Bilaga 5

Göteborgs Stad

SDF Örgryte-Härlandas Riktlinje för informationssäkerhet

Reglerande styrande dokument

- Policy
- ► **Riktlinje**
- Regel
- Anvisning
- Rutin
- Instruktion

Dokumentnamn: SDF Örgryte-Härlandas Riktlinje för informationssäkerhet			
Beslutad av: Stadsdelsdirektör	Gäller för: SDF Örgryte-Härlanda	Diarienummer: N133-0186/20	Datum och paragraf för beslutet: 2020-04-01
Dokumentsort: Riktlinje	Giltighetstid: Tills vidare	Senast reviderad: 2020-03-19	Dokumentansvarig: Utvecklingsledare säkerhet
Bilagor: Organisation inom informationssäkerhet med klargjorda roller och ansvar.			

Innehåll

Inledning

Syftet med denna riktlinje

Beskriva hur förvaltningen ska arbeta med identifiering, analys, utvärdering, behandling, övervakning och granskning av informationsrisker.

Riktlinjen bygger på stadens riktlinje och råd om informationssäkerhet.

Vem omfattas av riktlinjen

Denna riktlinje gäller tills vidare för samtliga medarbetare i SDF Örgryte-Härlanda.

Lagbestämmelser

Dataskyddsförordningen (GDPR)

Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster

Patientdatalagen (2008:355),

Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården

Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8)

Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9)

Koppling till andra styrande dokument

Säkerhetspolicy för Göteborgs Stad

Göteborgs Stads riktlinje för informationssäkerhet

Göteborgs Stads riktlinjer för hantering av säkerhetsrisker

Regler gällande informationssäkerhetsansvar för chefer i Göteborgs Stad

Regler för IT-användare i Göteborgs Stad

SDF Örgryte-Härlandas rutin för rapportering av incidenter enligt NIS-direktivet.

SDF Örgryte-Härlanda Organisation inom informationssäkerhet med klargjorda roller och ansvar

Göteborgs Stads generella regler för kommungemensamma interna tjänster

Stödjande dokument

Stadengemensamma råd:[1]

- Råd för riskanalys avseende informationssäkerhet.
- Råd för hur man genomför en informationsklassning
- Exempel på informationsklassning
- Förslag på lokala anvisningar/bestämmelser

[1] Hela staden – Säkerhet, samhällsskydd och beredskap – Informationssäkerhet

Riktlinje

Informationssäkerhet

Informationssäkerhet är de åtgärder som vidtas för att hindra att information sprids på ett otillbörligt sätt, förvanskas, förstörs eller är otillgänglig när den behövs.

Riktlinjerna gäller oavsett i vilken form informationen finns, till exempel på papper, elektroniskt media, film, ljudfil, yttras i en konversation med mera.

Koppling till GDPR

Hantering av personuppgifter enligt GDPR är en del av informationssäkerheten. De riktlinjer som gäller för informationssäkerhet gäller även för hantering av personuppgifter. Ytterligare riktlinjer eller regler kan finnas utifrån GDPR.

Koppling till MSB's föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster

Förvaltningen är leverantör av hälso- och sjukvård vilken räknas som en samhällsviktig tjänst.

Enligt riktlinjen ska leverantör av samhällsviktiga tjänster bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ISO-standarder. Stadens styrande dokument för informationssäkerhet bygger på dessa standarder. Förvaltningens metod för att leva upp till kraven i stadens styrande dokument är denna riktlinje.

Roller och ansvar

Ansvarsfördelning för i staden

Intraservice ansvarar för

- den grundläggande IT-infrastruktur som möjliggör användande av övriga kommungemensamma interna IT-tjänster
- driften av kommungemensamma IT-system

Förvaltningen ansvarar för sin interna hantering av IT-systemen och för driften av icke-kommungemensamma tjänster.

Roller och ansvar i förvaltningen

Ansvaret för informationssäkerheten följer linjeorganisationen.

Informationsägare är respektive chef.

Se bilaga Organisation inom informationssäkerhet med klargjorda roller och ansvar.

Identifiering och klassning av informationstillgångar

Alla verksamhetsansvariga chefer ansvarar för att identifiera och klassa sina informationstillgångar. För att identifiera dem kan man utgå från verksamhetens processer.

Inom Göteborgs Stad delas information in i tre klasser (0, 1, 2) beroende på vilken skada brister i informationssäkerheten kan orsaka där noll inte innebär någon skada och inte

kräver några särskilda skyddsåtgärder. För information i skyddsklass ett och två kan brister medföra skada respektive allvarlig skada för verksamheten, förvaltningen, annan organisation eller enskild och kräver däremot skyddsåtgärder.

