Handling 2026 nr 4

Revidering av Göteborgs Stads riktlinje för informationssäkerhet samt komplettering av kommunstyrelsens reglemente utifrån nya cybersäkerhetslagen

Till Göteborgs kommunfullmäktige

Kommunstyrelsens förslag

Kommunstyrelsen tillstyrker stadsledningskontorets förslag i tjänsteutlåtande den 8 december 2025 och föreslår att kommunfullmäktige beslutar:

1. Göteborgs Stads riktlinje för informationssäkerhet revideras i enlighet med bilaga 2 till stadsledningskontorets tjänsteutlåtande.
2. Kapitel 2 i Reglemente för Göteborgs Stads kommunstyrelse revideras med ett tillägg av en ny paragraf nummer 21 under rubriken Cybersäkerhet i enlighet med vad som framgår av stadsledningskontorets tjänsteutlåtande.

Göteborg den 14 januari 2026
Göteborgs kommunstyrelse

Jonas Attenius

Mathias Sköld

Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2025-12-08
Ärendenummer SLK-2025-01130

Handläggare
Linda Larsson, Amanda Lilleberg
Telefon: 031-368 03 09, 031- 368 04 71
E-post: fornamn.efternamn@stadshuset.goteborg.se

Revidering av Göteborgs Stads riktlinje för informationssäkerhet samt komplettering av kommunstyrelsens reglemente utifrån den nya cybersäkerhetslagen

Förslag till beslut

I kommunstyrelsen och kommunfullmäktige:

1. Göteborgs Stads riktlinje för informationssäkerhet revideras i enlighet med bilaga 2 till stadsledningskontorets tjänsteutlåtande.
2. Kapitel 2 i Reglemente för Göteborgs Stads kommunstyrelse revideras med ett tillägg av en ny paragraf nummer 21 under rubriken Cybersäkerhet i enlighet med vad som framgår av stadsledningskontorets tjänsteutlåtande.

Sammanfattning

En ny cybersäkerhetslag föreslås träda i kraft den 15 januari 2026. Lagen är en implementering av EU:s NIS2[1]-direktiv (EU 2022/2555) och innebär att regelverket för cybersäkerhet i Sverige utökas. Mot bakgrund av den nya lagen bedömer stadsledningskontoret att kommunfullmäktige behöver besluta om vissa justeringar i Göteborgs Stads riktlinje för informationssäkerhet samt om ett tillägg i kommunstyrelsens reglemente. Syftet med revideringarna är att förtydliga roller och ansvar för kommunstyrelsen samt för nämnder och styrelser utifrån kraven i den nya lagstiftningen.

Regeringen presenterade ett färdigt lagförslag i mitten av oktober 2025, vilket innebär en kort förberedelsetid inför det att lagen träder i kraft. Ytterligare föreskrifter och vägledning kommer att tillkomma efter att lagen börjat gälla. Mot den bakgrunden har stadsledningskontoret i detta skede prioriterat att identifiera de viktigaste åtgärderna som behöver beslutas av kommunfullmäktige inför att cybersäkerhetslagen träder i kraft, för att staden vid ikraftträdandet ska ha grundläggande förutsättningar att möta lagens krav. Parallellt är flera parter involverade i ett omfattande arbete i Göteborgs Stad med fokus på mer verksamhetsnära frågor. Det handlar bland annat om att förbereda informationsinsatser, utbildning, arbetsprocesser och annat stöd.

Med hänsyn till tidpunkten för lagens ikraftträdande behöver ärendet hanteras så skyndsamt som möjligt. I annat fall finns en risk att tillsynsmyndigheterna bedömer att Göteborgs Stad inte gjort en tillräcklig ansats för att uppfylla kraven i cybersäkerhetslagen. Det kan i sin tur leda till sanktionsavgift eller andra åtgärder.

[1] Network and Information Systems Directive 2

Bedömning ur ekonomisk dimension

Stadsledningskontoret bedömer att ett beslut om en justerad styrning på lokal nivå, där bland annat roller och ansvar tydliggörs, inte är kostnadsdrivande i sig självt. De kostnadseffekter som kan uppstå är i stället kopplade till den nya cybersäkerhetslagen som ställer ökade krav på exempelvis ett riskbaserat arbetssätt, incidenthantering och dokumentation. En otillräcklig cybersäkerhet kan leda till betydande incidenter vilket i sin tur kan ge andra ekonomiska konsekvenser, till exempel kostnader vid driftstörningar eller incidenter som påverkar verksamheten. Bristande efterlevnad av lagen eller kommande föreskrifter kan även medföra sanktionsavgifter. För att minska sådana risker är en tydlig och ändamålsenlig styrning avgörande. Sammantaget är det därför viktigt att den stadenövergripande styrningen på området tidigt fastslår roller och ansvar samt innehåller de skrivningar som krävs för att uppfylla de grundläggande kraven i cybersäkerhetslagen. När lagen träder i kraft och föreskrifter meddelats kan det bli aktuellt med kompletterande styrning.

Bedömning ur ekologisk dimension

Stadsledningskontoret har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Den nya cybersäkerhetslagen ställer högre krav på hur kommunen skyddar information som rör personer som bor i kommunen, verkar här, får service av kommunen eller besöker den, liksom information om kommunens verksamheter och anställda. Genom att uppdatera stadens riktlinjer för att implementera och följa kraven i den nya lagstiftningen stärks förutsättningarna för en säker och tillgänglig digital förvaltning. Boende, besökare och näringsliv kan därmed känna sig ännu tryggare i hur deras information i stadens informationssystem skyddas. En god informations- och cybersäkerhet minskar risken för att grupper eller individer drabbas oproportionerligt av intrång, felaktig hantering eller otillgängliga tjänster. Det bidrar även till kommunens förmåga att upprätthålla samhällsviktiga funktioner vid störningar. Det kan i förlängningen stärka trygghet och tillgänglighet för olika grupper i samhället och bidrar till förtroendet för den offentliga sektorn.

Samverkan

Information i centrala samverkansgruppen (CSG) 2025-11-27 och koncernfackliga rådet 2025-12-03.

Bilagor som ingår i beslutsunderlaget

1. Markerade förslag till ändringar i Göteborgs Stads riktlinje för informations- och cybersäkerhet
2. Förslag till Göteborgs Stads riktlinje för informations- och cybersäkerhet

Beskrivning av ärendet

En ny cybersäkerhetslag föreslås träda i kraft den 15 januari 2026. Med anledning av den nya lagen bedömer stadsledningskontoret att kommunfullmäktige behöver besluta om vissa justeringar i Göteborgs Stads riktlinje för informationssäkerhet. Vidare behöver kommunfullmäktige besluta om ett tillägg i kommunstyrelsens reglemente. Syftet med revideringarna är att förtydliga roller och ansvar i staden utifrån kraven i den nya lagstiftningen.

Cybersäkerhetslagen är en implementering av EU:s NIS2-direktiv (EU 2022/2555). NIS2-direktivet antogs den 14 december 2022 och trädde i kraft den 18 oktober 2024. Det ersatte det tidigare NIS[2]-direktivet från 2016, som var EU:s första gemensamma regelverk för cybersäkerhet. Det första NIS-direktivet implementerades i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och den tillhörande förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen). Beslut om cybersäkerhetslagens ikraftträdande förväntas fattas av riksdagen i december 2025. När den nya lagen träder i kraft upphör den tidigare NIS-lagen samt NIS-förordningen att gälla.

Beredning av ärendet

Cybersäkerhetslagen är en ny lagstiftning som omfattar flera verksamhetsområden. Det färdiga lagförslaget presenterades av regeringen i mitten av oktober 2025 och förväntas träda i kraft den 15 januari 2026. Ytterligare föreskrifter och vägledning kommer tillkomma efter att lagen börjat gälla. Mot den bakgrunden har stadsledningskontoret i detta skede prioriterat de viktigaste åtgärderna som behöver beslutas av kommunfullmäktige inför att cybersäkerhetslagen träder i kraft. Syftet är att ge staden förutsättningar att möta lagens krav.

Att vissa prioriteringar har varit nödvändiga initialt för att möta grundläggande krav i cybersäkerhetslagen medför att det kan finnas behov av ytterligare justeringar framöver, bland annat kopplat till de krav som följer av kommande föreskrifter. Stadsledningskontoret kommer att behöva bedöma detta när lagen har trätt i kraft samt föreskrifter meddelats. Därefter kommer stadsledningskontoret vid behov återkomma med förslag till ytterligare beslut gällande styrningen inom området.

Utöver de justeringar av styrdokument som föreslås i detta ärende är flera parter i staden involverade i ett omfattande arbete med fokus på mer verksamhetsnära frågor. Det handlar bland annat om att förbereda informationsinsatser, utbildning, arbetsprocesser och annat stöd för att ge förutsättningar att efterleva de nya krav som framgår av lagstiftningen.

Angränsande ärenden

Ett förslag till revidering av Göteborgs Stads regel för IT-användare behandlades i kommunstyrelsen 2025-09-24 § 70 som avslog revideringen. Stadsledningskontoret fick i uppdrag att återkomma med nytt förslag på regelverk som lever upp till legala förutsättningar och som är tillämpbart i ett praktiskt verksamhetsperspektiv. Inför det ska ytterligare underlag och analyser från andra kommuner samt Sveriges kommuner och regioner inhämtas. Tillkommande säkerhetskrav enligt cybersäkerhetslagen och kommande föreskrifter kan påverka hur reglerna behöver utformas. Ärendet om ett nytt förslag på regelverk är under beredning och har ännu inte ett planerat datum för behandling i kommunstyrelsen.

[2] The Directive on security of network and information systems

NIS2, ny cybersäkerhetslag och kommande föreskrifter

NIS och NIS2

Syftet med det tidigare NIS-direktivet var att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU. Direktivet omfattade leverantörer av samhällsviktiga tjänster inom sju särskilt definierade sektorer: energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Direktivet gällde dessutom för leverantörer av digitala tjänster. Regleringen innebar att vissa leverantörer av samhällsviktiga och digitala tjänster skulle vidta säkerhetsåtgärder för att hantera risker och förebygga incidenter i de nätverk och informationssystem som används för att tillhandahålla tjänsterna. Leverantörerna skulle även rapportera incidenter som hade en betydande eller avsevärd inverkan på tjänsternas kontinuitet.

