Upprättare: Lisa M Knutsson Fröjd

Fastställare: Regionstyrelsen

Informationssäkerhet - Övergripande direktiv, Region Gävleborg

Innehåll

1. Syfte och omfattning

Det övergripande direktivet är grunden för Region Gävleborgs ledningssystem för informationssäkerhet (LIS). Det övergripande direktivet fastställer ansvar roller och målsättning för arbetet med informationssäkerhet inom Region Gävleborg.

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 samhällskritiskt 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.

Region Gävleborg har såväl interna behov såsom externa behov på informationssäkerhet. Exempelvis finns det externa krav på Region Gävleborg gällande dataskydd, skydd för samhällsviktig verksamhet och infrastruktur och

som en del i den civila beredskapen. Den alltmer integrerade nationella e-hälsan kräver att alla deltagande aktörer har en nivå av säkerhet som inte äventyrar helheten. Region Gävleborg ska tillämpa de regler, rekommendationer och standarder för informationssäkerhet som den gemensamma e-hälsan förutsätter.

Region Gävleborg arbetar, likt som många andra myndigheter, för enklare tillgång till information och service och effektiviserar interna 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. Informationssäkerhetsansvarig

Informationssäkerhetsansvarig ska, i enlighet med regiondirektörens beslutade inriktning, strategiskt och operativt utöva ledningsansvaret för det övergripande informationssäkerhetsarbetet. Informationssäkerhetsansvarig 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 genomförs i verksamheterna och av den centrala informationssäkerhetsfunktionen.

På IT-förvaltningen ska en IT-säkerhetsansvarig finnas som har ansvaret för att utveckla och förvalta de IT-säkerhetsåtgärder som är följden av de krav som ställs avseende informationssäkerhet.

4.1.2. Verksamhetsansvar: chefer och medarbetare

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.
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 informationssäkerhetsansvariges plan för informationssäkerhetsarbetet.

4.2. Särskilt gällande dataskydd

Region Gävleborgs hantering av personuppgifter ska uppfylla de grundläggande principerna som anges i dataskyddsförordningen 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 genom 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. Även organisatoriskt samordnas informationssäkerhet och dataskydd.
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, tillgänglighet och spårbarhet.

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 direktiv och instruktioner 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

4.7. Mål

- För att hålla rätt nivå och rätt inriktning ska Region Gävleborgs informationssäkerhet grundas i riskanalyser och informationsklassningar på olika nivåer i organisationen.
- Det ska finnas ett tydligt ansvar för Region Gävleborgs informationshantering och de resurser som används för att stödja den.
- Ledningen ska 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.
- Det ska finnas en beslutad metod för informationsklassning som även innehåller standardiserade skyddsnivåer.
- Centrala säkerhetsåtgärder som informationsklassning, styrning av åtkomst, loggning, incident- och kontinuitetshantering ska vara prioriterade i informationssäkerhetsarbetet.
- I Region Gävleborg ska finnas tillräcklig kompetens inom informationssäkerhetsområdet för att kunna hantera den komplexa kravbilden. Kompetensen ska finnas både i form av spetskompetens och i form av en bred förståelse av betydelsen av informationssäkerhet hos medarbetarna.
- Region Gävleborg ska ha en säkerhetskultur som uppmuntrar engagemang hos alla medarbetare och, förutom att följa gemensamma regler, motiverar dem att delta i att ständigt förbättra informationssäkerheten.

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

Informationssäkerhetsfunktionen ansvarar för kommunikation och implementering.

6. Dokumentinformation

Dokumentet har uppdaterats av informationssäkerhetsfunktionen i samråd med Stabsdirektör och säkerhetschef. Direktivet är fastställt i Platina dokumenthantering av Ulrika Weglin på uppdrag av Regionstyrelsen efter beslut 2020-12-09, § 203.

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