Informationssäkerhet - Övergripande direktiv, Region Gävleborg

Innehåll

1. Syfte och omfattning

Region Gävleborg eftersträvar att följa ISO/IEC 27001:2022 Ledningssystem för informationssäkerhet. ISO/IEC 27001:2022 ställer krav på att högsta ledningen ska upprätta och besluta om en informationssäkerhetspolicy. Det övergripande direktivet motsvarar informationssäkerhetspolicy enligt ISO/IEC 27001:2022. Det övergripande direktivet är grunden för Region Gävleborgs ledningssystem för informationssäkerhet (LIS). Det övergripande direktivet målsättning för informationssäkerhetsarbetet inom Region Gävleborg samt organisationens åtagande om att uppfylla tillämpliga krav på informationssäkerhet.

Direktivet omfattar all information som Region Gävleborgs verksamheter äger och hanterar.

2. Allmänt

Region Gävleborg, liksom övriga regioner, har ansvar för verksamheter som är några av de mest betydelsefulla för samhället och enskilda individer. För att verksamheterna ska fungera i det digitala samhället krävs det en fungerande informationshantering. Till följd av det är Region Gävleborgs

informationshantering både verksamhetskritisk och samhällskritisk som måste hanteras och skyddas på ett sådant sätt att den stödjer Region Gävleborgs huvuduppdrag. Bristfällig informationssäkerhet kan leda till risker för liv och hälsa, för den personliga integriteten och kan även leda till negativ ekonomisk påverkan och förtroendeskada för Region Gävleborg.

Det systematiska arbetet med informationssäkerhet ska utgå från standarden för informationssäkerhet enligt ISO 27000-serien. Lagar och förordningar utgör en grund för detta arbete, överenskomna avtal ska följas och externa intressenters, exempelvis patienter, krav och förväntningar införlivas.

Informationssäkerhetsarbetet ska bedrivas så det stödjer regionens arbete med digitalisering samtidigt som det skyddar regionen, medarbetarnas och externa intressenters information.
Region Gävleborg arbetar, likt som många andra myndigheter, för enklare tillgång till information och service och effektiviserar interna och externa processer med hjälp av digitala tjänster. En ökning av sårbarheten följer av digitaliseringen av samhällsbärande funktioner och det är av stor vikt att informationssäkerhet beaktas i digitaliseringen.

Sammantaget har regioner sannolikt samhällets mest komplexa krav på informationssäkerhet. Därför är en tydlig styrning och systematik nödvändig för att Region Gävleborg ska lyckas upprätthålla en informationshantering med tillräcklig säkerhet och kvalitet.

3. Ansvar och roller för direktivet

3.1. Stabsdirektör

Ansvar för att direktivet upprättas och hålls aktuellt

4. Beskrivning

4.1. Ansvar och roller för informationssäkerhet

Ansvaret för informationssäkerhet delas upp i ett ledningsansvar och ett verksamhetsansvar.

4.1.1. Ledningsansvar

4.1.1.1. Regiondirektören

Regionstyrelsen har det yttersta ansvaret för informationssäkerhetsarbetet inom Region Gävleborg. Regiondirektören har ansvaret för att genomföra de intentioner som formuleras i detta övergripande direktiv i Region Gävleborgs verksamhet. I detta ansvar ingår att säkerställa att det finns styrdokument för informationssäkerhet och resurser för att genomföra det som dessa styrdokument föreskriver. Regiondirektören ska även tillse att det finns ett gemensamt

dataskyddsombud för Region Gävleborg som kan fungera i denna egenskap för samtliga personuppgiftsansvariga inom organisationen. Dataskyddsombud utnämns enligt artikel 37 dataskyddsförordningen.

Regiondirektören och ledningsgruppen ska ha en uppdaterad lägesbild över identifierade risker avseende informationshantering och besluta om hur dessa risker ska hanteras. Arbetet med lägesbilden ska när så är lämpligt samordnas med Region Gävleborgs övriga riskhantering.

4.1.1.2. Enhetschef informationssäkerhetsenhet

Informationssäkerhetschef ska, i enlighet med regiondirektörens beslutade inriktning, strategiskt och operativt utöva ledningsansvaret för det övergripande informationssäkerhetsarbetet. Informationssäkerhetschef ska som stöd för Region Gävleborgs verksamhetsplanering årligen ta fram ett förslag på plan för aktiviteter och åtgärder för informationssäkerhetsarbetet, dels det arbetet som ska genomföras i respektive verksamheterna och av den centrala informationssäkerhetsenheten.

4.1.1.3. Särskilt avseende IT-säkerhet

På IT-förvaltningen ska det finnas ansvariga för IT-säkerhetsarbetet som har ansvaret för att utveckla och förvalta de IT-säkerhetsåtgärder som är följden av de krav som ställs avseende informationssäkerhet.
IT-förvaltningen har ett särskilt ansvar att omsätta funktionella krav på säkerhet till tekniska lösningar. IT-direktör ska därför årligen ta fram ett förslag på plan med budget för IT-säkerhetsåtgärder som följer plan för informationssäkerhetsarbetet.