Det nya NIS2-direktivet är en uppdatering av NIS-direktivet och syftar till att säkerställa en hög nivå av cybersäkerhet i hela EU. NIS2-direktivet skiljer sig från NIS-direktivet på flera sätt. Regleringen omfattar betydligt fler aktörer och ställer skärpta och tydligare krav på riskanalyser samt vilka säkerhetsåtgärder aktörer ska vidta. Även kraven på hur incidentrapportering ska genomföras skärps och förtydligas. Till skillnad från NIS-direktivet gäller den nya regleringen hela verksamheten hos en aktör och inte enbart säkerheten i de nätverk och informationssystem som används för en samhällsviktig eller digital tjänst. Vidare omfattade NIS sju sektorer, där NIS 2 nu omfattar 18 sektorer uppdelade på väsentliga och viktiga sektorer. En av de nya sektorerna är offentlig förvaltning. Utifrån ett kommunalt perspektiv är det därutöver vatten- och avloppsförsörjning och avfallshantering som är de mest relevanta områden som tillkommit. Sedan tidigare ingick bland annat digital infrastruktur, dricksvatten, energi, hälso- och sjukvård och transport. Det betyder sammantaget att många kommunala verksamheter som tidigare inte omfattades av NIS nu kommer att behöva uppfylla de nya kraven utifrån NIS2.

NIS2 ställer skärpta krav på styrning och ledning. Verksamhetsutövarens högsta ledning får ett tydligt ansvar för cybersäkerheten och ska aktivt säkerställa att riskhantering, rapportering och säkerhetsåtgärder är integrerade i verksamhetsstyrningen. Vidare har tillsynsdelen stärkts, där NIS2 ger större möjligheter för tillsynsmyndigheter att genomföra mer omfattande tillsyn och att besluta om administrativa sanktionsavgifter vid brister i efterlevnad.

Cybersäkerhetslagen

Den nya cybersäkerhetslagen är som ovan nämnts regeringens förslag till ny svensk lagstiftning för att implementera NIS2. Göteborgs Stad har tidigare yttrat sig över utredningen som ligger till grund för lagförslaget Nya regler om cybersäkerhet (SOU 2024:18). Kommunstyrelsen tog beslut om yttrandet 2024-05-15 § 443.

Cybersäkerhetslagen innebär en utvidgning av reglerna för cybersäkerhet i Sverige i linje med EU:s ambitioner och krav i NIS2-direktivet. I lagen tydliggörs roller och ansvar inom det systematiska cybersäkerhetsarbetet. Lagen ställer krav på att organisationers ledning ska säkerställa att cybersäkerhet integreras i verksamhetsstyrningen och att ledningen ska genomgå relevant utbildning. Vidare bör även utbildning genomföras för medarbetare. Säkerhetsarbetet ska ha en helhetssyn som skyddar både tekniska system och fysisk miljö mot olika typer av incidenter. Tillsynen förstärks, och myndigheter får större befogenheter att följa upp efterlevnaden av reglerna och vidta åtgärder vid brister. Bland annat blir sanktionsavgifterna högre än idag i det fall kraven inte efterlevs.

För offentlig förvaltning föreslås den vara som lägst 5 000 kr och som mest 10 000 000 kr. Dessutom införs krav på kontroll av säkerheten i leverantörskedjor för att hantera tredjepartsrisker.

Det nya regelverket i förhållande till kommunstyrelsen, stadens nämnder och de kommunala bolagen

Enligt NIS2 och cybersäkerhetslagen har verksamhetsutövaren det yttersta ansvaret för informations- och cybersäkerheten. Verksamhetsutövare är ett samlingsbegrepp för både offentliga och enskilda verksamhetsutövare. Det är verksamhetsutövarens ledning som ansvarar för att kraven i cybersäkerhetslagen uppfylls och efterlevs. När det gäller kommunens nämnder utgör dessa, enligt lagens förarbeten, tillsammans en verksamhetsutövare, där kommunstyrelsen är ledning. Cybersäkerhetslagen lägger därmed ett särskilt ansvar på kommunstyrelsen att styra, följa upp och säkerställa att cybersäkerhetsarbetet bedrivs systematiskt och riskbaserat i hela nämndorganisationen. Kommunstyrelsen har det yttersta ansvaret inför tillsynsmyndigheterna.

Samtidigt bedöms ansvaret för informations- och cybersäkerhet i staden följa nämndernas ordinarie ansvar för verksamheten enligt kommunallagen. Det betyder att varje nämnd ansvarar för att säkerställa att lagens krav och stadens styrning efterlevs i sin respektive verksamhet. Den nya lagen ändrar alltså inte verksamhetsansvaret men påverkar i vissa avseenden ansvarsfördelningen mellan kommunstyrelsen och övriga nämnder.

Varje kommunalt bolag som uppfyller lagens kriterier betraktas som en egen verksamhetsutövare. Det innebär att bolagets styrelse och vd utgör ledning och har ett självständigt ansvar för att säkerställa att informations- och cybersäkerheten upprätthålls och efterlevs inom bolagets verksamhet.

När ett kommunalt bolag använder ett system som är gemensamt för hela staden och tillhandahålls av en nämnd, är ansvaret för informations- och cybersäkerheten delat mellan bolaget och nämnden. Bolaget är verksamhetsutövare och ansvarar för att säkerställa att deras egna verksamhetsprocesser och data hanteras säkert enligt lagens krav. Nämnden, som tillhandahåller systemet, ansvarar för att systemet är utformat, driftsatt och underhållet så att det uppfyller kraven på säkerhet och att tillgången till systemet sker på ett säkert sätt. Det innebär att nämnden har ansvar för att säkerställa att systemets tekniska säkerhetsåtgärder är på plats, medan bolaget ansvarar för att använda systemet på ett säkert och korrekt sätt inom sin verksamhet. Båda parter behöver därför samarbeta och samordna sina cybersäkerhetsinsatser för att uppfylla lagens krav och minimera risker. Liknande förhållanden kan också gälla omvänt där ett bolag tillhandahåller ett system som används av andra verksamheter.

Föreskrifter kopplade till cybersäkerhetslagstiftningen

Myndigheten för samhällsskydd och beredskap (MSB) har fått i uppdrag av regeringen att förbereda föreskrifter enligt den nya cybersäkerhetslagen. Uppdraget innebär att ta fram förslag till nya föreskrifter om säkerhetsåtgärder och utbildning för verksamhetsutövare samt förslag till nya föreskrifter om incidentrapportering och informationsskyldighet. Utöver detta ska MSB även utveckla ett nationellt anmälningssystem för verksamhetsutövare. Föreskrifterna är tänkta att förtydliga ansvar som ligger hos de roller som beskrivs i cybersäkerhetslagstiftningen. De kommer även sätta tydliga krav på miniminivåer för att bedriva ett systematiskt och ändamålsenligt cybersäkerhetsarbete.

Post- och telestyrelsen (PTS) har fått i uppdrag att förbereda föreskrifter för vissa sektorer och områden som inte omfattas av MSB:s uppdrag. Det gäller särskilt områden som rör digital infrastruktur, telekommunikation, domännamnssystem och post- och budtjänster. PTS ansvarar även för regler kopplade till rymdsektorn och leverantörer av vissa digitala tjänster. En central del av PTS uppdrag är att fastställa vilka händelser som ska räknas som betydande incidenter inom de sektorer de ansvarar för. PTS ska också se till att de aktörer som omfattas av reglerna har tydliga krav på säkerhetsåtgärder och informationsskyldigheter.

Göteborgs Stads styrning inom informationssäkerhet och cybersäkerhet

Informationssäkerhet är ett övergripande begrepp som omfattar skyddet av information oavsett om den ges i digital, skriftlig eller muntlig form. Cybersäkerhet är en del av informationssäkerheten och handlar specifikt om att skydda information och system i den digitala miljön mot cyberhot, attacker och obehörig åtkomst. Ett effektivt cybersäkerhetsarbete bygger därför på en bred och systematisk informationssäkerhet i hela organisationen. Göteborgs Stads nuvarande riktlinje för informationssäkerhet ska skapa förutsättningar för ett systematiskt och långsiktigt informationssäkerhetsarbete. Riktlinjen omfattar alla informationstillgångar oavsett om de behandlas manuellt eller digitalt och oberoende av i vilken form eller miljö de förekommer. Likt kommande cybersäkerhetslagstiftning poängterar riktlinjen vikten av att arbeta systematiskt och riskbaserat. Utifrån den nya cybersäkerhetslagen saknas dock vissa områden som behöver regleras. De är främst kopplade till roller och ansvar inom organisationen.

Göteborgs Stads regel för IT-användare fastställer ansvar och åtagande för IT-användare i staden samt hur dessa får använda stadens IT-resurser såsom persondator, nätverk, servrar, mobiltelefoni, programvaror, internet och så vidare. Med IT-användare i Göteborgs Stad avses anställda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i eller med stadens IT-resurser.

Föreslagna ändringar i kommunstyrelsens reglemente samt Göteborgs Stads riktlinje för informationssäkerhet

Nedan redogörs för de behov av förändringar som aktualiseras i förhållande till den nya cybersäkerhetslagen.

Kommunstyrelsens reglemente

I cybersäkerhetslagstiftningen pekas tydligt på verksamhetsutövarens ansvar inom cybersäkerhet. Det är verksamhetsutövarens ledning som ansvarar för att kraven i cybersäkerhetslagen uppfylls och efterlevs. Kommunstyrelsen utgör ledning i förhållande till stadens nämnder. Det finns skäl att synliggöra detta genom att göra ett tillägg i kommunstyrelsens reglemente som förtydligar ansvaret. Det tillägg som föreslås är:

”Kommunstyrelsen har det övergripande ansvaret för cybersäkerhet i förhållande till stadens nämnder i enlighet med cybersäkerhetslagen (XXXX:XXX)[3]”.

Tillägget skrivs in i kapitel 2 i reglementet, i en ny paragraf med nummer 21 och med en egen rubrik Cybersäkerhet. Som en följdändring justeras numret på efterföljande paragrafer i kapitel 2.

[3] Vid ärendets beredning har lagen ännu inte fått något SFS-nummer.

Göteborgs Stads riktlinje för informationssäkerhet

Nedan beskrivs de väsentliga ändringar som föreslås i riktlinjen för informationssäkerhet. Utöver dessa har ett antal språkliga justeringar och förtydliganden gjorts som inte innebär ändring i sak. För samtliga ändringar, se markeringar i bilaga 1.

