HEDEMORA KOMMUN	**STYRDOKUMENT**	Sida 1(8)
Skapad av: Säkerhetschefen	Datum 2021-11-22	Diarienummer: KS178-21 003
	Giltighet fr o m: 2022-05-31	Senast reviderad: 2018-06-12, § 75
Godkänt/antaget av: Kommunfullmäktige, 2022-05-31, § 73		
Dokumentansvarig: Säkerhetschef		

Informationssäkerhetspolicy och Dataskyddsstrategi

Dok. Kategori:	Policy och strategi
Stadie:	Beslutad
Gallring:	Bevaras
Kort beskrivning:	Denna informationssäkerhetspolicy är egentligen en strategi, men benämningen är vedertagen i branschen, varför den kvarstår i detta dokument. Strategi - anger långsiktiga mål, vägval, prioriteringar och pekar ut handlingsriktningar

Hedemora kommuns olika styrdokument

Organiserade styrdokument	Aktiverande styrdokument
Visar tydligt roll och ansvarsfördelning. - Reglemente - Delegationsordning - Bolagsordning	Visar vad kommunen vill förändra och uppnå. - Strategi - Mål och budget - Program - Ägardirektiv - Handlingsplan och övrig plan - Förvaltningarnas verksamhetsplan - Bolagens affärsplan - Aktivitetsplan
Normerande styrdokument Tydliggör kommunens förhållningssätt och arbetssätt. - Policy - Riktlinje - Rutin och vägledning	**Regler för dem som bor och verkar i Hedemora kommun** Tydliggör villkoren för kommunal service och vilka krav kommunen ställer på de som bor och verkar i kommunen. - Avgifter (inkl. taxor) - Regler (inkl. lokala föreskrifter och lokala ordningar

Mer information om de olika styrdokumenten finns i Hedemora kommuns riktlinje ”Riktlinjer för styrdokument”.

Globala målen – Agenda 2030

Mål 16 i Agenda 2030 *handlar om Fredliga och inkluderande samhällen. Fredliga samhällen och frihet från våld utgör både ett mål och ett medel för hållbar utveckling. En väl fungerande statsförvaltning med ansvarsfulla institutioner, transparens och rättsstatens principer har alla ett fundamentalt egenvärde. De utgör grund för god samhällsstyrning inklusive korruptionsbekämpning och är viktiga drivkrafter för utveckling. Alla människor är lika inför lagen och ska ha lika tillgång till rättvisa sant ska ha möjlighet att utöva inflytande och ansvarsutkrävande över beslutsfattare. God samhällsstyrning och rättsstatens principer är grundläggande mål och medel för utveckling. Begreppen demokrati och de mänskliga rättigheterna återfinns inte uttryckligen under mål 16. Dessa begrepp förekommer dock tydligt i den politiska deklarationen i 2030-agendan.*

Delmål i mål 16

16.10 Säkerställa allmän tillgång till information och skydda grundläggande friheter, i enlighet med nationell lagstiftning och internationella avtal.

INFORMATIONSSÄKERHETSPOLICY och DATASKYDDSSTRATEGI

antaget av kommunfullmäktige den 31 maj 2022, § 73.

Inledning

Ett systematiskt och riskbaserat informationssäkerhets- och dataskyddsarbete är en nödvändig del i och förutsättning för en framgångsrik digitalisering och en digital infrastruktur som möjliggör informationsutbyte inom offentlig sektor och mellan offentlig och privat sektor. Det är även nödvändigt utifrån de verksamheter som omfattas av säkerhetsskyddslagen (2018:585) eller EU:s NIS-direktiv (implementerats i Sverige genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga digitala tjänster).

Denna informationssäkerhetspolicy och dataskyddsstrategi gäller för allt informationssäkerhetsarbete och dataskyddsarbete inom Hedemora kommun och är en del av Hedemora kommuns hantering av informationstillgångar. Alla kommunens nämnder och helägda kommunala bolag, omfattas av styrdokumentet, vilket innebär att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Detta styrdokument och andra relevanta styrdokument kring informationssäkerhet och dataskydd gäller även för externa aktörer när dessa använder sig av kommunen och/eller dess bolags informationstillgångar.

