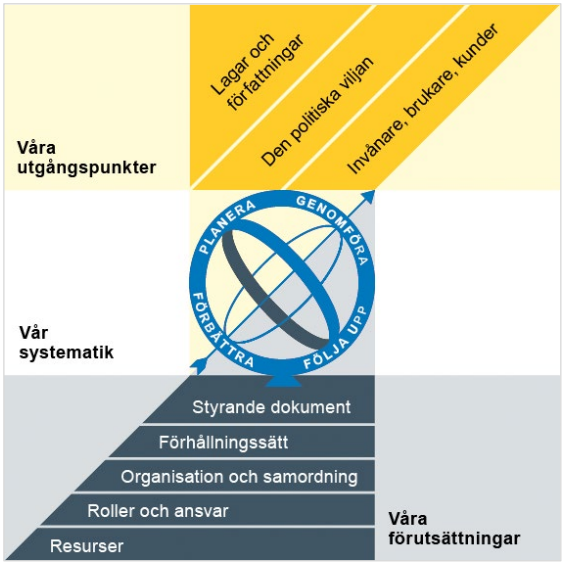
Göteborgs Stad

Göteborgs Stads rutin för hantering av informations- och cybersäkerhetsincidenter

Reglerande styrande dokument

Policy
Riktlinje
Regel
Anvisning
► **Rutin**

Göteborgs Stads styrsystem



Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.

Styrande dokument			
Kommunala föreskrifter	Riktade styrande dokument	Planerande styrande dokument	Reglerande styrande dokument

Dokumentnamn: Göteborgs Stads rutin för hantering av informations- och cybersäkerhetsincidenter

Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Stadsdirektör	Berörda nämnder och styrelser	SLK-2026-00691	2026-06-15
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Göteborg	Tills vidare		Säkerhetschef

Bilagor:

Innehåll

Inledning

Syftet med denna rutin

Denna rutin syftar till att säkerställa att Göteborgs Stad har ett enhetligt, systematiskt och ändamålsenligt arbetssätt för hantering av informations- och cybersäkerhetsincidenter. Rutinen fastställer hur incidenter ska identifieras, hanteras, anmälas och följas upp i enlighet med gällande lagkrav.

Syftet med rutinen är även att tydliggöra roller och ansvar i incidenthantering samt säkerställa en hantering av incidenters eventuella konsekvenser i linje med befintliga arbetssätt för krishantering i Göteborgs Stad.

Vem omfattas av rutinen

Denna rutin gäller tills vidare för nämnder inom Göteborgs Stad. Rutinen gäller tills vidare för styrelserna i Göteborgs Stad vid användning av stadens gemensamma system och infrastruktur. Detta då kommunstyrelsen, i enlighet med cybersäkerhetslagen, ytterst ansvarar för att cybersäkerheten upprätthålls i dessa system. Liknande förhållanden kan gälla omvänt där ett bolag tillhandahåller ett system som används av andra verksamheter.

Bakgrund

Genom NIS2-direktivet och cybersäkerhetslagen (2025:1506) ställs utökade krav på att verksamhetsutövare bedriver ett systematiskt och riskbaserat arbete med att skydda sina nätverks- och informationssystem. Göteborgs Stads nämnder utgör tillsammans en offentlig verksamhetsutövare och omfattas därmed av dessa krav. Verksamhetsutövare ska vidta lämpliga och proportionella tekniska, organisatoriska och driftsrelaterade säkerhetsåtgärder för att skydda nätverks- och informationssystem samt tillhörande fysiska miljöer mot incidenter. För att efterleva Cybersäkerhetslagen krävs det att Göteborgs Stad har ett gemensamt arbetssätt för incidenthantering.

