Härnösands kommun

POLICY

Datum
2023-11-20

Policy för informationssäkerhet och personuppgiftsbehandling

Dokumentnamn	Policy för informationssäkerhet och personuppgiftsbehandling		Dokumenttyp Policy	
Fastställd/upprättad av	Kommunfullmäktige		Datum 2023-11-20	Diarienummer 2023-000480
Dokumentansvarig/processägare	Informationssäkerhetssamordnare och dataskyddsombud	Version 1.0	Senast reviderad 2023-11-20	Giltig t o m 2027-12-31
Dokumentinformation	Styrdokument för informationssäkerhet och personuppgiftsbehandling			
Dokumentet gäller för	Samtliga nämnder och bolag i Härnösands kommun			
Annan information	Styrdokumentet gäller för Härnösands kommun och kommunala bolag			

Härnösands kommun

Innehållsförteckning

1 Sammanfattning av dokumentets sakliga innehåll

Denna policy innehåller Härnösands kommuns viljeriktning och övergripande principer gällande informationssäkerhet och dataskydd. Policyn med kompletterande riktlinjer ska tillämpas i alla situationer där Härnösands kommun och de kommunala bolagen, i fortsättningen benämnda tillsammans som *Härnösands kommun* eller *kommunen*, hanterar information med eller utan personuppgifter.

Dokumentet syftar till att säkerställa en effektiv styrning och ledning i det systematiska arbetet med informationssäkerhet och behandling av personuppgifter, så kallat dataskydd.

En god informationssäkerhet och personuppgiftshantering bidrar till att skapa förtroende för kommunen och dess bolag hos kommuninvånare och avtalsparter. Det är också en förutsättning för att kunna delta i den digitalisering av samhället som pågår.

2 Förhållandet till andra styrdokument

I Härnösands kommun finns ett stort antal styrande dokument som kompletterar varandra för att säkerställa att kommunen når sin vision och sina mål. I de fall det föreligger en konflikt mellan olika styrdokument av samma dignitet ska Policy och riktlinjer för informationssäkerhet och personuppgiftsbehandling ha företräde i de fall de ger ett högre skydd för information och registrerade.

3 Om informationssäkerhet och dataskydd

Härnösands kommuns informationstillgångar består av all information som hanteras i kommunens verksamheter. För att kunna fullgöra de uppdrag som kommunen har på ett effektivt och rättssäkert sätt, samt fullt ut dra fördel av digitaliseringens möjligheter måste informationen hanteras på ett säkert och lagligt sätt.

Informationssäkerhet och dataskydd kräver säkerhetsåtgärder i form av administrativa och organisatoriska åtgärder såsom styrdokument, regler, rutiner och kunskapshöjande insatser. Vidare krävs tekniska åtgärder så som behörighetskontroller, brandväggar och loggning liksom fysiskt skydd i form av exempelvis lås, larm och brandskydd för lokaler. Vilken nivå av skydd som krävs beror på rättsliga krav, kommunens egna prioriteringar och målsättningar samt de förväntningar som samhällets aktörer har kring tillgänglighet och skydd för deras information.

Rättsliga krav på informationssäkerhet och dataskydd återfinns bland annat i offentlighet- och sekretesslagen, arkivlagen, dataskyddsförordningen, lag om informationssäkerhet för samhällsviktiga och digitala tjänster samt Säkerhetsskyddslagen.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån tre aspekter:

- Konfidentialitet: att information inte tillgängliggörs eller avslöjas till obehörig

- Riktighet: att information är korrekt, aktuell och fullständig

- Tillgänglighet: att information är åtkomlig och användbar för behöriga.

Utifrån dessa aspekter klassificeras informationen för att kunna bedöma lämpliga skyddsåtgärder.

Information består till stora delar av personuppgifter. Dessa åtnjuter ett särskilt skydd genom dataskyddsförordningen. Regelverket innebär krav på informationssäkerhet men uppställer också ett stort antal rättsliga skyldigheter för personuppgiftsansvariga och rättigheter för dem vars personuppgifter registrerats.

Dessa skyldigheter och rättigheter kan inte enbart uppfyllas genom att vidta åtgärder på informationssäkerhetsområdet utan kräver handläggning och uppföljning på annat vis.

4 Mål med informationssäkerhet och dataskydd

Arbetet med informationssäkerhet och skydd för personuppgifter ska ske systematiskt, långsiktigt och med fokus på förebyggande åtgärder. Varje nämnd och styrelse ansvarar för sitt informationssäkerhets- och dataskyddsarbete utifrån intressenter och lagkrav. Varje verksamhet ska ha en planering för informationssäkerhet och dataskydd som beaktar att en framgångsrik digitalisering inkluderar ett aktivt informationssäkerhetsarbete för att motverka såväl säkerhetsmässiga som ekonomiska risker när nya tjänster utvecklas, köps in och tas i bruk.