4.1.2. Chefer

Ansvaret för informationssäkerheten ska följa verksamhetsansvaret.
Att utveckla och upprätthålla informationssäkerhet enligt ledningssystem för informationssäkerhet är en del i Region Gävleborgs generella chefsansvar. Detta innebär ansvar för tillämpningen av ledningssystemets regelverk i den egna verksamheten. Ansvaret omfattar bland annat att tillse att personalen hanterar information enligt gällande styrdokument och att implementera informationssäkerhetsregler för den egna verksamheten.

4.1.3. Medarbetare

Medarbetare ansvarar för att följa Region Gävleborgs ledningssystem för informationssäkerhet samt genomföra obligatoriska utbildningar inom området.

4.2. Särskilt gällande dataskydd

Region Gävleborgs hantering av personuppgifter ska uppfylla de grundläggande principerna som anges i allmänna dataskyddsförordningen (2016/679) samt övrig dataskyddslagstiftning och Region Gävleborg ska särskilt kunna redovisa hur bestämmelserna i dataskyddsförordningen efterlevs. Region Gävleborg ska säkerställa att de registrerades rättigheter (artikel 12-23 dataskyddsförordningen) tillgodoses.

I Region Gävleborgs processer och digitala lösningar ska integritet som standard och inbyggt dataskydd finns med i alla steg genom organisatoriska och tekniska lösningar.

Region Gävleborgs dataskyddsombud ska genomföra fortlöpande kontroller, säkerställa att dataskyddet fungerar enligt ovanstående och, om så inte sker, rapportera till personuppgiftsansvariga och regiondirektören samt i vissa fall till dataskyddsmyndigheten.

4.3. Inriktning och tillämpning

Region Gävleborgs inriktning är att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet med anpassning till kraven i ISO 27000-serien.
Tillräckliga resurser ska tilldelas för informationssäkerhetsarbetet och årlig återrapportering ska ske till regionstyrelsen.

Ledningssystemets regler gäller all information som hanteras av verksamheten, medarbetare och externa parter för att utföra organisationens uppdrag. Reglerna ska även tillämpas då Region Gävleborg köper produkter och tjänster som kan påverka Region Gävleborgs informationssäkerhet.
De krav som följer av dataskyddsförordningen ska integreras i det systematiska informationssäkerhetsarbetet.

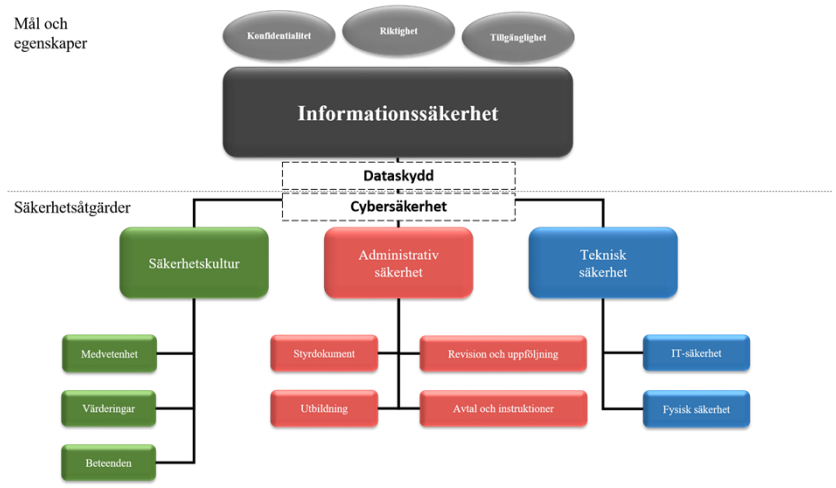
Informationshantering ska skyddas på ett kostnadseffektivt sätt där risk vägs mot nytta och beslut ska dokumenteras och kommuniceras.

4.4. Definition

Med informationssäkerhet avses att hantera information med rätt nivå av konfidentialitet, riktighet, och tillgänglighet.

Det övergripande syftet är att ha rätt nivå av informationssäkerhet, det skapas genom ett antal olika åtgärder som visas i nedan bild.
Åtgärder omfattar:

- **Säkerhetskultur** rör de gemensamma värderingar, kunskaper, attityder och beteenden hos medarbetare inom en verksamhet som är inriktade på att skapa säkerhet. Säkerhetskulturen är grundläggande för verksamhetens förmåga att skydda sin information, data, integritet och sina medarbetare. En adekvat säkerhetskultur stärker verksamhetens informationssäkerhetsförmåga.
- **Administrativ säkerhet** handlar om att se till att det finns ändamålsenliga styrdokument som beskriver hur information ska hanteras i organisationen.
- **Teknisk säkerhet** delas typiskt in i två delar: fysisk säkerhet och IT-säkerhet.
  - Fysisk säkerhet är saker som larm till lokalerna, kodlås till kontorsrum, kassaskåp för att skydda känslig information som lagras på IT-utrustning eller i pappersformat.



