Policy för informationssäkerhet och dataskydd

Typ av dokument	Beslutat av	Beslutsdatum	Diarienummer
Policy	*Kommunfullmäktige*	*2023-06-07 § 110*	*KS 2023/56*
Dokumentägare	**Giltighetstid**	**Framtagen av**	**Reviderad**
Sektor stödfunktioner	*Tillsvidare*	*Digitaliseringsenheten*	

Stenungsunds kommun

Innehållsförteckning

1. Inledning

Policyn är ett centralt styrdokument som redovisar kommunens viljeinriktning inom informationssäkerhet och dataskydd. Policyn kompletteras med underliggande styrdokument i form av riktlinjer samt regler och rutiner.

2. Definition

2.1 Informationssäkerhet

Information används i hela kommunen, av alla, och utgör en fundamental beståndsdel på samma sätt som medarbetare, lokaler och utrustning.

Därför måste vi skydda vår information så:

- att den alltid finns när vi behöver den (tillgänglighet)
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den (konfidentialitet)

Skyddet behöver anpassas efter behovet så att det är tillräckligt bra, inte för svagt, alltför krångligt eller dyrare än det behöver vara.

2.2 Dataskydd (skydd av personuppgifter)

Dataskydd handlar om skydd av personuppgifter och att behandling av dessa sker i enlighet med rådande dataskyddslagstiftning såsom dataskyddsförordningen (GDPR).

Dataskydd ställer krav på informationssäkerhet men innebär också mycket mer än att säkerställa de tre aspekterna *tillgänglighet*, *riktighet* och *konfidentialitet* som informationssäkerhetsarbetet tar sikte på. Till exempel kan information ha bäst tänkbara skydd ur ett informationssäkerhetsperspektiv men om det innehåller personuppgifter och behandlingen inte vilar på en rättslig grund är den olaglig och fallerar ur ett dataskyddsperspektiv.

En god nivå av informationssäkerhet innebär inte per automatik ett gott dataskydd - ett gott dataskydd innebär att alla dataskyddslagar följs.

2.3 Sammanfattning

Kommunens arbete med informationssäkerhet respektive dataskydd ska ske integrerat men med förståelsen för att de ser till olika perspektiv och skyddar olika intressen.

Arbetet omfattar att införa och förvalta **administrativa regelverk** så som denna policy kompletterad med underliggande styrdokument, **tekniskt skydd** med bland annat brandväggar och kryptering samt **fysiskt skydd** med till exempel skal- och brandskydd. Det handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge kommunens information, och de registrerades personuppgifter, adekvat skydd.

3. Resultat och effekter

Det systematiska dataskyddsarbetet är ett självändamål. Informationssäkerhet å andra sidan är inte ett självändamål utan ämnar bistå kommunen i att uppnå sina verksamhetsmål genom de positiva effekter som arbetets resultat genererar.

Förväntade resultat

Alla kommunens medarbetare känner till informationssäkerhet och dataskydd och har förståelse för sin roll i det.

All kommunens information är identifierad och klassad, har tilldelats skyddsnivå och värnas om med adekvata skyddsåtgärder.

All kommunens personuppgiftsbehandling är kartlagd, dokumenterad i registerförteckning med tillhörande tröskelanalyser eller konsekvensbedömning och sker i enlighet med rådande dataskyddslagar.

Kommunen har tydliga processer för såväl informationssäkerhetsincidenter som personuppgiftsincidenter.

Förväntade effekter

Personuppgiftsincidenter är sällsynta men alla medarbetare kan identifiera en incident och gör korrekt rapportering enligt rutin. Incidenten rapporteras vidare till tillsynsmyndighet där så är tillämpbart.

Informationssäkerhetsincidenter är sällsynta men i de fall de sker finns rutiner och kontinuitetsplaner som minskar risken för allvarliga konsekvenser.

Förtroendevalda, ledning, medarbetare och omvärld känner sig trygga med att Stenungsunds kommun hanterar information och personuppgifter på ett korrekt och säkert sätt.

Förutsättningar för processorienterad arkivredovisning med röd tråd till informationssäkerhet (och dataskydd) finns.

Digitalisering, en metod för verksamhetsutveckling, kan accelerera och blir mer ändamålsenlig eftersom kommunen har bättre kunskap om och styrning av information och processer.

4. Principer för arbetet

Informationssäkerhets- och dataskyddsarbetet ska vara verksamhetsdrivet och ske systematiskt vilket innebär att verksamheterna själva bär ansvaret för sin informationssäkerhet och sitt dataskydd. De har bäst kunskap om hur känslig och kritisk deras informationsmängder inklusive personuppgifter är och kan därmed bäst bedöma informationens skyddsvärde.