En central del av ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete är en enhetlig rutin för incidenthantering som säkerställer att oönskade händelser och incidenter identifieras, hanteras och anmäls strukturerat och skyndsamt. Detta möjliggör att konsekvenser av incidenter begränsas, återställningstider förkortas och påverkan på verksamheten minimeras. Incidenthanteringsrutiner bidrar till att upprätthålla tillgänglighet, riktighet och konfidentialitet i Göteborgs Stads information, nätverk- och informationssystem samt till att stärka verksamhetens motståndskraft mot incidenter i såväl fredstid som vid kris och höjd beredskap.

En tydlig process för incidenthantering är även en förutsättning för att uppfylla lagkrav på rapportering av betydande incidenter till behöriga myndigheter samt för att möjliggöra ett kontinuerligt lärande som stärker det förebyggande informations- och cybersäkerhetsarbetet i Göteborgs Stad.

Koppling till andra styrande dokument

I Göteborgs Stads riktlinje för informations- och cybersäkerhet fastställs ramarna för stadens hantering av informations- och cybersäkerhetsincidenter.

I Göteborgs Stads riktlinje för krishantering förtydligas nämnders och bolagsstyrelsers ansvar samt vilka funktioner och vilken förmåga som krävs för att bedriva samverkan och ledning vid samhällsstörningar (krishantering).

Göteborgs Stads riktlinje för kriskommunikation beskriver hur nämnder och styrelser ska kommunicera vid kris och samhällsstörningar och kompletterar Göteborgs Stads riktlinje för krishantering.

Lagbestämmelser

Området cybersäkerhet regleras i cybersäkerhetslagen, cybersäkerhetsförordningen samt tillhörande föreskrifter. Cybersäkerhetslagen är den svenska implementeringen av EU direktivet NIS2[1]. I anslutning till NIS2 finns även EU-kommissionens genomförandeförordning som preciserar direktivets tillämpning. För de nämnder och styrelser som omfattas av cybersäkerhetslagen gäller utökade krav i enlighet med de specifika föreskrifter som gäller för respektive verksamhet.

Dokumentation

Samtliga steg i incidenthanteringen ska dokumenteras noggrant med datum och klockslag. Det ska finnas en detaljerad beslutslogg och lista på åtgärder som vidtagits vid varje enskild incident för att få en tydlig spårbarhet.

Vad är en informations- och cybersäkerhetsincident

Enligt cybersäkerhetslagen är en incident, en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

I Göteborgs Stad avser en informations- och cybersäkerhetsincident en incident enligt cybersäkerhetslagen. I detta dokument benämns sådana händelser fortsättningsvis som ”incidenter”.

Exempel på incidenter är:

- röjande av lösenord eller pinkoder,
- förlust av passerkort eller viktig information,

[1] [1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

- att en användare klickar på en skadlig länk i ett e-postmeddelande,
- felaktigt tilldelade behörigheter,
- att obehöriga personer vistas i verksamhetens lokaler,
- publicering av konfidentiell information i externa kanaler,
- delning av konfidentiell information i generativa AI-tjänster,
- att en medarbetare avsiktligt tillskansar sig information som denne inte har rätt att ta del av,
- överbelastningsattacker (DDoS-attacker) mot Göteborgs Stads webbsidor
- cyberattacker mot kommunens nätverk- och informationssystem, exempelvis ärendehanteringssystem,
- tekniska fel som orsakar driftavbrott i mer än fyra timmar

Observera att det som anges i listan ovan endast är exempel på händelser som utgör incidenter. Även andra händelser som påverkar information eller system kan utgöra en incident.

En betydande incident enligt cybersäkerhetslagen är en incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för Göteborgs Stad, eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada.

I de fall där incidenten även innefattar personuppgifter behöver incidenten även hanteras som en personuppgiftincident och anmälas i enlighet med dataskyddsförordningen (GDPR).

Rutin

Incidenthanteringsprocessen

Förebygga och upptäcka incidenter

Inom Göteborgs Stad ska arbete med omvärldsbevakning, övervakning av nätverks- och informationssystem samt identifiering av hot och sårbarheter bedrivas inom ramen för incidenthantering i respektive nämnd. Detta inkluderar användning av automatiserade verktyg för hot- och sårbarhetsanalys samt att tillgodogöra sig relevant information från

exempelvis Sveriges nationella CSIRT (Computer Security Incident Response Team), CERT-SE.