Riktlinjen föreslås byta namn för att förstärka kopplingen till cybersäkerhetslagen och framåt heta Göteborgs Stads riktlinje för informations- och cybersäkerhet. I inledningskapitlet har tillägg gjorts för att bland annat förtydliga riktlinjens bakgrund, relevanta lagbestämmelser och kopplingen till andra styrande dokument. Med anledning av att nya roller tillkommit genom lagen föreslås tillägg under rubriken ”Roller och ansvar”. De rollerna är verksamhetsutövare, ledning, riskägare, informationssäkerhetssamordnare och incidenthanterare. De föreslagna tilläggen lyder följande:

– *Verksamhetsutövaren* ansvarar för informations- och cybersäkerheten. Kommunens nämnder utgör tillsammans en verksamhetsutövare, medan kommunala bolag som omfattas av lagen utgör egna verksamhetsutövare.
– *Ledningen* ansvarar ytterst för att kraven i cybersäkerhetslagen uppfylls och efterlevs. För nämnderna är det kommunstyrelsen som utgör ledning, och för kommunala bolag styrelsen och vd. Ledningen ansvarar för att leda och styra verksamhetsutövarens arbete med cybersäkerhet genom att bland annat besluta om mål och inriktning, fatta de beslut som behövs för att säkerställa att arbetet med att genomföra säkerhetsåtgärder bedrivs systematiskt och riskbaserat samt följa upp och övervaka genomförandet av säkerhetsåtgärderna. Ledningen är det organ som enligt cybersäkerhetslagen kan ställas till svars för överträdelser när det gäller verksamhetsutövarens säkerhetsåtgärder.
– *Riskägare* är den nämnd eller styrelse som ansvarar för en informations- och cybersäkerhetsrisk som identifieras och hanteras inom sitt ansvarsområde. Nämnder och bolag ska följa de beslut och den styrning som fastställs av respektive ledning.
– *Informationssäkerhetssamordnare* är en funktion som varje nämnd och styrelse ansvarar för att ha i organisationen. Funktionen har i uppgift att samordna och utvärdera arbetet med säkerhetsåtgärder som stöd för nämndens eller styrelsens arbete med informations- och cybersäkerhet.
– *Incidenthanterare* är en funktion som varje nämnd och styrelse ansvarar att ha i organisationen. Funktionen har i uppgift att hantera och åtgärda informations- och cybersäkerhetsincidenter i verksamheten.

Under rollen systemägare har förtydligande gjorts att för styrelserna gäller ett ansvar att förhålla sig till kommunstyrelsens beslutade styrning inom cybersäkerhet vid användning av stadens gemensamma system och infrastruktur. Anledningen är att 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.

Ett tillägg avseende en befintlig funktion i staden, CISO (Chief Information Security Officer) har också gjorts. Funktionen finns på stadsledningskontoret utifrån kommunstyrelsens ansvar att leda och samordna stadens informations- och cybersäkerhetsarbete. CISO leder, samordnar och följer upp stadens samlade arbete med informations- och cybersäkerhet. Tillägget tydliggör funktionens roll gentemot övrig verksamhet i staden och dess organisatoriska placering.

En ny rubrik ”Systematiskt riskbaserat arbete” har tillkommit under ”Organisatoriska säkerhetsåtgärder”. Här framgår att nämnder och styrelser har ett ansvar för att arbeta systematiskt med riskhantering och vilka moment som ingår i detta.

Rubriken ”Uppföljning av informationssäkerhet” har ändrats till ”Övervakning, uppföljning och uppsikt” för att bättre stämma överens med hur cybersäkerhetslagen beskriver verksamhetsutövarens och ledningens ansvar. Avsnittet har utökats för att tydliggöra att verksamhetsutövarens ledning ska övervaka att säkerhetsåtgärder genomförs i respektive verksamhet. Avsnittet har även kompletterats med ett förtydligande om att nämnder och styrelser ska lämna den information till kommunstyrelsen som behövs för att kommunstyrelsen ska kunna fullgöra sitt ansvar.

I riktlinjens bilaga 3 har listan med begreppsdefinitioner uppdaterats. Det beror dels på att begrepp tillkommit genom lagstiftningen, dels på behovet av tydligare och gemensamma definitioner inom staden för att kunna arbeta effektivt och minska risken för missförstånd eller olika tolkningar. Dessa definitioner kan behöva revideras oftare än övriga delar av riktlinjen, utifrån ändringar i nationell styrning. Enligt kommunstyrelsens delegation får stadsdirektören fatta beslut om redaktionella ändringar i styrande dokument som är beslutade av kommunstyrelsen och kommunfullmäktige när det behövs för att anpassa dokumenten till ny struktur eller till följd av ändring i lag, så länge ändringarna inte innebär ändring i sak. Ändringar av begreppsdefinitioner i riktlinjens bilaga 3 bedöms vara av sådan redaktionell karaktär och kan därmed framåt beslutas av stadsdirektören.

Stadsledningskontorets bedömning

Cybersäkerhetslagen omfattar samtliga nämnder i Göteborgs Stad samt de kommunala bolag vars verksamhet omfattas i lagen. I samband med att ny lagstiftning träder i kraft bedömer stadsledningskontoret att berörda styrdokument skyndsamt behöver justeras för att tydliggöra ansvaret i staden. Cybersäkerhet är ett högaktuellt område, och det bedöms angeläget att tidigt sätta roller och ansvar internt i Göteborgs Stad för att kunna möta de krav som den nya cybersäkerhetslagen ställer. Om en incident uppstår är det viktigt att veta hur ansvaren är fördelade, och att det finns en grund för ett systematiskt och riskbaserat arbetssätt.

De ändringar som föreslås är de som stadsledningskontoret i dagsläget bedömer är prioriterade utifrån att cybersäkerhetslagen beräknas träda i kraft med kort varsel, redan i mitten av januari 2026. Framåt kommer det sannolikt tillkomma ytterligare nationell styrning, framför allt i form av redan aviserade föreskrifter från MSB och PTS. Det kan även tillkomma ytterligare vägledning från de tillsynsmyndigheter som bevakar efterlevnaden av lagen. Vidare kan det finnas behov av att se över angränsande styrning, exempelvis kopplat till stadens gemensamma tjänster. Därutöver har stadsledningskontoret sedan tidigare identifierat behov av att förtydliga nämnders och styrelsers ansvar i frågor om dataskydd utifrån dataskyddslagstiftningen. Det har inte funnits möjlighet att hantera denna typ av ändringar i detta ärende, eftersom lagstiftningen träder i kraft med kort varsel.

Sammantaget bedömer stadsledningskontoret att arbetet med styrningen på området fortsatt behöver ses över och att Göteborgs Stads riktlinje för informationssäkerhet sannolikt behöver revideras ytterligare i närtid. Stadsledningskontoret bedömer också att kommunstyrelsen, utifrån sitt ansvar som ledning, framåt behöver fatta ytterligare beslut. Det handlar bland annat om ramverk för kravställning av leverantörer för att säkerställa cybersäkerhet i hela leverantörskedjan samt om anvisningar eller liknande för ett enhetligt arbete i staden risk- och incidenthantering.

Framåt behöver Göteborgs Stad också utveckla arbetsprocesser och samverkansytor för att ha förutsättningar för att effektivt och ändamålsenligt arbeta med cybersäkerhet och omhänderta kraven i lagstiftningen. I detta kommer samtliga nämnder och många bolag behöva vidta åtgärder. Den nya cybersäkerhetslagen bedöms särskilt ha betydelse för nämnden för Intraservice utifrån att nämnden är risk- och systemägare för många av stadens system.

Utifrån cybersäkerhetslagen har kommunstyrelsen rollen som ledning i förhållande till stadens nämnder. Med det följer ett särskilt ansvar för kommunstyrelsen i cybersäkerhetsfrågor jämfört med annan verksamhet. Stadsledningskontoret bedömer att den föreslagna kompletteringen i kommunstyrelsens reglemente är viktig för att synliggöra kommunstyrelsens ansvar i förhållande till stadens nämnder. Anledningen är att kommunstyrelsen får ett beslutsmandat i frågor som berör hela stadens och enskilda nämnders cybersäkerhet. När det gäller de av stadens bolag som själva är verksamhetsutövare enligt cybersäkerhetslagen framgår det i förarbetena att det är styrelserna och vd som är ledning. Därmed bedömer stadsledningskontoret att detta inte behöver anges i respektive ägardirektiv.

Regeringens färdiga lagförslag avseende cybersäkerhetslag presenterades i mitten av oktober 2025 och ska träda i kraft den 15 januari 2026. Det är därmed angeläget med en skyndsam hantering utifrån lagens ikraftträdande. Skulle de behov av ändringar som stadsledningskontoret föreslår i detta ärende inte hanteras finns risk för att Göteborgs Stad vid tillsyn inte bedöms ha gjort en tillräcklig ansats för att möta de krav som satts upp i cybersäkerhetslagen. Det kan leda till sanktionsavgift eller annan tillämplig åtgärd.

Christina Eide	Eva Hessman
Direktör Utveckling och hållbarhet	Stadsdirektör

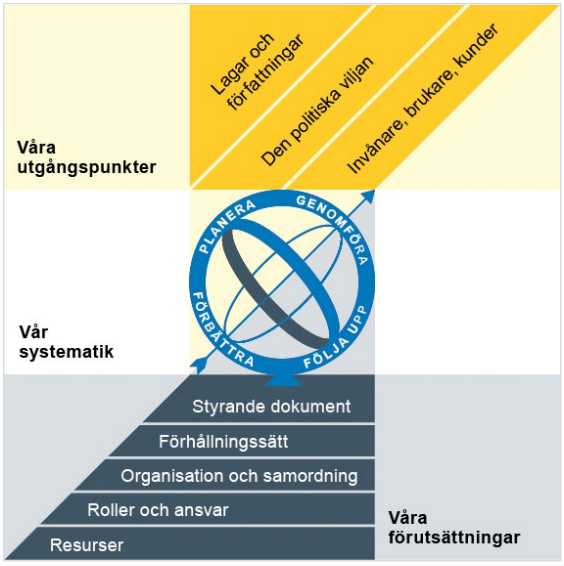
Göteborgs Stad

Göteborgs Stads riktlinje för informations- och cybersäkerhet

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



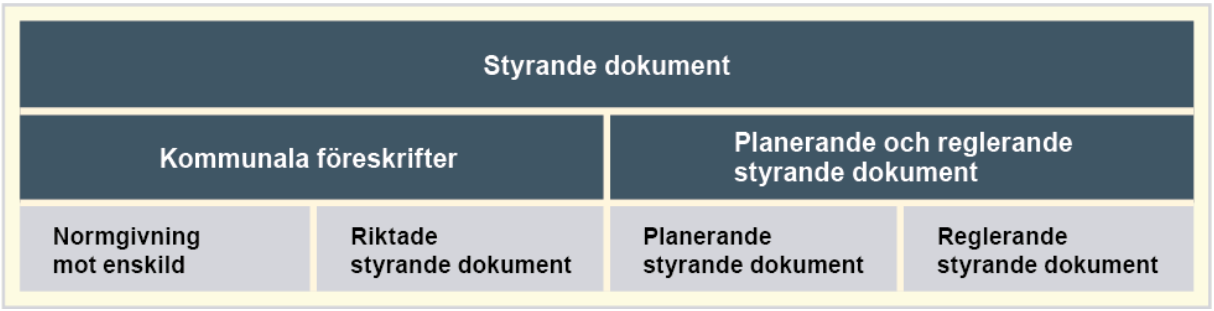
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Kommunfullmäktige	Stadens nämnder och styrelser	[Nummer]	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	[Datum]	Säkerhetschef

Bilagor:
1. Göteborgs Stads klassificeringsmodell
2. Göteborgs Stads klassificeringsmodell - beskrivning av konsekvensnivåer
3. Begreppsdefinition

Innehåll

Inledning

Syftet med denna riktlinje

Syftet med Göteborgs Stads riktlinje för informations- och cybersäkerhet är att skapa förutsättningar för ett systematiskt, riskbaserat och långsiktigt arbete genom att tydliggöra roller, ansvar, mandat och övergripande krav.