Med skada avses att informationen sprids på ett otillbörligt sätt, förvanskas, förstörs eller är otillgänglig när den behövs.

Exempel på informationstillgångar som kan komma att klassas skyddsklass ett eller två.

- Personuppgifter (omfattas förutom av regler för informationssäkerhet också av GDPR)
- Kontinuitetsplaner (se nedan)
- Information om sårbarheter, risker och skyddsåtgärder
- Larmlistor
- Krisledningsplan
- Upphandlingsinformation

För ytterligare råd se följande dokument på stadens intranät. De finns under Hela staden – Säkerhet, samhällsskydd och beredskap – Informationssäkerhet

- Råd för hur man genomför en informationsklassning
- Råd – Exempel på informationsklassning

Riskanalys

Genom riskanalys ska verksamheten bedöma vilka händelser som kan innebära skada kopplat till information i skyddsklass ett eller två. Riskerna ska värderas utifrån sannolikhet och konsekvens (COSO).

Riskanalyser ska genomföras kontinuerligt, minst i samband med nulägesanalysen.

Riskanalyser ska också genomföras inför:

- Införande av nytt informationssystem
- Förändrad organisation
- Förändrad verksamhet
- Förändrat regelverk

Risker kan till exempel vara:

- Obehörig får del av personuppgifter (egna eller andras) genom felaktig användarhantering av tjänst.
- Obehörig får del av personuppgifter (egna eller andras) genom brister i behörighetshantering.
- Information är inte uppdaterad på alla medier där den finns.
- Information är inte tillgänglig på grund av otillgängligt nätverk.

För ytterligare råd se följande dokument på stadens intranät. De finns under Hela staden – Säkerhet, samhällsskydd och beredskap – Informationssäkerhet

- Råd för riskanalys avseende informationssäkerhet.

Skyddsåtgärder

Informationsägaren (respektive chef) ansvarar för att erforderligt skydd finns. I huvudsak handlar det om att säkerställa att bara behörig person har tillgång till information och att informationen är tillgänglig, uppdaterad och riktig. I IT-system styrs tillgången av behörigheter. Verksamheten ansvarar för behörighetskontroll. För tillgång till information på andra medier, till exempel papper, USB-minne, ansvarar verksamheten för att bara behöriga personer har tillträde till lokal, förvaringsskåp etc där informationen förvaras.

När det gäller kommungemensamma IT-system och tjänster ansvarar utvecklingsledare IT för att följa upp att överenskomna regel- och säkerhetsmässiga krav uppfylls gentemot Intraservice.

För icke-kommungemensamma IT-system och tjänster ansvarar verksamheten för att regel- och säkerhetsmässiga krav enligt stadens riktlinje för informationssäkerhet är uppfyllda.

Verksamheten ansvarar för att säkerställa att information är uppdaterad och riktig.

För ytterligare råd se följande dokument på stadens intranät. De finns under Hela staden – Säkerhet, samhällsskydd och beredskap – Informationssäkerhet

- Råd - Förslag på lokala anvisningar/bestämmelser

Hantering av incidenter

Vid misstanke om incident kontaktar ansvarig chef utvecklingsledare IT och/eller utvecklingsledare säkerhet. I samråd tar de beslut om hur incidenten ska hanteras

För Hälso- och sjukvård gäller särskilda rutiner vid incidenter enligt NIS-reglering. E SDF Örgryte-Härlandas rutin för rapportering av incidenter enligt NIS-direktivet.

Kontinuitetsplanering

Verksamhetsansvarig chef ansvarar för att besluta om tillgänglighetskrav, det vill säga den längsta tid som information i skyddsklass ett och två kan vara otillgänglig eller informationssystemet bedöms kunna vara ur funktion innan verksamheten påverkas i oacceptabel omfattning.

Alla verksamheter ska ha en kontinuitetsplan för information i skyddsklass ett och två som säkerställer verksamheten utifrån tillgänglighetskraven.

Kontinuitetsplaneringen kan behöva innehålla både redundant information och återstarts- och reservrutiner.

Revidering av kontinuitetsplaner
Kontinuitetsplaner ska hållas aktuella och helt eller delvis testas årligen samt finnas tillgänglig för berörda i händelse av avbrott.