Som en del av det förebyggande arbetet ska respektive nämnd säkerställa att nödvändiga organisatoriska förutsättningar finns på plats, såsom fastställda roller, mandat, kontaktvägar och rutiner för kommunikation vid incidenter. Både inom och utanför ordinarie arbetstid.

Vidare ska erfarenheter från inträffade incidenter omsättas i förbättringsåtgärder i syfte att stärka det förebyggande arbetet och förbättra förmågan att förebygga att liknande händelser sker i framtiden.

Alla nämnder i Göteborgs Stad ska upprätta en incidenthanteringsplan. Det vill säga en plan som innefattar en strukturerad process för att förbereda sig på, upptäcka, hantera och återhämta sig från informations- och cybersäkerhetsincidenter. För stöd kring upprättande av en incidenthanteringsplan, se rekommendationer kring detta hos Nationellt cybersäkerhetscenter (NCSC) alternativt de metodstöd Myndigheten för civilt försvar tillhandahåller kring informationssäkerhetsincidenter.

Anmälan i ISDB

Incidenter ska hanteras och dokumenteras i systemstödet ISDB (Informationssäkerhetsdatabasen). Cybersäkerhetslagen kräver att incidenter dokumenteras noggrant och på ett spårbart sätt, för att i ett senare skede kunna utreda, följa upp samt arbeta systematiskt med riskhantering och erfarenhetsåterföring kring incidenter. Nedan följer beskrivning av Göteborgs Stads incidenthanteringsrutin och dess förfarande i ISDB.

I händelse av en incident ska följande göras.

Berörd förvaltning

- Anmäl incident via formulär som nås via genväg på Göteborgs Stads intranät. Vid osäkerhet kring anmälan, kontakta närmaste chef eller verksamhetens informationssäkerhetssamordnare. Anmälan förs med automatik in i ISDB**.** En e-postnotifiering skickas automatiskt från ISDB till verksamhetens incidenthanteringsfunktion och anmäld funktionsbrevlåda.

- Incidenthanteringsfunktionen[2] loggar in i ISDB för fortsatt hantering, vilket innefattar:
    - utredning och bedömning av incidenten och dess allvarlighetsgrad samt omfattning och om den är betydande
    - vidtagande av akuta åtgärder
    - identifiering av grundorsaker till incidenten och
    - vidtagande av långsiktiga åtgärder för att incidenten inte ska inträffa igen.

  Detta ska göras så fort incidenten har upptäckts.

[2] Enligt roll i Göteborgs Stads riktlinje för informations- och cybersäkerhet.

Om ISDB av någon anledning inte är tillgängligt vid tillfället när incidenten sker, ska incidenten hanteras enligt denna rutin manuellt. När systemet åter är tillgängligt ska dokumentationen registreras i efterhand i ISDB.

OBS

Anmälan och dess förfarande avser anmälan av en informations- och cybersäkerhetsincident i ISDB.

Upplysning avser den upplysning som ska göras till tillsynsmyndighet inom 24 timmar.

Rapportering avser rapportering och dess olika skeden till tillsynsmyndigheten.

Hantering och bedömning av incident

Ansvar för hantering av incidenten ska fastställas utifrån incidentens karaktär. Ansvarsfördelningen ska tillämpas i enlighet med de roller och ansvar som anges i Göteborgs Stads riktlinje för informations- och cybersäkerhet. Följande ansvar- och rollfördelning ska följas i arbetet med hantering av incidenter.