Riktlinjen omfattar alla informationstillgångar oavsett om de behandlas manuellt eller digitalt och oberoende av i vilken form eller miljö de förekommer.

Säkerhetsskyddsklassificerad information med betydelse för Sveriges säkerhet som regleras i säkerhetsskyddslagen hanteras inte i denna riktlinje, utan i Göteborgs Stads riktlinje för säkerhetsskydd.

Vem omfattas av riktlinjen

Riktlinjen gäller tills vidare för Göteborgs Stads nämnder och styrelser.

Bakgrund

Göteborgs Stad ansvarar för många viktiga samhällsfunktioner. Alla verksamheter är beroende av viktig information och system som behöver skyddas. Om systemen slutar fungera, om känslig information läcker ut, eller om det inte går att lita på informationen kan det leda till allvarliga konsekvenser för samhällsviktig verksamhet och medborgarnas säkerhet. Det gäller inte bara digitala system och digitala informationsresurser, utan kan också handla om analog information. Området informations- och cybersäkerhet innefattar IT-säkerhet, OT-säkerhet[1], fysisk säkerhet och säkerhet i leveranskedjan.

Lagbestämmelser

Området cybersäkerhet regleras i cybersäkerhetslagen, cybersäkerhetsförordningen samt tillhörande föreskrifter. Cybersäkerhetslagen är den svenska implementeringen av EU-direktivet NIS2[2]. 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.

Det finns även kopplingar till annan EU-lagstiftning, såsom AI-förordningen och DORA (Digital Operational Resilience Act), som tillsammans syftar till att stärka den digitala motståndskraften inom

[1] Ett OT-system (operationell teknologi) är ett system som styr, övervakar eller automatiserar fysiska processer. Det används främst inom industri, energi, transport, fastighetsautomation och kritisk infrastruktur.
[2] 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).

både offentlig och privat sektor. Vidare finns EU-lagstiftning inom dataskydd (GDPR) som syftar till att skydda enskildas personliga integritet och skapa en enhetlig nivå för dataskydd inom EU.

Sammantaget innebär detta att stadens verksamheter inte bara behöver förhålla sig till denna riktlinje utan också reglering på nationell och EU-nivå.

Koppling till andra styrande dokument

I Göteborgs Stads säkerhetspolicy fastställs principerna för stadens säkerhetsarbete. Informations- och cybersäkerhet utgör en del av detta arbete, och denna riktlinje konkretiserar styrningen inom området. Vidare är informations- och cybersäkerhet grundläggande för hanteringen av stadens informationstillgångar och påverkar, direkt eller indirekt, styrningen inom flera verksamhetsområden.

Riktlinje

Denna riktlinje anger hur Göteborgs Stad ska arbeta med informations- och cybersäkerhet. Ett ändamålsenligt säkerhetsarbete skapar förtroende både inom och utanför organisationen.

Läsanvisning

Terminologin på informations- och cybersäkerhetsområdet är under utveckling. I bilaga 3 till riktlinjen finns en lista med definitioner av olika centrala begrepp. Begrepp som används i cybersäkerhetslagen och tillhörande föreskrifter har samma innebörd i den här riktlinjen som i lag och föreskrift.

I det fall riktlinjen anger olika krav gällande nämnder och styrelser anges detta särskilt.

Göteborgs Stads metod för säker informationshantering

Inom Göteborg Stad ska ett systematiskt och långsiktigt informations- och cybersäkerhetsarbete bedrivas. Göteborgs Stads metod för säker informationshantering bygger på ett antal steg där informationsägaren inleder med att klassificera information, genomför en riskanalys för att därefter vidta lämpliga organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder. De olika stegen beskrivs i riktlinjen.

Informationssäkerhet innebär skydd av informationstillgångar avseende:

- *Konfidentialitet*, att information inte tillgängliggörs eller avslöjas för obehöriga.
- *Riktighet* inklusive autenticitet, att informationen skyddas mot oönskad förändring, att information är korrekt, inte manipulerad, förstörd eller förfalskad samt kommer från pålitlig källa.
- *Tillgänglighet*, att information är tillgänglig och användbar när den behövs.

Det är verksamhetens behov och informationens skyddsvärde som styr hur informationen ska skyddas. Informationens klassificering och de krav som det medför ska efterlevas under hela informationens livscykel inklusive avveckling.

Riskbaserat informations- och cybersäkerhetsarbete

I takt med att omvärlden och stadens verksamheter förändras omformas också behoven inom informations- och cybersäkerhet. Göteborgs Stad behöver därför ha kunskap om de hot, risker och sårbarheter som påverkar eller som kan komma att påverka staden. Detta uppnås genom omvärldsanalys och genom att ha ett riskbaserat förhållningssätt i informations- och cybersäkerhetsarbetet.

Ett riskbaserat förhållningssätt innebär att varje verksamhet ska identifiera, bedöma, hantera och följa upp informations- och cybersäkerhetsrisker och utifrån detta vidta lämpliga säkerhetsåtgärder.

Roller och ansvar

I enlighet med vad som gäller för övrig verksamhet i staden är grundprincipen att ansvaret för informations- och cybersäkerheten är kopplad till nämndernas och styrelsernas ordinarie ansvar. Det innebär att ansvarig nämnd eller styrelse för en verksamhet också har ett ansvar för att informations- och cybersäkerheten upprätthålls och efterföljs i denna verksamhet.

När det gäller cybersäkerheten i nämnderna riktar sig cybersäkerhetslagen till kommunen som helhet och lägger ett särskilt ansvar på kommunstyrelsen som ledning. För att tydliggöra hur arbetet ska bedrivas i staden behöver därför vissa roller och ansvar i riktlinjen definieras specifikt utifrån cybersäkerhetslagens krav, medan andra är generella och gäller för informations- och cybersäkerhetsarbetet i hela staden.

Verksamhetsutövare

Verksamhetsutövare är ett samlingsbegrepp i cybersäkerhetslagen för offentliga och enskilda verksamhetsutövare. Verksamhetsutövaren ansvarar för cybersäkerheten. Kommunens nämnder utgör tillsammans en offentlig verksamhetsutövare. Kommunala bolag som uppfyller kraven för att omfattas av lagen är enskilda verksamhetsutövare.

Ledning

Verksamhetsutövarens ledning ansvarar ytterst för att kraven i cybersäkerhetslagen uppfylls och efterlevs. För kommunala bolag som omfattas av cybersäkerhetslagen utgörs ledningen av styrelsen och vd. För kommunens nämnder utgörs ledningen av kommunstyrelsen.

Ledningen ansvarar för att leda och styra verksamhetsutövarens arbete med cybersäkerhet genom att bland annat besluta om mål och inriktning, fatta de beslut som behövs för att säkerställa att arbetet med att genomföra säkerhetsåtgärder bedrivs systematiskt och riskbaserat samt följa upp och övervaka genomförandet av säkerhetsåtgärderna.

Ledningen är det organ som enligt cybersäkerhetslagen kan ställas till svars för överträdelser när det gäller verksamhetsutövarens säkerhetsåtgärder.

CISO – Chief Information Security Officer

Göteborgs Stad har en CISO (Chief Information Security Officer). Funktionen finns på stadsledningskontoret utifrån kommunstyrelsens ansvar att leda och samordna stadens informations-

och cybersäkerhetsarbete. CISO leder, samordnar och följer upp stadens samlade arbete med informations- och cybersäkerhet.

Informationssäkerhetssamordnare

Varje nämnd och styrelse ska ha en utpekad funktion som arbetar med att samordna och utvärdera arbetet med säkerhetsåtgärder som stöd för nämndens eller styrelsens arbete med informations- och cybersäkerhet.

Incidenthanterare

Varje nämnd och styrelse ska ha en utpekad funktion som har i uppdrag att hantera och åtgärda informations- och cybersäkerhetsincidenter i verksamheten.

Informationsägare

Varje nämnd och styrelse ansvarar för den information som skapas och hanteras i verksamheten och har rollen som informationsägare. Informationsägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.

Riskägare

Varje nämnd och styrelse är riskägare inom sitt verksamhetsområde och ansvarar för att hantera de informations- och cyberhetssäkerhetsrisker som identifieras.

Nämnder och bolag ska följa de beslut och den styrning som fastställs av ledningen. Vem som utgör ledning för nämnder respektive bolag framgår ovan, under rubriken ”Ledning”.

Systemägare

Varje nämnd och styrelse ska ha utpekade systemägare som har ett överordnat ansvar för administration, drift och säkerhet för sina system. Ett system kan innehålla information som tillhör en eller flera informationsägare. Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.

Styrelserna ansvarar för att förhålla sig till kommunstyrelsens beslutade styrning inom cybersäkerhet 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.

Klassificering av information

En förutsättning för att arbeta med säkerhetsåtgärder är att informationen klassificeras. Informationsklassificering möjliggör att information skyddas på ett adekvat sätt, vilket höjer kvalitet och effektivitet genom att undvika att information får ett överskydd med höga kostnader som följd eller tvärtom, att information inte får det skydd som den behöver.

Göteborgs Stads klassificeringsmodell ska användas vid klassificeringen (se bilaga 1).

Nämnder och styrelser ansvarar för att:

- Säkerställa att informationen klassificeras utifrån säkerhetsaspekterna konfidentialitet, riktighet, inklusive autenticitet och tillgänglighet.
- Klassificering görs utifrån de konsekvenser eller skada som bristande informationssäkerhet skulle kunna medföra utifrån perspektiven: verksamhet, samhälle, individ, ekonomi och varumärke/förtroende (se bilaga 2).
- Säkerställa att lagar, föreskrifter och verksamhetskrav vägs in i informationsklassificeringen.

Organisatoriska säkerhetsåtgärder

Systematiskt riskbaserat arbete

Varje nämnd och styrelse ska arbeta systematiskt med riskhantering.

Nämnder och styrelser ansvarar för att:

- Säkerställa att risker avseende informations- och cybersäkerhet identifieras, analyseras, hanteras och följs upp.
- Säkerställa att säkerhetsåtgärder införs, följs upp och vid behov förbättras.
- Säkerställa att omvärldsbevakning bedrivs på ett systematiskt sätt för att hålla sig uppdaterad om hot, sårbarheter och teknisk utveckling.

Hantering av informationstillgångar

Med informationstillgångar menas verksamhetens information och de resurser som hanterar informationen. Exempel på informationstillgångar finns i bilaga 3 (begreppsdefinitioner).