Redundans
Kontinuitetsplanen ska beskriva hur information som normalt finns på elektroniskt media också finns tillgänglig på papper på dedicerad plats. Exempel på sådan information:

- Rutiner

- Planeringen för det närmaste dygnet och till och med första vardagen efter helgdag.
- Handlingsplaner för avvikande händelser
- Dokumentation över system/instruktioner
- Kontaktlistor

För information i skyddsklass två ska informationen finnas på två platser med vederhäftigt inbrotts- och brandskydd.

Återstarts- och reservrutiner
Kontinuitetsplaner som inkluderar IT-baserade informationssystem ska omfatta återstarts- och reservrutiner för driftverksamheten som vidtas inom ramen för ordinarie drift så att återstart kan ske inom fastställd tid

Återstarts- och reservrutiner för IT-baserade informationssystem såsom säkerhetskopiering och återläsning ska finnas och vara dokumenterade samt verifierade och anpassade för aktuell verksamhet.

Utvecklingsledare IT ansvarar för att följa upp återstarts- och reservrutiner, inklusive säkerhetskopiering och återläsning, som avtalats med Intraservice.

Verksamhetsansvarig chef ansvarar för att följa upp återstarts- och reservrutiner, inklusive säkerhetskopiering och återläsning, för icke-kommungemensamma IT-system.

Förteckning över informationssystem

Förvaltningen ska ha en förteckning över information i skyddsklass ett eller två och hur den hanteras.

Förteckningen ska innehålla uppgifter om

- Information
- Skyddsklass för konfidentialitet, riktighet och tillgänglighet
- System för hantering
- Systemägare
- Tillgänglighetskrav
- Skyddsåtgärder
- Informationsägare
- Kontinuitetsplanering

Utvecklingsledare IT ansvarar för förteckningen. Respektive informationsägare ansvarar för att tillhandahålla och revidera uppgifterna.

Utbildning

Alla medarbetare ska årligen gå den datorstödda informationssäkerhetsutbildningen DISA. Utbildningen finns på stadens intranät. Var och en ansvarar för att gå den vid lämplig tidpunkt. Verksamhetsansvarig chef ansvarar för att följa upp att underställda medarbetare har gått.

Chefer ska vartannat år gå grundutbildning i informationssäkerhet där fokus ligger på ansvar enligt stadens styrdokument. Utvecklingsledare IT och utvecklingsledare säkerhet

ansvarar för att arrangera utbildningar. Nyanställda chefer ska gå grundutbildningen inom ett år.

Uppföljning

Intern kontroll
Stadsdelsdirektören ska årligen i sitt förslag till nämnden om intern kontrollplan föreslå ett moment som rör informationssäkerhet. Momenten tas fram genom ordinarie arbete med risk- och väsentlighetsanalys.

Uppföljning av behörigheter

Respektive chef ska

- Inventera personalens behörigheter. Utvecklingsledare IT ska kunna vara behjälplig med att få fram underlag. Även temporär/inlånad/inhyrd personal ska inkluderas.
- Följa upp att behörigheter för personalen som lämnat under året är inaktiverade/borttagna. Även temporär/inlånad/inhyrd personal ska inkluderas.
- Göra en bedömning om eventuella behörighetsförändringar som kan vara nödvändiga beroende på förändrat uppdrag, ansvar, avslut etc

Utvecklingsledare säkerhet ska

- Genomföra ett stickprov på tre enheter i verksamheten om ovan nämnda uppföljning (eller motsvarande) genomförts och dokumenterats. Avvikelser ska rapporteras till verksamhetens ledning. Stickprovet ska dokumenteras och sparas

Säkerhetsnivå
Ansvarig chef ansvarar för att incidenter och skador diarieförs.

Utvecklingsledare IT ska årligen följa upp att regel- och säkerhetsmässiga krav uppfylls för kommungemensamma IT-system och tjänster. En sammanställning över brister ska rapporteras till utvecklingsledare säkerhet för att inkluderas i rapport till nämnden tillsammans med rapport över incidenter och skador.

Utvecklingsledare säkerhet sammanställer årligen rapport över incidenter och skador. Stadsdelsdirektören rapporterar till nämnden.

Utvecklingsledare säkerhet ska årligen följa upp med verksamhetsansvariga chefer om deras medarbetare har gått informationssäkerhetsutbildningen DISA och omfattningen av chefer som har gått grundutbildning i informationssäkerhet.

Utvecklingsledare säkerhet ska årligen följa upp att verksamheterna har en kontinuitetsplanering.

Bilaga: Organisation inom informationssäkerhet med klargjorda roller och ansvar.