Systemägare

- För incidenter som kan härledas till ett system ansvarar systemägaren för hanteringen. Då en incident påverkar flera förvaltningar inom Göteborgs Stad är det systemägaren som samordnar incidenthanteringen och ansvarar för en sammanhållen rapportering till tillsynsmyndighet. Hantering av incidenten infattar även att informera andra berörda verksamheter av incidenter för att dessa ska få kännedom av incidenten.
- Gällande ramavtal i Göteborgs Stad och incidenter, är det den som avropat på ett ramavtal och köpt in ett system som själva är systemägare och den part som ska hantera incidenten.
- Om en verksamhet är tjänsteleverantör till andra verksamheter inom staden ansvarar tjänsteleverantören, i egenskap av systemägare, för att hantera incidenten.

Informationsägare

- För incidenter som saknar koppling till ett specifikt system ansvarar informationsägaren för incidenthanteringen.

Stadsledningskontoret

- Stadsledningskontoret har utifrån cybersäkerhetslagen och ledningens ansvar för säkerhetsåtgärder, ett övergripande ansvar för incidenthanteringen. Eftersom incidenthantering är en av de säkerhetsåtgärder som lagen kräver ska vidtas, ansvarar stadsledningskontoret även för att följa upp och övervaka

incidenthanteringsprocessen samt varje enskild betydande incident. Därför behöver stadsledningskontoret informeras om samtliga betydande incidenter. Stadsledningskontoret är även en rådgivande part i incidenthanteringen.

Betydande incident

Vid inträffad incident ska incidenthanteringsfunktionen inom berörd verksamhet genomföra en bedömning av incidentens omfattning och allvarlighetsgrad. I bedömningen ska incidentens potentiella och faktiska konsekvenser inom den egna verksamheten beaktas, liksom eventuell påverkan på andra verksamheter. Denna bedömning ska göras utifrån skada på verksamhet, samhälle, individ, ekonomi och varumärke.

I enlighet med cybersäkerhetslagen ska det i bedömningen ingå att fastställa om incidenten utgör en betydande incident samt att identifiera vilken eller vilka sektorer och sektorkritiska system som berörs av den betydande incidenten.

Vid anmälningsförfarandet behöver den verksamhet som är ansvarig för incidenthanteringen och därav rapportering till tillsynsmyndigheten, i sin rapportering, gå igenom samtliga steg som beskrivs i föreskrifterna: Myndigheten för civilt försvars föreskrifter om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare (MCFFS 2026:8) samt föreskrifter från Post- och telestyrelsen för de verksamheter i Göteborgs Stad som omfattas av sektorsverksamhet inom digital infrastruktur. I rapportering till den myndighet är det viktigt att beakta sektorsspecifika kriterier för incidentrapportering.

1. **Upplysning till utpekad myndighet för incidenthantering**

Enligt cybersäkerhetslagen ska Göteborgs Stad upplysa utpekad myndighet om en betydande incident så snart det kan ske, dock senast 24 timmar efter det att Göteborgs Stad har fått kännedom om incidenten.

2. **Incidentrapportering till utpekad myndighet för incidenthantering**

Incidentanmälan göras senast 72 timmar efter att Göteborgs Stad har fått kännedom om incidenten. Underlag till rapporten kan hämtas ut från ISDB.

3. **Delrapport och slutrapport till utpekad myndighet för incidenthantering**

Göteborgs Stad ska lämna en delrapport med relevanta statusuppdateringar för den betydande incidenten på begäran av utpekad myndighet. Senast en månad efter incidentanmälan ska Göteborgs Stad lämna en slutrapport till samma myndighet. Om den betydande incidenten fortfarande är pågående ska i stället en lägesrapport lämnas vid denna tidpunkt och därefter en slutrapport inom en månad efter det att incidenten har hanterats.

Den verksamhet där incidenthanteringsansvaret är placerat ska säkerställa att rapportering sker inom föreskrivna tidsramar. Förtydliganden av tidsfrister och rapporteringskrav gällande sektorsspecifika kriterier, se tillämpliga föreskrifter.

Från Göteborgs Stad ska endast en (1) upplysning, en (1) incidentrapport och en (1) slutrapport skickas till utpekad myndighet för incidenthantering vid betydande incidenter som berör flera verksamheter.