Nämnder och styrelser ansvarar för att:

- Säkerställa att det finns en förteckning över verksamhetens informationstillgångar.
- Säkerställa att förteckningen innehåller sådan information som är nödvändig för återhämtning efter en störning eller incident.
- Säkerställa att förteckningen minst omfattar ändamål för behandling eller lagring av information, informationsägare, systemägare och tillgångens informationsklass utifrån säkerhetsaspekterna konfidentialitet, riktighet inklusive autenticitet och tillgänglighet.
- Säkerställa att det i förteckning definieras och dokumenteras regler, lagar samt avtalsrättsliga åtaganden för respektive informationstillgång.
- Säkerställa att anställda och externa användare lämnar tillbaka de informationstillgångar som de förfogar över då deras anställning, uppdrag eller avtal ändras.

Åtkomst till information

Nämnder och styrelser ansvarar för att:

- Säkerställa att åtkomst och behörighet till information ges restriktivt utifrån arbetsuppgifter och organisatorisk tillhörighet.

- Säkerställa att behörigheter följs upp vid behov. Vid byte eller förändring av tjänst ska behörigheter och åtkomst till information ses över.
- Säkerställa att åtkomst till information bygger på personliga användaridentiteter och är spårbar till en fysisk person.
- Säkerställa att autentisering och åtkomstkontroll till administratörs- och systemkonton sker med unika lösenord och baseras på flerfaktorsautentisering.
- Säkerställa att regelverk och rutin för registrering och avregistrering av behörigheter fastställs innan system tas i bruk.

Integritet och skydd av personuppgifter

Nämnder och styrelser ansvarar för att:

- Säkerställa att krav för upprätthållande av personlig integritet och skydd av personuppgifter, enligt tillämpliga lagar och författningar samt avtalskrav, identifieras och uppfylls.
- Säkerställa att det finns rutiner för behandling av personuppgifter och informationstexter till registrerade.
- Säkerställa att lämpliga säkerhetsåtgärder införs för att skydda personuppgifter.

Informations- och cybersäkerhet vid införande av nya system

Nämnder och styrelser ansvarar för att:

- Säkerställa att informations- och cybersäkerhet integreras i projektledningen.
- Säkerställa verifiering av leverantörens informations- och cybersäkerhet innan verksamheten inför ett nytt system. Leverantören kan åläggas att uppvisa verifiering.

Säkerhet i leveranskedjan

Nämnder och styrelser ansvarar för att:

- Säkerställa att informations- och cybersäkerheten integreras i upphandling av system. I leverantörsavtalet ska det förutom säkerhetskrav även framgå ansvarsfördelning, hur informationen ska hanteras, återlämnas och avvecklas.
- Säkerställa att det finns avtal med leverantörer som får åtkomst och behandlar information som ägs av Göteborgs Stad. Vid åtkomst till sekretessbelagd information ska även sekretessavtal ingås.
- Säkerställa att det finns personuppgiftsbiträdesavtal i de fall leverantören behandlar personuppgifter på uppdrag av Göteborgs Stad.

Hantering av informations- och cybersäkerhetsincidenter

Nämnder och styrelser ansvarar för att:

- Säkerställa att inträffade incidenter hanteras och åtgärdas skyndsamt för att minimera skador i verksamheten.

- Säkerställa att incidenter där informations-, rapporterings- eller anmälningsskyldighet finns enligt lag eller förordning, anmäls till ansvarig myndighet.

Kontinuitetshantering

Nämnder och styrelser ansvarar för att:

- Säkerställa att det finns en åtgärdsplan, så kallad kontinuitetsplan, för att verksamhet fortsatt kan bedrivas på en tolerabel nivå vid en allvarlig störning eller avbrott, utifrån ledningens fastställda acceptabla avbrottstider.

Personalrelaterade säkerhetsåtgärder

Nämnder och styrelser ansvarar för att:

Före anställning

- Säkerställa att arbetssökandes referenser och formella meriter såsom utbildning och yrkeslegitimation kontrolleras och att den arbetssökandes identitet verifieras.
- Vid rekrytering till särskilt informationssäkerhetskritiska arbetsuppgifter ska fler och mer detaljerade kontroller övervägas.

Under anställning

- Säkerställa att anställda under anställningstiden görs medvetna om sitt ansvar för informations- och cybersäkerhet och tillhandahålla utbildning vid behov.

Utbildning

- Säkerställa att anställda inom Göteborgs Stad får den utbildning i informations- och cybersäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Detsamma gäller vid förflyttning och omplacering av redan anställda.

Avslut eller ändring av anställning

- Säkerställa att det finns en fastställd rutin för hantering av anställda som avslutar sin anställning. Rutinen ska säkerställa att information, datorer/utrustning, passerkort, tjänstekort etcetera återlämnas och att åtkomsträttigheter upphör vid anställningens slut.

Fysiska säkerhetsåtgärder

Nämnder och styrelser ansvarar för att:

- Säkerställa att informationsklassning, riskbedömning och informationens skyddsvärde ligger till grund för det fysiska skalskydd som ska finnas för att skydda informationstillgångar. Vid utformning av centrala IT-utrymmen ska behovet av brandskydd, tillträdesskydd, skalskydd, el och reservkraft, miljö och kyla, skydd mot vätska, interiör, teknisk övervakning och larm med mera utvärderas.
- Säkerställa att säkerhetsåtgärder testas regelbundet.

Tekniska säkerhetsåtgärder

Driftsäkerhet

Göteborgs Stad ska som regel ha en systemmiljö med åtskilda produktions-, utvecklings-, test- och utbildningsmiljöer.

Nämnder och styrelser ansvarar för att:

- Säkerställa att säkerhetskopiering och testning för att återskapa information görs regelbundet.
- Säkerställa att det finns spårbarhet för viktiga och säkerhetskritiska händelser.
- Säkerställa att det finns ett installerat skydd av skadlig kod på enheter som kan drabbas av skadlig kod och obehörigt nyttjande.
- Säkerställa skyndsam installering av leverantörers säkerhetsuppdateringar. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringarna testas och analyseras innan de installeras i produktionsmiljön.

Systemdokumentation

Det ska finnas dokumentation för varje system. Dokumentationen ska bestå av system- och driftdokumentation.

Nämnder och styrelser ansvarar för att:

- Säkerställa att det finns systemdokumentationen som minst omfattar vilka olika komponenter systemet består av, en övergripande beskrivning av de olika delarnas uppgift samt en dokumentation över de funktioner som är relevanta för informationssäkerheten. Det ska även framgå vem som är systemägare.
- Säkerställa att det finns driftdokumentation som minst omfattar rutiner för säkerhetskopiering, återstarts- och återställningsrutiner, incidenthantering, ändringshantering samt information om logghantering. Det ska även framgå vem som är driftansvarig.
- Säkerställa att det finns en kopia av dokumentationen som förvaras skild från originalen och de ska vara åtkomliga även om lagringsytan de normalt sett förvaras på är otillgänglig.

Nätverkssäkerhet och säkerhet i nätverkstjänster

Göteborgs Stads verksamheter är beroende av ett fungerande nätverk. För att förhindra obehörig åtkomst till nätverk och anslutna tjänster ska det finnas säkerhetsåtgärder på plats för att säkerställa konfidentialitet och riktighet för information som överförs. Detsamma gäller för att upprätthålla tillgänglighet till nätverkets tjänster.

Nämnder och styrelser ansvarar för att:

- Säkerställa att loggning och övervakning tillämpas för att upptäcka avvikelser som kan påverka eller vara relevanta för informations- och cybersäkerheten.
- Säkerställa att det finns rutiner och uppdaterad dokumentation för hantering av nätverksenheter.

Anskaffning, utveckling, underhåll och avveckling av IT-system

Informations- och cybersäkerhetskraven ska vara en del av en upphandling av system och definieras utifrån informationsägarens informationsklassificering och riskbedömning.

Nämnder och styrelser ansvarar för att:

- Säkerställa att det finns rutiner för utveckling och testning av system samt ändringshantering.
- Säkerställa att alla system regelbundet analyseras för att identifiera sårbarheter som kan påverka informations- och cybersäkerheten.

Övervakning, uppföljning och uppsikt

Ledningen ansvarar för att övervaka genomförandet av säkerhetsåtgärder utifrån cybersäkerhetslagen för respektive verksamhetsutövare. Kommunstyrelsen har också uppsiktsplikt utifrån kommunallagen för stadens informations- och cybersäkerhetsarbete.

Nämnder och styrelser ska lämna kommunstyrelsen den information som behövs för att kommunstyrelsen ska kunna fullgöra sitt ansvar.

Varje nämnd och styrelse ansvarar för att följa upp informations- och cybersäkerheten och vidta de åtgärder som krävs för att säkerställa att styrande dokument, lagar och andra regelverk inom informations- och cybersäkerhet efterlevs inom den egna verksamheten.

Bilaga 1. Göteborgs Stads klassificeringsmodell

	Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
4	Sveriges Säkerhet Säkerhetsskydd	**K4** Information som omfattas av Säkerhetsskyddslagstiftningen *Särskild hantering - Riktlinje för säkerhetsskydd.*		
3	Allvarlig skada (hög skyddsnivå)	**K3** Viktig information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**R3** Viktig information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**T3** Viktig information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
2	Betydande (utökad skyddsnivå)	**K2** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R2** Information som, om den ej är riktig och fullständig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T2** Information som, om den ej är tillgänglig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
1	Måttlig (grundläggande nivå)	**K1** "Intern" information som om den tillgängliggörs, röjs eller sprids till obehöriga kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R1** Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller på individer	**T1** Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer
0	Försumbar skada (ingen skyddsnivå)	**K0** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R0** Information där förlust av riktighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T0** Information där förlust av tillgänglighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer

Bilaga 2. Göteborgs Stads klassificeringsmodell – beskrivning av konsekvensnivåer

Allvarlig skada (hög skyddsnivå 3)

- *Övergripande*: Mycket allvarlig skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet*: Det är stora svårigheter för verksamheten att fullfölja en eller flera av sina uppdrag. Omfattande skador på verksamhetens tillgångar. Kan ge stor påverkan på andra myndigheter och organisationer (ekonomiskt eller genom extraordinära åtgärder).
- *Samhälle*: Samhällsviktiga funktioner i egen eller annans organisation påverkas.
- *Individ*: Mycket allvarlig negativ påverkan på enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i mycket hög skadekostnad för verksamheten
- *Varumärke:* Mycket allvarlig/katastrofal påverkan på varumärke och förtroende.

Betydande skada (utökad skyddsnivå 2)

- *Övergripande:* Betydande skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet:* Verksamheten kan ha besvär med att fullfölja ett eller flera av sina uppdrag. Resulterar i betydande skador på verksamhetens tillgångar. Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom extraordinära åtgärder).
- *Samhälle:* Samhällsviktiga funktioner i egen eller annans organisation påverkas i liten utsträckning.
- *Individ:* Betydande negativ påverkan på enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i betydande skadekostnad för verksamheten.
- *Varumärke:* Allvarlig/betydande skada på varumärke - förtroende.

