommunens informationssäkerhetsplan följs för respektive system.

IT-säkerhet/Informationssäkerhet

Enligt Söderköpings kommuns IT plan följer säkerhetsansvaret linjeorganisationen vilket innebär att var och en som är ansvarig för någon del av verksamheten även ansvarar för att IT-säkerheten efterlevs inom sitt område.

Verksamhetens system ska vara informationsklassade med SKLs verktyg KLASSA. Detta utförs vid nya system och tjänster eller vid större förändringar i systemet.

SÖDERKÖPING.SE

Informationssäkerhet ska säkerställa riktighet, sekretess, spårbarhet och tillgänglighet av informationen i våra system. Rutiner för att säkerställa detta ska finnas för respektive system.

Alla användare ska följa kommunens ”Informationssäkerhetsinstruktion för användare i Söderköpings kommun”. All personal ska genomgå den grundläggande informationssäkerhetsutbildning (DISA) http://disa.msb.se.

Ansvarig chef ansvarar för att nya användare har läst informationssäkerhetsinstruktion samt genomfört DISA utbildning.

Incidenthantering

Varje förvaltning ska kunna upptäcka, hantera och rapportera personuppgiftsincidenter som sker inom den egna verksamheten. En säkerhetsincident är en händelse som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Detta kan gälla såväl olovlig åtkomst till datasystem som till uppgifter i pappersform. Förlust av ett nedskrivet lösenord som går att använda till att se personuppgifter är en incident, likaså e-post med personuppgifter som skickas till obehörig person eller ett borttappat USB med personuppgifter.

Alla incidenter som innebär att personuppgifter som hanteras i våra system och tjänster har röjts eller riskerar att röjas för en obehörig ska anmälas enligt formulär på Kanalen. Sök på Incidentrapportering. En incident ska anmälas inom 48 timmar efter att incidenten upptäcktes.

https://intranet.soderkoping.se/service-och-stod-i-arbetet/dataskyddsforordningen/incidentrapportering/

Meddela även ansvarig chef/administrativ chef när en säkerhetsincident upptäckts.

Uppföljning och kontroller

I systemets förvaltningsplan eller i ett årshjul ska det framgå när återkommande kontroller som exempelvis behörigheter och händelseloggning ska genomföras. Det ska finnas rutiner för hur loggning m.m.ska hanteras vid enskilda incidenter.

En årlig kontroll av våra verksamhetssystem genomförs på iniativ av ansvarig chef med stöd av systemansvarig och enligt framtagen ”Checklista vid årlig uppföljning av system, digitala verktyg och tjänster på socialförvaltningen”.