[1]

4.5. Avgränsning

Region Gävleborgs informationssäkerhetsrutiner hanterar inte de krav som följer av säkerhetsskyddslagen.

4.6. Beskrivning av Region Gävleborgs systematiska arbete för informationssäkerhet

Region Gävleborgs ledningssystem styr Region Gävleborgs informationshantering så att informationen hanteras med den säkerhet som ledningen bedömt lämplig utifrån verksamhetens behov och externa krav. Styrningen omfattar att identifiera och analysera, utforma, använda och följa upp och förbättra verksamhetens informationshantering och informationssäkerhet.
Detta övergripande direktiv samt övriga styrdokument är ordnade i en hierarkisk struktur och ingår i LIS. Dokumentationen ska ses som en helhet och det ska finnas en spårbarhet mellan olika ingående dokument.
Ledningssystemets består inte endast av dokumentationen men förutsätter medarbetarnas kunskap, medvetenhet och motivation. Forum för dialog och utveckling i säkerhetsfrågor samt målgruppsanpassat material är därför centrala funktioner i ledningssystemet

Det systematiska informationssäkerhetsarbetet ska bidra till att Region Gävleborg upprätthåller en nivå av informationssäkerhet som

- grundar sig i ett riskbaserat arbetssätt
- innebär en säker och lagenligt informationshantering

[1] Grafisk ritning av informationssäkerhetsområdet är allmänt vedertagen nationellt, se exempelvis Beskrivning Informationssäkerhet.pdf (fmv.se)

- möjliggör digitaliseringssatsningar och underlätta transformering
- har en tillräcklig kompetensnivå
- har en positiv effekt på kvalitet och effektivitets mål
- bidrar till en hög säkerhetskultur och uppmuntrar till engagemang hos samtliga medarbetare och, förutom att följa gemensamma regler, motiverar dem att delta i att ständigt förbättra informationssäkerheten.

4.7. Övergripande målsättning

- Region Gävleborgs information ska identifieras och förtecknas.
- Säkerhetsåtgärder ska följa av informationsklassning och riskanalyser. Centrala säkerhetsåtgärder som informationsklassning, styrning av åtkomst, loggning, incident- och kontinuitetshantering ska vara prioriterade i informationssäkerhetsarbetet.
- Det ska finnas ett tydligt ansvar för Region Gävleborgs informationshantering och de resurser som används för att stödja den.
- Ledningen ska ha en god kompetensnivå avseende informationssäkerhetsarbetet och är ansvarig för att bedöma vilka risker som är acceptabla och vilka som måste åtgärdas och förmedla detta via det generella chefsansvaret.
- Ansvaret för informationssäkerhet är ett verksamhetsansvar och styrningen av informationssäkerhet ska utgå från nyttan i verksamhetsprocesserna. Ansvaret ska vara känt och accepterat.
- Externa krav på dataskydd, skydd för samhällsviktig verksamhet och infrastruktur samt för civilt försvar och beredskap som i sin tur ställer krav på informationssäkerhetsåtgärder ska vara integrerade i det generella informationssäkerhetsarbetet.
- Region Gävleborgs informationssäkerhetsarbete ska vara utformat så att det tar hänsyn till de starkt skiftande krav som kan finnas inom Region Gävleborgs olika verksamheter.
- I Region Gävleborg ska finnas tillräcklig kompetens inom informationssäkerhetsområdet för att kunna hantera den komplexa kravbilden. Kompetensen ska finnas både i form av specialistkompetens och i form av en bred förståelse av betydelsen av informationssäkerhet hos medarbetarna.

4.8. Uppföljning

Uppföljning av Region Gävleborgs arbete med informationssäkerhet ska ske på ett regelbundet och strukturerat sätt samt utföras genom interna kontroller och revisioner av oberoende part.

5. Plan för kommunikation och implementering

Informationssäkerhetsenheten ansvarar för kommunikation och implementering.

6. Dokumentinformation

Dokumentet har uppdaterats av informationssäkerhetsenheten i samråd samtliga förvaltningar inom Region Gävleborg. Direktivet är fastställt i Platina dokumenthantering av Ulrika Weglin på uppdrag av Regionstyrelsen efter beslut 2024-06-04, § 183.

Kommentar [KFL-K-I1]: Ändras senare

7. Referenser

Dokumentnamn	Plats
Patientdatalagen, SFS 2008:355	www.riksdagen.se
Journalföring och behandling av personuppgifter i hälso- och sjukvården	www.socialstyrelsen.se
Europaparlamentets och rådets förordning (EU) 2016/679 (GDPR/Dataskyddsförordningen)	https://eur-lex.europa.eu
Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster	www.riksdagen.se
11-314992 Informationssäkerhet – Direktiv för ansvar och roller Region Gävleborg	Platina