Måttlig skada (grundläggande skyddsnivå 1)

- *Övergripande:* Måttlig skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet:* Verksamheten har inte några större svårigheter att fullfölja och utföra sina uppdrag. Resultera endast i mindre skador på verksamhetens tillgångar.
- *Samhälle:* Obetydlig påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- *Individ:* Enstaka personuppgifter som inte är känsliga kan komma att spridas och förorsaka begränsad negativ påverkan på enskilds individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i viss skadekostnad för verksamheten.
- Viss påverkan på varumärke och förtroende.

Försumbar skada (ingen skyddsnivå 0)

- *Övergripande:* Ingen/försumbar skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.

- *Verksamhet:* Inga svårigheter för verksamheten att fullfölja sina uppdrag. Ingen skada på verksamhetens tillgångar och ingen påverkan på andra myndigheter eller organisationer.
- *Samhälle:* Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- *Individ:* Enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa påverkas minimalt.
- *Ekonomi:* Resulterar i ingen eller mycket begränsad skadekostnad.
- *Varumärke:* Ingen påverkan på varumärket eller förtroendet.

Bilaga 3. Begreppsdefinition

Nedan återfinns definitioner på begrepp som tillämpas i denna riktlinje.

Begrepp	Definition
Autentisering	Verifiering av att en användare är den person den påstår sig vara.
Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specifikt sätt.
Cybersäkerhet	All verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.
Informationstillgång	Med informationstillgång menas verksamhetens information och de resurser som hanterar informationen. Exempel på informationstillgångar är: • information (avtal, lösenord, rutiner, anteckningar, dokument etcetera) • program (applikation, operativsystem etcetera) • tjänster (kommunikationstjänst, abonnemang etcetera) • fysiska tillgångar (dator, telefon, lokala nätverk, skrivare etcetera) • människor och deras kompetens, färdigheter och erfarenheter • immateriella tillgångar (rykte och image etcetera)
Incident	En händelse som undergräver konfidentialitet, riktighet, autenticitet eller tillgänglighet hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.
Risk	Innebär att ett hot kan utnyttja sårbarheter i information, data eller i de system som hanterar dem, vilket kan leda till förlust av information eller kontroll över system och därigenom orsaka negativa konsekvenser för verksamheten. Detta omfattar även risker kopplade till brister i konfidentialitet, riktighet eller tillgänglighet hos informationstillgångar.
Riskkriterier	Riskkriterier är riskacceptans, riskvärde och risknivå. Riskacceptans är beslutade regler gällande vilka risker som kan tillåtas att kvarstå utan att de åtgärdas och vilka risker som måste åtgärdas på något sätt. Riskvärde är riskens sammanvägda värde av både värdet för sannolikhet och värdet för konsekvens. Risknivå är en kategorisering av hur allvarlig risken är, baserad på riskvärdet och beskriver hur allvarlig risken är i praktiken.
Spårbarhet	Möjlighet att kunna härleda utförda aktiviteter i systemet till en identifierad användare.
System	Ett nätverks- och informationssystem är ett system som består av teknisk utrustning, programvara och digital information som tillsammans gör det möjligt att lagra, behandla och överföra information. Det kan omfatta allt från elektroniska kommunikationsnät till sammankopplade enheter som automatiskt hanterar data. Begreppet inkluderar också de digitala uppgifter som behövs för att systemen ska fungera, skyddas och underhållas, samt de

	mänskliga aktiviteter och rutiner som krävs för att använda och driva systemen på ett säkert och effektivt sätt. System delas upp i IT-system och OT-system: Ett IT-system är ett informationssystem som primärt hanterar digital information för administrativa, ekonomiska, analytiska eller kommunikationsrelaterade syften. Ett OT-system (operationell teknologi) är ett system som styr, övervakar eller automatiserar fysiska processer. Det används främst inom industri, energi, transport, fastighetsautomation och kritisk infrastruktur.
Säkerhetsåtgärd	Identifierad uppsättning åtgärder för att möta en organisations informations- och cybersäkerhetsrisker

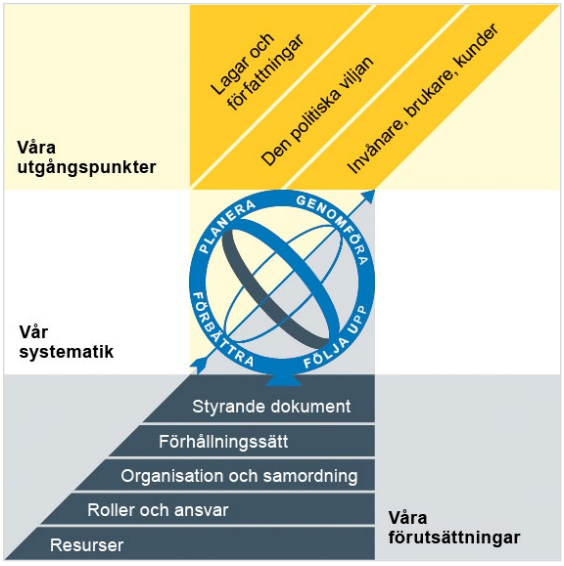
Göteborgs Stad

Göteborgs Stads riktlinje för informations- och cybersäkerhet

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



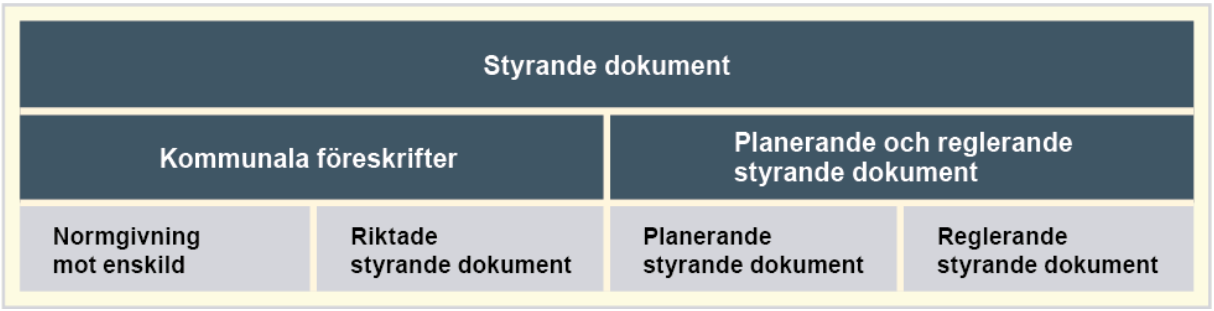
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Kommunfullmäktige	Stadens nämnder och styrelser	[Nummer]	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	[Datum]	Säkerhetschef

Bilagor:
1. Göteborgs Stads klassificeringsmodell
2. Göteborgs Stads klassificeringsmodell - beskrivning av konsekvensnivåer
3. Begreppsdefinition

Innehåll

Inledning

Syftet med denna riktlinje

Syftet med Göteborgs Stads riktlinje för informations- och cybersäkerhet är att skapa förutsättningar för ett systematiskt, riskbaserat och långsiktigt arbete genom att tydliggöra roller, ansvar, mandat och övergripande krav.

Riktlinjen omfattar alla informationstillgångar oavsett om de behandlas manuellt eller digitalt och oberoende av i vilken form eller miljö de förekommer.

Säkerhetsskyddsklassificerad information med betydelse för Sveriges säkerhet som regleras i säkerhetsskyddslagen hanteras inte i denna riktlinje, utan i Göteborgs Stads riktlinje för säkerhetsskydd.

Vem omfattas av riktlinjen

Riktlinjen gäller tills vidare för Göteborgs Stads nämnder och styrelser.

Bakgrund

Göteborgs Stad ansvarar för många viktiga samhällsfunktioner. Alla verksamheter är beroende av viktig information och system som behöver skyddas. Om systemen slutar fungera, om känslig information läcker ut, eller om det inte går att lita på informationen kan det leda till allvarliga konsekvenser för samhällsviktig verksamhet och medborgarnas säkerhet. Det gäller inte bara digitala system och digitala informationsresurser, utan kan också handla om analog information. Området informations- och cybersäkerhet innefattar IT-säkerhet, OT-säkerhet[1], fysisk säkerhet och säkerhet i leveranskedjan.

Lagbestämmelser

Området cybersäkerhet regleras i cybersäkerhetslagen, cybersäkerhetsförordningen samt tillhörande föreskrifter. Cybersäkerhetslagen är den svenska implementeringen av EU-direktivet NIS2[2]. 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.

Det finns även kopplingar till annan EU-lagstiftning, såsom AI-förordningen och DORA (Digital Operational Resilience Act), som tillsammans syftar till att stärka den digitala motståndskraften inom

[1] Ett OT-system (operationell teknologi) är ett system som styr, övervakar eller automatiserar fysiska processer. Det används främst inom industri, energi, transport, fastighetsautomation och kritisk infrastruktur.
[2] 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).

både offentlig och privat sektor. Vidare finns EU-lagstiftning inom dataskydd (GDPR) som syftar till att skydda enskildas personliga integritet och skapa en enhetlig nivå för dataskydd inom EU.

Sammantaget innebär detta att stadens verksamheter inte bara behöver förhålla sig till denna riktlinje utan också reglering på nationell och EU-nivå.

Koppling till andra styrande dokument

I Göteborgs Stads säkerhetspolicy fastställs principerna för stadens säkerhetsarbete. Informations- och cybersäkerhet utgör en del av detta arbete, och denna riktlinje konkretiserar styrningen inom området. Vidare är informations- och cybersäkerhet grundläggande för hanteringen av stadens informationstillgångar och påverkar, direkt eller indirekt, styrningen inom flera verksamhetsområden.

Riktlinje

Denna riktlinje anger hur Göteborgs Stad ska arbeta med informations- och cybersäkerhet. Ett ändamålsenligt säkerhetsarbete skapar förtroende både inom och utanför organisationen.

Läsanvisning

Terminologin på informations- och cybersäkerhetsområdet är under utveckling. I bilaga 3 till riktlinjen finns en lista med definitioner av olika centrala begrepp. Begrepp som används i cybersäkerhetslagen och tillhörande föreskrifter har samma innebörd i den här riktlinjen som i lag och föreskrift.

I det fall riktlinjen anger olika krav gällande nämnder och styrelser anges detta särskilt.

Göteborgs Stads metod för säker informationshantering

Inom Göteborg Stad ska ett systematiskt och långsiktigt informations- och cybersäkerhetsarbete bedrivas. Göteborgs Stads metod för säker informationshantering bygger på ett antal steg där informationsägaren inleder med att klassificera information, genomför en riskanalys för att därefter vidta lämpliga organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder. De olika stegen beskrivs i riktlinjen.