Utifrån informationens och personuppgifternas skyddsvärde ska verksamheten ställa krav på de aktörer som direkt eller indirekt hanterar informationen eller personuppgifterna. Det gäller såväl kommunens systemförvaltarorganisation som Soltak IT och externa systemleverantörer.

Kommunens stödfunktion avseende informationssäkerhet- och dataskydd ansvarar för att erhålla metod för det systematiska arbetssättet och verkar normerande, stödjande och kontrollerande gentemot verksamheterna.

Informationssäkerhets- och dataskyddsarbetet ska:

- stödja förvaltningens verksamheter att uppnå sina mål
- bygga på MSB:s metodstöd för systematiskt informationssäkerhetsarbete och kompletteras med delar för dataskydd.
- i termer av ansvar följa det ordinarie verksamhetsansvaret. Detta gäller hela vägen från ledning till enskilda medarbetare. Det yttersta ansvaret är därmed förlagt på högsta ledningen.
    - Ansvar för informationsbehandlingsresurser i form av IT-system ska vara tydligt knutet till en viss organisatorisk chefsbefattning och post. Se exempel i tabell nedan. Den som ansvarar för informationsbehandlingsresursen ansvarar för att information, särskilt personuppgifter, behandlas korrekt samt de risker som föreligger.

IT-system	**System-, risk- och informationsägare**
IT-system A	Enhetschef digitalisering
IT-system B	Enhetschef medborgarservice
IT-system C	Verksamhetschef bygg och miljö
IT-system …	Chef…

- tillämpa den kommungemensamma modellen för risk och informationsklassning med tillhörande konsekvenskategorier, konsekvenskriterier, skyddsnivåer och skyddsåtgärder.
- beaktas i de riskanalyser som föregår arbetet med kommunens internkontrollplan.
- årligen sammanfattas i en rapport till kommunstyrelsen.

5. Ansvar och roller

Grundprincipen är att ansvaret för informationssäkerhet respektive dataskydd följer det ordinarie verksamhetsansvaret. Detta gäller från kommunstyrelsen till den enskilde medarbetaren och innebär att den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt osv.) också är ansvarig för informationssäkerhet och dataskydd inom verksamhetsområdet.

Kommunfullmäktige – fastställer policy för informationssäkerhet och dataskydd.

Kommunstyrelsen – ansvarar för att kommunens policy för informationssäkerhet och dataskydd följs och för samordning av arbetet i kommunen. Kommunstyrelsen ansvarar även för att riktlinjer avseende informationssäkerhet och dataskydd utarbetas och hålls aktuella. Kommunstyrelsen samt de övriga nämnderna är personuppgiftsansvariga för de personuppgiftsbehandlingar som sker inom sina respektive områden. Kommunstyrelsen ska årligen fastställa en övergripande handlingsplan för informationssäkerhetsarbetet.

Kommundirektör – har kommunstyrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt och ansvarar för att övergripande tillämpningsanvisningar utarbetas och hålls aktuella i enlighet med policy och riktlinjer.

Sektorchef – är ytterst ansvarig för informationssäkerhet och dataskydd inom sin sektor.

Enskilda medarbetare - alla medarbetare har ett ansvar för kommunens informationssäkerhet. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler.

Informationssäkerhetssamordnare – det ska finnas en utpekad informationssäkerhetssamordnare som har det övergripande ansvaret att leda, utveckla och samordna kommunens informationssäkerhetsarbete.

Dataskyddsamordnare - det ska finnas en utpekad dataskyddssamordnare som har det övergripande ansvaret att leda, utveckla och samordna kommunens dataskyddsarbete. Dataskyddssamordnaren kan vara samma person som informationssäkerhetssamordnare. I ett sådant fall är denne medarbetare ”Informationssäkerhetssamordnare med samordningsansvar för dataskydd”.

Dataskyddsombud - har en stödjande, vägledande roll gentemot kommunen och ska tillse efterlevnad av gällande dataskyddslagstiftning. Kontaktperson för de registrerade, för kommunen och för tillsynsmyndigheten.

6. Hantering av undantag och avvikelser

Varje medarbetare är skyldig att rapportera avvikelser från styrdokument inom informationssäkerhet- och dataskyddsområdet. Avvikelserna rapporteras enligt gällande rutin och hanteras sedan enligt bestämd process så att erfarenheter kan tas till vara som en del av ett kontinuerligt förbättringsarbete. Större avvikelser rapporteras så snart som möjligt till kommundirektör och vid behov till kommunstyrelsen.

Mindre avvikelser sammanfattas i den årliga rapporten till kommunstyrelsen.

Beslut om godkännande av undantag som berör informationssäkerhet eller dataskydd ska fattas av kommunstyrelsen. Undantagen ska dokumenteras och får aldrig vara permanenta utan ska ha en giltighetstid på som längst två år. Om behov av undantag kvarstår ska ärendet beredas på nytt och nytt beslut fattas om eventuellt godkännande.