Arbetet med informationssäkerhet och dataskydd ska

- bidra till att Härnösands kommun når sin vision och sina övergripande planer och mål med verksamheten.
- medföra en robust, säker och tillförlitlig informationshantering med få incidenter.
- möjliggöra en trygg, säker och effektiv digitalisering som inte riskerar verksamhetens kontinuitet eller medborgarnas rätt till integritet.
- bidra till att leva upp till verksamhetens, medborgares och externa aktörers behov och förväntningar vad gäller tillgänglighet till information samt skydd för personuppgifter och information som omfattas av sekretess.
- efterleva krav i lagar, förordningar, föreskrifter och avtal.
- bidra till att stärka Sveriges totalförsvarsförmåga.

5 Principer

Information är en strategisk tillgång, och tillgång till riktig information är en förutsättning för att fullgöra det uppdrag som kommuner har. Skyddet för personuppgifter är vidare en mänsklig rättighet. Följande principer ska vara vägledande i allt arbete med Härnösands kommuns information, oavsett om den hanteras av kommunkoncernen eller av externa parter;

- Informationssäkerhet och dataskydd bygger på en helhetssyn som innefattar processer, människor och teknik. Arbetet ska bedrivas resurseffektivt, vilket förutsätter att samtliga aspekter av informationssäkerhet och dataskydd beaktas tidigt i alla initiativ.
- Varje verksamhet ansvarar för sin informationshantering och tillhörande riktlinjer på ett sådant sätt att de arbetsuppgifter som följer av dokumenten kan genomföras.
- Varje verksamhet ska genomföra informationsklassning, risk- och sårbarhetsanalyser samt vid behov konsekvensbedömningar i enlighet med artikel 35 dataskyddsförordningen.
- Varje verksamhet ska, utifrån lagstiftning och riskerna med informationshanteringen, ställa krav på de aktörer som hanterar informationen.
- All information och alla informationstillgångar, såsom informationssystem och digitala tjänster, ska ha tydligt ägarskap.
- Arbetet med informationssäkerhet och dataskydd ska bedrivas långsiktigt och förebyggande, och ge förutsättningar att hantera säkerhets- och personuppgiftsincidenter, störningar och eventuella kriser.
- Arbetet med informationssäkerhet och dataskydd ska genom ett ledningssystem för informationssäkerhet (LIS) vara systematiskt och bygga på etablerade standards[1].
- Arbetet med informationssäkerhet och dataskydd inom kommunstyrelsen ska vara normerande, stödjande och kontrollerande i förhållande till kommunens övriga verksamheter.
- Vägledande för beslut, inriktningar och åtgärder ska utgå från normgivande standarder, metodstöd och rekommendationer.

[1] MSBs metodstöd för systematiskt informationssäkerhetsarbete bygger på standarden SS-EN ISO/IEC 27001 Ledningssystem för informationssäkerhet

6 Organisation och ansvarsfördelning

Huvudprincip - Ansvaret för informationssäkerhet och dataskydd följer verksamhetsansvaret på alla nivåer inom kommunorganisationen. Ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten och dataskyddet inom verksamhetsområdet.

Ansvaret och tillhörande åligganden för respektive roller beskrivs utförligare i tillhörande riktlinjer.

Kommunfullmäktige fastställer denna policy avseende informationssäkerhet och personuppgiftsbehandling som ska gälla för Härnösands kommun.

Kommunstyrelsen

- ska leda, samordna och följa upp det systematiska arbetet med informationssäkerhet och dataskydd.
- utfärdar de kommunövergripande riktlinjer som kompletterar policyn.

Nämnder och styrelser

- har det yttersta ansvaret för informationssäkerhet och dataskydd inom respektive verksamhet.
- är personuppgiftsansvariga enligt dataskyddsförordningen för sin verksamhet. Ansvaret kan inte delegeras. Personuppgiftsansvarig ska ge förutsättningar för och kunna visa att dataskyddsförordningen och kompletterande lagstiftning kring behandling av personuppgifter efterlevs. Ansvaret omfattar att utse och anmäla dataskyddsombud samt säkerställa dataskyddsombudets oberoende ställning.

7 Rapportering och uppföljning

Kommunstyrelsen ska följa upp det systematiska och strategiska arbetet med informationssäkerhet och dataskydd minst en gång per år.

Nämnder och styrelser

- Är ansvarig för att tillse att verksamheterna arbetar för att nå de kommunövergripande målen i denna policy genom att följa de grundläggande principerna för informationssäkerhetsområdet.
- Genom god intern kontroll ska nämnd/styrelse regelbundet följa upp efterlevnaden av denna policy med dess principer för måluppföljning, samt säkerställa att tillhörande riktlinjer tillämpas i arbetet
- Ska i rollen som personuppgiftsansvariga, årligen följa upp hur personuppgifter behandlas och hur arbete med att kvalitetssäkra dataskyddet fortlöper. I rollen ingår att tillse att inrapporterade incidenter sammanställs och analyseras, samt vilka åtgärder som är vidtagna och förbättringsförslag.