Informationssäkerhet innebär skydd av informationstillgångar avseende:

- *Konfidentialitet*, att information inte tillgängliggörs eller avslöjas för obehöriga.
- *Riktighet* inklusive autenticitet, att informationen skyddas mot oönskad förändring, att information är korrekt, inte manipulerad, förstörd eller förfalskad samt kommer från pålitlig källa.
- *Tillgänglighet*, att information är tillgänglig och användbar när den behövs.

Det är verksamhetens behov och informationens skyddsvärde som styr hur informationen ska skyddas. Informationens klassificering och de krav som det medför ska efterlevas under hela informationens livscykel inklusive avveckling.

Riskbaserat informations- och cybersäkerhetsarbete

I takt med att omvärlden och stadens verksamheter förändras omformas också behoven inom informations- och cybersäkerhet. Göteborgs Stad behöver därför ha kunskap om de hot, risker och sårbarheter som påverkar eller som kan komma att påverka staden. Detta uppnås genom omvärldsanalys och genom att ha ett riskbaserat förhållningssätt i informations- och cybersäkerhetsarbetet.

Ett riskbaserat förhållningssätt innebär att varje verksamhet ska identifiera, bedöma, hantera och följa upp informations- och cybersäkerhetsrisker och utifrån detta vidta lämpliga säkerhetsåtgärder.

Roller och ansvar

I enlighet med vad som gäller för övrig verksamhet i staden är grundprincipen att ansvaret för informations- och cybersäkerheten är kopplad till nämndernas och styrelsernas ordinarie ansvar. Det innebär att ansvarig nämnd eller styrelse för en verksamhet också har ett ansvar för att informations- och cybersäkerheten upprätthålls och efterföljs i denna verksamhet.

När det gäller cybersäkerheten i nämnderna riktar sig cybersäkerhetslagen till kommunen som helhet och lägger ett särskilt ansvar på kommunstyrelsen som ledning. För att tydliggöra hur arbetet ska bedrivas i staden behöver därför vissa roller och ansvar i riktlinjen definieras specifikt utifrån cybersäkerhetslagens krav, medan andra är generella och gäller för informations- och cybersäkerhetsarbetet i hela staden.

Verksamhetsutövare

Verksamhetsutövare är ett samlingsbegrepp i cybersäkerhetslagen för offentliga och enskilda verksamhetsutövare. Verksamhetsutövaren ansvarar för cybersäkerheten. Kommunens nämnder utgör tillsammans en offentlig verksamhetsutövare. Kommunala bolag som uppfyller kraven för att omfattas av lagen är enskilda verksamhetsutövare.

Ledning

Verksamhetsutövarens ledning ansvarar ytterst för att kraven i cybersäkerhetslagen uppfylls och efterlevs. För kommunala bolag som omfattas av cybersäkerhetslagen utgörs ledningen av styrelsen och vd. För kommunens nämnder utgörs ledningen av kommunstyrelsen.

Ledningen ansvarar för att leda och styra verksamhetsutövarens arbete med cybersäkerhet genom att bland annat besluta om mål och inriktning, fatta de beslut som behövs för att säkerställa att arbetet med att genomföra säkerhetsåtgärder bedrivs systematiskt och riskbaserat samt följa upp och övervaka genomförandet av säkerhetsåtgärderna.

Ledningen är det organ som enligt cybersäkerhetslagen kan ställas till svars för överträdelser när det gäller verksamhetsutövarens säkerhetsåtgärder.

CISO – Chief Information Security Officer

Göteborgs Stad har en CISO (Chief Information Security Officer). Funktionen finns på stadsledningskontoret utifrån kommunstyrelsens ansvar att leda och samordna stadens informations-

och cybersäkerhetsarbete. CISO leder, samordnar och följer upp stadens samlade arbete med informations- och cybersäkerhet.

Informationssäkerhetssamordnare

Varje nämnd och styrelse ska ha en utpekad funktion som arbetar med att samordna och utvärdera arbetet med säkerhetsåtgärder som stöd för nämndens eller styrelsens arbete med informations- och cybersäkerhet.

Incidenthanterare

Varje nämnd och styrelse ska ha en utpekad funktion som har i uppdrag att hantera och åtgärda informations- och cybersäkerhetsincidenter i verksamheten.

Informationsägare

Varje nämnd och styrelse ansvarar för den information som skapas och hanteras i verksamheten och har rollen som informationsägare. Informationsägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.

Riskägare

Varje nämnd och styrelse är riskägare inom sitt verksamhetsområde och ansvarar för att hantera de informations- och cyberhetssäkerhetsrisker som identifieras.

Nämnder och bolag ska följa de beslut och den styrning som fastställs av ledningen. Vem som utgör ledning för nämnder respektive bolag framgår ovan, under rubriken ”Ledning”.

Systemägare

Varje nämnd och styrelse ska ha utpekade systemägare som har ett överordnat ansvar för administration, drift och säkerhet för sina system. Ett system kan innehålla information som tillhör en eller flera informationsägare. Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.

Styrelserna ansvarar för att förhålla sig till kommunstyrelsens beslutade styrning inom cybersäkerhet 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.

Klassificering av information

En förutsättning för att arbeta med säkerhetsåtgärder är att informationen klassificeras. Informationsklassificering möjliggör att information skyddas på ett adekvat sätt, vilket höjer kvalitet och effektivitet genom att undvika att information får ett överskydd med höga kostnader som följd eller tvärtom, att information inte får det skydd som den behöver.

Göteborgs Stads klassificeringsmodell ska användas vid klassificeringen (se bilaga 1).

Nämnder och styrelser ansvarar för att:

- Säkerställa att informationen klassificeras utifrån säkerhetsaspekterna konfidentialitet, riktighet, inklusive autenticitet och tillgänglighet.
- Klassificering görs utifrån de konsekvenser eller skada som bristande informationssäkerhet skulle kunna medföra utifrån perspektiven: verksamhet, samhälle, individ, ekonomi och varumärke/förtroende (se bilaga 2).
- Säkerställa att lagar, föreskrifter och verksamhetskrav vägs in i informationsklassificeringen.

Organisatoriska säkerhetsåtgärder

Systematiskt riskbaserat arbete

Varje nämnd och styrelse ska arbeta systematiskt med riskhantering.

Nämnder och styrelser ansvarar för att:

- Säkerställa att risker avseende informations- och cybersäkerhet identifieras, analyseras, hanteras och följs upp.
- Säkerställa att säkerhetsåtgärder införs, följs upp och vid behov förbättras.
- Säkerställa att omvärldsbevakning bedrivs på ett systematiskt sätt för att hålla sig uppdaterad om hot, sårbarheter och teknisk utveckling.

Hantering av informationstillgångar

Med informationstillgångar menas verksamhetens information och de resurser som hanterar informationen. Exempel på informationstillgångar finns i bilaga 3 (begreppsdefinitioner).

Nämnder och styrelser ansvarar för att:

- Säkerställa att det finns en förteckning över verksamhetens informationstillgångar.
- Säkerställa att förteckningen innehåller sådan information som är nödvändig för återhämtning efter en störning eller incident.
- Säkerställa att förteckningen minst omfattar ändamål för behandling eller lagring av information, informationsägare, systemägare och tillgångens informationsklass utifrån säkerhetsaspekterna konfidentialitet, riktighet inklusive autenticitet och tillgänglighet.
- Säkerställa att det i förteckning definieras och dokumenteras regler, lagar samt avtalsrättsliga åtaganden för respektive informationstillgång.
- Säkerställa att anställda och externa användare lämnar tillbaka de informationstillgångar som de förfogar över då deras anställning, uppdrag eller avtal ändras.

Åtkomst till information

Nämnder och styrelser ansvarar för att:

- Säkerställa att åtkomst och behörighet till information ges restriktivt utifrån arbetsuppgifter och organisatorisk tillhörighet.

- Säkerställa att behörigheter följs upp vid behov. Vid byte eller förändring av tjänst ska behörigheter och åtkomst till information ses över.
- Säkerställa att åtkomst till information bygger på personliga användaridentiteter och är spårbar till en fysisk person.
- Säkerställa att autentisering och åtkomstkontroll till administratörs- och systemkonton sker med unika lösenord och baseras på flerfaktorsautentisering.
- Säkerställa att regelverk och rutin för registrering och avregistrering av behörigheter fastställs innan system tas i bruk.

Integritet och skydd av personuppgifter

Nämnder och styrelser ansvarar för att:

- Säkerställa att krav för upprätthållande av personlig integritet och skydd av personuppgifter, enligt tillämpliga lagar och författningar samt avtalskrav, identifieras och uppfylls.
- Säkerställa att det finns rutiner för behandling av personuppgifter och informationstexter till registrerade.
- Säkerställa att lämpliga säkerhetsåtgärder införs för att skydda personuppgifter.

Informations- och cybersäkerhet vid införande av nya system

Nämnder och styrelser ansvarar för att:

- Säkerställa att informations- och cybersäkerhet integreras i projektledningen.
- Säkerställa verifiering av leverantörens informations- och cybersäkerhet innan verksamheten inför ett nytt system. Leverantören kan åläggas att uppvisa verifiering.

Säkerhet i leveranskedjan

Nämnder och styrelser ansvarar för att:

- Säkerställa att informations- och cybersäkerheten integreras i upphandling av system. I leverantörsavtalet ska det förutom säkerhetskrav även framgå ansvarsfördelning, hur informationen ska hanteras, återlämnas och avvecklas.
- Säkerställa att det finns avtal med leverantörer som får åtkomst och behandlar information som ägs av Göteborgs Stad. Vid åtkomst till sekretessbelagd information ska även sekretessavtal ingås.
- Säkerställa att det finns personuppgiftsbiträdesavtal i de fall leverantören behandlar personuppgifter på uppdrag av Göteborgs Stad.

Hantering av informations- och cybersäkerhetsincidenter

Nämnder och styrelser ansvarar för att:

- Säkerställa att inträffade incidenter hanteras och åtgärdas skyndsamt för att minimera skador i verksamheten.

– Säkerställa att incidenter där informations-, rapporterings- eller anmälningsskyldighet finns enligt lag eller förordning, anmäls till ansvarig myndighet.

Kontinuitetshantering

Nämnder och styrelser ansvarar för att:

– Säkerställa att det finns en åtgärdsplan, så kallad kontinuitetsplan, för att verksamhet fortsatt kan bedrivas på en tolerabel nivå vid en allvarlig störning eller avbrott, utifrån ledningens fastställda acceptabla avbrottstider.

Personalrelaterade säkerhetsåtgärder

Nämnder och styrelser ansvarar för att:

Före anställning

– Säkerställa att arbetssökandes referenser och formella meriter såsom utbildning och yrkeslegitimation kontrolleras och att den arbetssökandes identitet verifieras.
– Vid rekrytering till särskilt informationssäkerhetskritiska arbetsuppgifter ska fler och mer detaljerade kontroller övervägas.