Styrdokumentet syftar till att klarlägga:

- Definition av information, informationssäkerhet och dataskydd
- Mål
- Principer och arbetssätt
- Uppföljning, utvärdering, övervakning, rapportering, revidering

Organisation, ansvar och roller samt hur styrdokumentet ska tillämpas framgår av:

- Handlingsplan för informationssäkerhet, dataskydd och digitaliseringsutveckling (organisation, ansvar och roller)
    - Projektmodell för digitaliseringsprojekt i Hedemora kommun
- Riktlinje för informationssäkerhet och dataskydd
    - Riktlinje för informationssäkerhet i IT-miljön
    - Riktlinje för GDPR-arbetet i Hedemora kommuns nämnder och bolag

Informationssäkerhets- och dataskyddsarbetet i kommunen ska:

- garantera hög kvalitet, effektivitet och tillförlitlighet i informationshanteringen.
- hindra och/eller minska effekterna av oönskade händelser.
- höja säkerhetsmedvetandet hos de anställda.
- skydda medborgares integritet samt bidra till att utnyttjande av informationsteknik har deras förtroende.

Information

Information finns i kommunens alla verksamheter och är en i dagens samhälle värdefull, viktig och kritisk tillgång. Information innebär upplysningar om faktiska och tänkta förhållanden. Information kan innehålla uppgifter om personer, men behöver inte göra detta. Information kan uttryckas i och representeras av mänskliga tankar och kunskaper, ord som skrivs på papper, tal som förmedlas muntligt eller via telefon eller data i form av tecken och signaler i olika digitala och analoga media. Information som tillgång (informationstillgångar) handlar alltså om mer än information som hanteras av IT-system.

Informationssäkerhet

Informationssäkerhet handlar om säkerhet för information. Det innebär att se till att informationstillgångar finns tillgängliga när de behövs, att de är korrekta och att obehöriga inte får åtkomst till dem. En väl utvecklad och integrerad informationssäkerhet bidrar till att etablera en effektiv och ändamålsenlig informationshantering, vilket skapar förtroende både inom och utanför organisationen och direkt bidrar till att:

- möjliggöra digitaliseringssatsningar och underlätta transformering,
- undvika incidenter – bygga ett skydd mot it-attacker och läckage av personuppgifter,
- säker verksamhetsstyrning,
- bevara förtroende mot medborgarna, samt
- införa en metodik och ett arbetssätt för att efterleva lagstiftning och löpande uppföljning.

Informationssäkerhet är verksamhetsorienterat, eftersom det handlar om säkerhet kring information som har tillskrivits ett värde och en betydelse i en verksamhetskontext. Informationens relevans och värde är avgörande vid bedömning av vilken grad av skydd som är rimlig i en viss situation. Ju högre värde man tillskriver informationen, desto högre skydd behöver den. Det är således informationens värde som styr vilken säkerhet som krävs, i form av t ex fysiskt skydd som lokaler, lås och passersystem, brandskydd eller vilken IT-säkerhet som krävs och således vilket IT-system man ska ha. Informationssäkerhet handlar om bevarande av konfidentialitet, riktighet och tillgänglighet hos information, medans IT-säkerhet handlar om bevarande av konfidentialitet, riktighet och tillgänglighet hos information i digitala IT-system och andra IT-resurser.

- **Konfidentialitet** innebär att information inte tillgängliggörs eller avslöjas till obehörig. Det ska säkerställas att information är tillgänglig endast för dem som har behörighet för åtkomst.
- **Riktighet** innebär att information är korrekt, aktuell och fullständig. Ett skydd mot oönskad förändring, dvs skydd av information och behandlingsmetoder så att de förblir korrekta och fullständiga.
- **Tillgänglighet** innebär att information är åtkomlig och användbar av behörig vid rätt tillfälle, dvs ett säkerställande av att behöriga användare vid behov har tillgång till den information som de behöver för sitt arbete.