När en betydande incident är rapporterad ska en kopia på rapporten skickas till CISO på stadsledningskontoret som har uppföljningsansvaret gällande alla betydande incidenter.

Rådgivning

Vid behov av stöd och råd gällande betydande incident kontakta stadens CISO dagtid alternativt CERT-SE. För rådgivning utanför arbetstid kontakta CERT-SE.

Informera inriktning- och samordningskontakt (ISK) samt stadens CISO

Vid varje incident som bedöms som betydande ska inriktning- och samordningskontakten (ISK) i den verksamhet där incidenten hanteras informeras, detta ska göras av incidenthanteringsfunktionen i respektive verksamhet. Stadens CISO ska skyndsamt informeras om alla betydande incidenter inom Göteborgs Stad.

ISK i respektive verksamhet ska i sin tur göra en bedömning huruvida stadsledningskontorets tjänsteperson i beredskap (TiB) ska informeras utifrån vad konsekvenserna av incidenten har inneburit eller kan innebära för staden.

Vid ”inte betydande” incident

Incidenter som inte bedöms vara betydande hanteras enligt denna rutin, bortsett från rapporteringskraven till utpekad myndighet för incidentrapportering. Dock ska bedömningen att incidenten inte är rapporteringspliktig dokumenteras.

Krishantering vid cybersäkerhetsincident

Enligt cybersäkerhetlagen och tillhörande föreskrifter ska incidenthanteringsprocessen integreras med krishanteringsprocessen. Det finns krav på att Göteborgs Stad ska kunna minimera konsekvenser av incidenter som inte kan omhändertas inom incidenthanteringsprocessen. Göteborgs Stad ska tydliggöra hur roller, ansvarsområden och befogenheter fördelas under en kris samt hur kriskommunikation ska genomföras. Detta krav omhändertas genom Göteborgs Stads riktlinje för krishantering samt respektive verksamhets egen krishanteringsplan. En incidents konsekvenser kan behöva hanteras utifrån denna styrning också inom berörda verksamheter. Därför är det viktigt att incidenthanteringsfunktionen informerar sin verksamhets ISK vid betydande incidenter. Respektive verksamhets ISK ansvarar för att vid behov informera stadsledningskontorets TiB.

De uppgifter som respektives verksamhets ISK och stadsledningskontorets TiB dokumenterar kan vara värdefull att få med i incidentrapporten till tillsynsmyndigheten. Det är därför viktigt att inhämta och värdera informationen, vilket incidenthanteringsfunktionen ansvarar för.

Kommunikation

Ansvar för information och kommunikation om en cybersäkerhetsincident följer ordinarie verksamhetsansvar och systemägarskapet. Systemägaren ansvarar för att informera berörda verksamheter i linjen och de målgrupper som är påverkade av incidenten.

Behovet av kommunikation kan variera beroende på incidentens omfattning och konsekvenser. Det kan därför vara bra att överväga såväl intern som extern kommunikation, särskilt när incidenten påverkar många, väcker frågor eller kräver samordnade budskap. Vid betydande incidenter kan en kommunikationsplan vara ett stöd i arbetet. Det kan också vara värdefullt att i förväg ha tagit fram budskapsstöd eller kommunikationsplaner för olika scenarier.

Lärdomar och erfarenhetsåterföring

Det sista steget i incidenthanteringsprocessen är att avsluta incidenten genom att samla in de lärdomar och erfarenheter som hanteringen av incidenten har gett. Det innebär att både positiva och negativa lärdomar från incidenten ska dokumenteras och analyseras, vilket incidenthanteringsfunktionen ska göra i ISDB. Resultat ska vara underlag till förbättringsåtgärder i tillämpliga delar i organisationen, för att samma händelse inte ska ske i framtiden.

I händelse av en betydande incident ska relevanta erfarenheter av incidenten spridas till berörda verksamheter i Göteborg Stad. Riskanalyser som har koppling till incidenten ska uppdateras efter inträffad incident för att hålla analyser uppdaterade och relevanta.