Under anställning

– Säkerställa att anställda under anställningstiden görs medvetna om sitt ansvar för informations- och cybersäkerhet och tillhandahålla utbildning vid behov.

Utbildning

– Säkerställa att anställda inom Göteborgs Stad får den utbildning i informations- och cybersäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Detsamma gäller vid förflyttning och omplacering av redan anställda.

Avslut eller ändring av anställning

– Säkerställa att det finns en fastställd rutin för hantering av anställda som avslutar sin anställning. Rutinen ska säkerställa att information, datorer/utrustning, passerkort, tjänstekort etcetera återlämnas och att åtkomsträttigheter upphör vid anställningens slut.

Fysiska säkerhetsåtgärder

Nämnder och styrelser ansvarar för att:

– Säkerställa att informationsklassning, riskbedömning och informationens skyddsvärde ligger till grund för det fysiska skalskydd som ska finnas för att skydda informationstillgångar. Vid utformning av centrala IT-utrymmen ska behovet av brandskydd, tillträdesskydd, skalskydd, el och reservkraft, miljö och kyla, skydd mot vätska, interiör, teknisk övervakning och larm med mera utvärderas.
– Säkerställa att säkerhetsåtgärder testas regelbundet.

Tekniska säkerhetsåtgärder

Driftsäkerhet

Göteborgs Stad ska som regel ha en systemmiljö med åtskilda produktions-, utvecklings-, test- och utbildningsmiljöer.

Nämnder och styrelser ansvarar för att:

- Säkerställa att säkerhetskopiering och testning för att återskapa information görs regelbundet.
- Säkerställa att det finns spårbarhet för viktiga och säkerhetskritiska händelser.
- Säkerställa att det finns ett installerat skydd av skadlig kod på enheter som kan drabbas av skadlig kod och obehörigt nyttjande.
- Säkerställa skyndsam installering av leverantörers säkerhetsuppdateringar. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringarna testas och analyseras innan de installeras i produktionsmiljön.

Systemdokumentation

Det ska finnas dokumentation för varje system. Dokumentationen ska bestå av system- och driftdokumentation.

Nämnder och styrelser ansvarar för att:

- Säkerställa att det finns systemdokumentationen som minst omfattar vilka olika komponenter systemet består av, en övergripande beskrivning av de olika delarnas uppgift samt en dokumentation över de funktioner som är relevanta för informationssäkerheten. Det ska även framgå vem som är systemägare.
- Säkerställa att det finns driftdokumentation som minst omfattar rutiner för säkerhetskopiering, återstarts- och återställningsrutiner, incidenthantering, ändringshantering samt information om logghantering. Det ska även framgå vem som är driftansvarig.
- Säkerställa att det finns en kopia av dokumentationen som förvaras skild från originalen och de ska vara åtkomliga även om lagringsytan de normalt sett förvaras på är otillgänglig.

Nätverkssäkerhet och säkerhet i nätverkstjänster

Göteborgs Stads verksamheter är beroende av ett fungerande nätverk. För att förhindra obehörig åtkomst till nätverk och anslutna tjänster ska det finnas säkerhetsåtgärder på plats för att säkerställa konfidentialitet och riktighet för information som överförs. Detsamma gäller för att upprätthålla tillgänglighet till nätverkets tjänster.

Nämnder och styrelser ansvarar för att:

- Säkerställa att loggning och övervakning tillämpas för att upptäcka avvikelser som kan påverka eller vara relevanta för informations- och cybersäkerheten.
- Säkerställa att det finns rutiner och uppdaterad dokumentation för hantering av nätverksenheter.

Anskaffning, utveckling, underhåll och avveckling av IT-system

Informations- och cybersäkerhetskraven ska vara en del av en upphandling av system och definieras utifrån informationsägarens informationsklassificering och riskbedömning.

Nämnder och styrelser ansvarar för att:

- Säkerställa att det finns rutiner för utveckling och testning av system samt ändringshantering.
- Säkerställa att alla system regelbundet analyseras för att identifiera sårbarheter som kan påverka informations- och cybersäkerheten.

Övervakning, uppföljning och uppsikt

Ledningen ansvarar för att övervaka genomförandet av säkerhetsåtgärder utifrån cybersäkerhetslagen för respektive verksamhetsutövare. Kommunstyrelsen har också uppsiktsplikt utifrån kommunallagen för stadens informations- och cybersäkerhetsarbete.

Nämnder och styrelser ska lämna kommunstyrelsen den information som behövs för att kommunstyrelsen ska kunna fullgöra sitt ansvar.

Varje nämnd och styrelse ansvarar för att följa upp informations- och cybersäkerheten och vidta de åtgärder som krävs för att säkerställa att styrande dokument, lagar och andra regelverk inom informations- och cybersäkerhet efterlevs inom den egna verksamheten.

Bilaga 1. Göteborgs Stads klassificeringsmodell

	Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
4	Sveriges Säkerhet Säkerhetsskydd	**K4** Information som omfattas av Säkerhetsskyddslagstiftningen *Särskild hantering - Riktlinje för säkerhetsskydd.*		
3	Allvarlig skada (hög skyddsnivå)	**K3** Viktig information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**R3** Viktig information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**T3** Viktig information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
2	Betydande (utökad skyddsnivå)	**K2** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R2** Information som, om den ej är riktig och fullständig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T2** Information som, om den ej är tillgänglig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
1	Måttlig (grundläggande nivå)	**K1** "Intern" information som om den tillgängliggörs, röjs eller sprids till obehöriga kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R1** Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller på individer	**T1** Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer
0	Försumbar skada (ingen skyddsnivå)	**K0** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R0** Information där förlust av riktighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T0** Information där förlust av tillgänglighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer

Bilaga 2. Göteborgs Stads klassificeringsmodell – beskrivning av konsekvensnivåer

Allvarlig skada (hög skyddsnivå 3)

- *Övergripande*: Mycket allvarlig skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet*: Det är stora svårigheter för verksamheten att fullfölja en eller flera av sina uppdrag. Omfattande skador på verksamhetens tillgångar. Kan ge stor påverkan på andra myndigheter och organisationer (ekonomiskt eller genom extraordinära åtgärder).
- *Samhälle*: Samhällsviktiga funktioner i egen eller annans organisation påverkas.
- *Individ*: Mycket allvarlig negativ påverkan på enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i mycket hög skadekostnad för verksamheten
- *Varumärke:* Mycket allvarlig/katastrofal påverkan på varumärke och förtroende.

Betydande skada (utökad skyddsnivå 2)

- *Övergripande:* Betydande skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet:* Verksamheten kan ha besvär med att fullfölja ett eller flera av sina uppdrag. Resulterar i betydande skador på verksamhetens tillgångar. Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom extraordinära åtgärder).
- *Samhälle:* Samhällsviktiga funktioner i egen eller annans organisation påverkas i liten utsträckning.
- *Individ:* Betydande negativ påverkan på enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i betydande skadekostnad för verksamheten.
- *Varumärke:* Allvarlig/betydande skada på varumärke - förtroende.

Måttlig skada (grundläggande skyddsnivå 1)

- *Övergripande:* Måttlig skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet:* Verksamheten har inte några större svårigheter att fullfölja och utföra sina uppdrag. Resultera endast i mindre skador på verksamhetens tillgångar.
- *Samhälle:* Obetydlig påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- *Individ:* Enstaka personuppgifter som inte är känsliga kan komma att spridas och förorsaka begränsad negativ påverkan på enskilds individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i viss skadekostnad för verksamheten.
- Viss påverkan på varumärke och förtroende.

Försumbar skada (ingen skyddsnivå 0)

- *Övergripande:* Ingen/försumbar skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.

- *Verksamhet:* Inga svårigheter för verksamheten att fullfölja sina uppdrag. Ingen skada på verksamhetens tillgångar och ingen påverkan på andra myndigheter eller organisationer.
- *Samhälle:* Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- *Individ:* Enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa påverkas minimalt.
- *Ekonomi:* Resulterar i ingen eller mycket begränsad skadekostnad.
- *Varumärke:* Ingen påverkan på varumärket eller förtroendet.

Bilaga 3. Begreppsdefinition

Nedan återfinns definitioner på begrepp som tillämpas i denna riktlinje.

Begrepp	Definition
Autentisering	Verifiering av att en användare är den person den påstår sig vara.
Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specifikt sätt.
Cybersäkerhet	All verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.
Informationstillgång	Med informationstillgång menas verksamhetens information och de resurser som hanterar informationen. Exempel på informationstillgångar är: • information (avtal, lösenord, rutiner, anteckningar, dokument etcetera) • program (applikation, operativsystem etcetera) • tjänster (kommunikationstjänst, abonnemang etcetera) • fysiska tillgångar (dator, telefon, lokala nätverk, skrivare etcetera) • människor och deras kompetens, färdigheter och erfarenheter • immateriella tillgångar (rykte och image etcetera)
Incident	En händelse som undergräver konfidentialitet, riktighet, autenticitet eller tillgänglighet hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.
Risk	Innebär att ett hot kan utnyttja sårbarheter i information, data eller i de system som hanterar dem, vilket kan leda till förlust av information eller kontroll över system och därigenom orsaka negativa konsekvenser för verksamheten. Detta omfattar även risker kopplade till brister i konfidentialitet, riktighet eller tillgänglighet hos informationstillgångar.
Riskkriterier	Riskkriterier är riskacceptans, riskvärde och risknivå. Riskacceptans är beslutade regler gällande vilka risker som kan tillåtas att kvarstå utan att de åtgärdas och vilka risker som måste åtgärdas på något sätt. Riskvärde är riskens sammanvägda värde av både värdet för sannolikhet och värdet för konsekvens. Risknivå är en kategorisering av hur allvarlig risken är, baserad på riskvärdet och beskriver hur allvarlig risken är i praktiken.
Spårbarhet	Möjlighet att kunna härleda utförda aktiviteter i systemet till en identifierad användare.
System	Ett nätverks- och informationssystem är ett system som består av teknisk utrustning, programvara och digital information som tillsammans gör det möjligt att lagra, behandla och överföra information. Det kan omfatta allt från elektroniska kommunikationsnät till sammankopplade enheter som automatiskt hanterar data. Begreppet inkluderar också de digitala uppgifter som behövs för att systemen ska fungera, skyddas och underhållas, samt de

	mänskliga aktiviteter och rutiner som krävs för att använda och driva systemen på ett säkert och effektivt sätt. System delas upp i IT-system och OT-system: Ett IT-system är ett informationssystem som primärt hanterar digital information för administrativa, ekonomiska, analytiska eller kommunikationsrelaterade syften. Ett OT-system (operationell teknologi) är ett system som styr, övervakar eller automatiserar fysiska processer. Det används främst inom industri, energi, transport, fastighetsautomation och kritisk infrastruktur.
Säkerhetsåtgärd	Identifierad uppsättning åtgärder för att möta en organisations informations- och cybersäkerhetsrisker