Informationssäkerhet begränsas således inte till säkerhet i IT-resurser utan omfattar information i alla dess former och oavsett hur informationen lagras, kopiera, scannas eller bearbetas på annat sätt och kommuniceras. Information kan t ex vara i form av text, ljud, bilder och film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Informationssäkerhet är en del av kommunens lednings- och kvalitetsprocess, som ska bidra till att ett informationssystem kan användas på avsett sätt och med avsedd funktionalitet.

Dataskydd (GDPR)

Dataskydd har sin utgångspunkt i EU:s rättighetsstadga artikel 8 om skydd av personuppgifter och en individs rätt till integritet. Tillsammans med rättighetsstadgans artikel 7 (rätten till privatliv) utgör de en del av de mänskliga rättigheterna. Dataskydd är en viktig del av den personliga integriteten. Ändamålet med dataskyddsförordningen (EU 2016/679 General Data Protection Regulation (GDPR) är respekten för människans integritet. Förutom att den handlar om värderingar och människosyn, handlar den även om hur en organisation kan skapa effektivitet och kvalitet i arbetet. Att säkerställa att personuppgifter har tillräckligt skydd är en del av informationssäkerhetsarbetet.

Globala målen Agenda 2030

Agenda 2030 är en integrerad del i Hedemora kommuns styrmodell. Ett av hållbarhetsmålen, Mål 16, handlar om fredliga och inkluderande samhället.

Det handlar bland annat om att alla människor är lika inför lagen och ska ha lika tillgång till rättvisa sant ska ha möjlighet att utöva inflytande och ansvarsutkrävande över beslutsfattare. God samhällsstyrning och rättsstatens principer är grundläggande mål och medel för en god demokratisk utveckling. Mål 16 har ett delmål i 16.10 att säkerställa allmän tillgång till information och skydda grundläggande friheter, i enlighet med nationell lagstiftning och internationella avtal.

Kommunens arbete med informationssäkerhet och dataskydd är viktiga delar för att uppnå hållbarhetsmålet.

Målsättning för Informationssäkerhetsarbetet

Informationssäkerhetsarbetet har inget egenvärde, utan ska bidra till att Hedemora kommun når sina övergripande visioner, Mål & budget och styrmodell ”Hållbara Hedemora”. Hedemora kommun ska uppnå och upprätthålla en informationssäkerhet som

- innebär att all information ses som en viktig tillgång för kommunen och skyddas i paritet med dess värde,
- innebär en robust, säker och tillförlitlig informationshantering,
- möjliggör ett aktivt medverkande i det digitala samhället och stödjer kommunens utvecklingsarbete,
- bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personlig integritet (personuppgiftshantering),
- motsvarar invånarens, externa verksamheters och medarbetares behov och förväntningar,
- efterlever krav i lagar, förordningar, föreskrifter och avtal,
- efterlever fastställda dokumenthanteringsplaner och gallringsbeslut, övrig sekretesslagstiftning,
- förebygger oväntade händelser i informationssystem (IT-system) och i hanteringen av andra informationstillgångar,
- säkerställer att det finns kända rutiner för hantering av incidenter,

- innebär att all personal ges tillräcklig kunskap om gällande regelverk kring kommunens informationssäkerhetsarbete för att kunna utföra sina arbetsuppgifter i enlighet med detsamma,
- säkerställer att det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation,

Målsättningen ska säkerställa att Hedemora kommun kan tillhandahålla relevant information som

- endast delges behöriga personer, kan levereras vid rätt tidpunkt och till skäliga kostnader,
- är riktig genom att vara fullständig, komplett och aktuell,
- genom spårning skyddar känslig information mot oönskad insyn och förändring,
- efterfrågas och som organisationen har ett ansvar att tillhandahålla.

Målsättning för Dataskyddsarbetet (GDPR)

Hedemora kommun ska bedriva ett effektivt organiserat och strukturerat dataskyddsarbete som uppfyller kraven i dataskyddslagstiftningen (inkl. EU 2016/679 General Data Protection Regulation (GDPR) – Dataskyddsförordningen) för att säkerställa skyddet av invånarnas och medarbetarnas integritet. Invånarnas och medarbetarnas integritet är en viktig del i arbetet med kommunens vision, Mål & budget och styrmodell ”Hållbara Hedemora”. Hedemora kommun ska uppnå och upprätthålla ett dataskydd

- som hela tiden arbetar utifrån **“Inbyggt dataskydd och Dataskydd som standard”**. Det innebär att inga personuppgifter ska behandlas i onödan och att man hela tiden ska sträva efter att bli bättre och således arbeta utifrån principen om ständiga förbättringar i sitt dataskyddsarbete. Dataskyddsarbetet ska bygga på ett riskbaserat förhållningssätt. Vid nyinvesteringar och i sitt utvecklingsarbete ska man utgå ifrån att möjliggöra och underlätta för digitalisering och på ett effektivt sätt uppfylla dataskyddslagstiftningen, vilket bland annat innebär att arbeta för att minimera behandling av personuppgifter i ostrukturerat material (ex. material i e-post, word, excel, papper, pärmar) och upprätthålla nödvändig säkerhet. Behandling av personuppgifter ska i möjligaste mån behandlas i strukturerat material, dvs vara sökbart i ett IT-system,
- där de **grundläggande dataskyddsprinciperna** (proportionalitet, ansvarsskyldighet (accountability), ändamålsbegränsning, uppgiftsminimering, riktighet, lagringsminimering, integritet/konfidentialitet, laglighet, korrekthet och öppenhet) genomsyrar all kommunal verksamhet,
- där man så långt som möjligt vid **organisering och utförande** av dataskyddsarbetet eftersträvar effektivitet, samordning och samverkan för kommunkoncernen som helhet.
- där **servicenivån** i kommunens förvaltningar och bolag ska följa gällande lagstiftning, förordningar, föreskrifter, avtal och kommunens tjänstegarantier samt tillgodose invånarnas fri- och rättigheter utifrån ett GDPR- perspektiv. Servicen ska utmärkas av tillit och uppfattas som välkomnande, trygg och enkel.
- som säkerställer att rutiner för incidenthantering är kända i kommunens verksamheter,
- genom att ha ett framtaget aktuellt **utbildningsprogram i dataskydd** för samtliga medarbetare och chefer. En kontinuerlig kompetensutveckling för kommunens medarbetare och chefer i dataskydd är en viktig förutsättning för ett gott dataskydd i kommunen/bolaget.

Principer och arbetssätt

Hedemora kommun ska arbeta med informationssäkerhet och dataskydd på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet och dataskydd ska gentemot kommunens verksamheter vara normerande, stödjande och kontrollerande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande Hedemora kommuns informationstillgångar samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå. Kommunen ska hantera verksamheternas information utifrån säkerställd konfidentialitet, riktighet och tillgänglighet.

Arbetet med informationssäkerhet och dataskydd ska

- bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik,
- bygga på ledningens aktiva engagemang. Det handlar om ett förändringsarbete som kräver ett proaktivt arbete från ledningens sida och att den regelbundet informerar sig,
- vara verksamhetsdriven, vilket innebär att verksamheter utifrån informationens skyddsvärde ger instruktioner och ställer krav på de aktörer som hanterar informationen, exempelvis kommunens- och de helägda kommunala bolagens IT-avdelning och externa systemleverantörer,
- vara systematiskt, riskbaserat och bygga på den etablerade standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS). SS-ISO/IEC 27001, 27002 och 27701 ska tillämpas i genomförandet av informationssäkerhets- och GDPR-arbetet (integritetsarbetet), Myndigheten för samhällsskydd och beredskaps (MSB) metodstöd LIS ska användas som ramverk för informationssäkerhetsarbetet,
- all information ska informationsklassas. Informationsklassning syftar till att ge känslig och kritisk information ett starkare skydd än annan information. Hedemora kommun ska tillämpa en enhetlig modell för informationsklassning, som anger olika nivåer av skyddskrav vari information ska klassas baserat på interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet. All information ska även ha tillräcklig spårbarhet inkl. autenticitet och oavvislighet gentemot sitt skyddsvärde. Spårbarhet innebär att aktiviteter och hur information förändrats ska kunna spåras genom t ex loggning. Autenticitet innebär att en mottagare av information kan förlita sig på att avsändaren verkligen är den hen utger sig för att vara. Oavvislighet innebär att en part inte kan förneka att denne gjort en viss handling, t ex en beställning.
- säkerställa att hotbilden för varje enskilt samhällsviktigt informationssystem (IT-system och andra IT-resurser) och i andra informationstillgångar fortlöpande ses över och analyseras då Hedemora kommun och dess omvärld, inkl. hotbild, är under ständig förändring,
- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa,
- bygga på Hedemora kommuns värdegrund KRAM (Kundfokus, Respekt, Ansvar och Mod), ta hänsyn till verksamheters behov, externa krav samt rådande hotbild,
- vara väl kommunicerat i verksamheten; all personal ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och en god dataskyddskultur, och kunna leva upp till kommunens styrdokument kring informationssäkerhet och dataskydd,

- ske i aktiv samverkan med det omgivande samhället såsom myndigheter, företag och nätverk, särskilt sådana som är normgivande inom informationssäkerhet och dataskydd, t ex SKR (Sveriges kommuner och landsting), MSB (Myndigheten för samhällsskydd och beredskap), SIS (Swedish Standards Institute) och IMY (Integritetsskyddsmyndigheten), erforderliga informationssäkerhets- och dataskyddskrav ska finnas med i alla typer av upphandlingar som hanterar informationstillgångar,
- informationssäkerhets- och dataskyddskrav ska finnas med och vara framtagna senast i förstudiefas i projekt. Dessa kan dock förändras över tid i projektet beroende på vad som framkommer under projektets gång.

Integrerad del av organisationens normala verksamhet

Informationssäkerhets- och dataskyddsarbetet ska bedrivas som en integrerad del av organisationens normala verksamhet och styrsystem och således ingå i kommunens Mål & budget, aktivitetsplanerna för kommunstyrelsen, respektive nämnd och helägt kommunalt bolag. Årliga mål för arbetet ska därför fastställas i verksamhetsplanerna.

För de årliga aktiverna bör anges:

- vad ska utföras och prioriteras under året,
- tidsplan (när och hur, sluttidpunkt),
- resurser för arbetet (personella och ekonomiska),
- när och hur uppföljning, utvärdering och avrapportering ska ske,
- när och hur kommunens medarbetare ska informeras och utbildas.

Uppföljning, utvärdering, övervakning, rapportering och revidering

Efterlevnaden och tillämpningen av gällande lagstiftning, förordningar, föreskrifter, avtal, informationssäkerhetspolicy och dataskyddsstrategi ska regelbundet följas upp och utvärderas av verksamheterna själva. Samtliga enskilda verksamheter har alltid huvudansvaret att följa upp, utvärdera och vidta erforderliga åtgärder samt revidera sina styrdokument som man äger.

Informationssäkerhetssamordnare och dataskyddsombud har för sina respektive områden i uppgift att övervaka efterlevnaden av lagstiftning, förordningar, föreskrifter och avtal, om beslutade åtgärder är genomförda, om årliga mål är uppfyllda, om styrdokument följs samt att informera/rapportera om brister i efterlevnaden och eventuella behov av åtgärder och revideringar av styrdokument till verksamheterna som man uppmärksammat vid sin övervakning.

Informationssäkerhetssamordnare ska minst en gång per år rapportera läge och status gällande informationssäkerhet till mellanliggande förvaltningsnivå (ledningsgrupp) samt årligen rapportera till kommundirektör och kommunstyrelsen. Särskilda skäl som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

Dataskyddsombudet ska regelbundet bjudas in att delta i möten på högsta (nämnd/styrelse) och mellanliggande (ledningsgrupp) förvaltningsnivå när beslut med följder för dataskyddet fattas. Dataskyddsombudet ska rapportera direkt till den högsta förvaltningsnivån (nämnden/styrelsen).