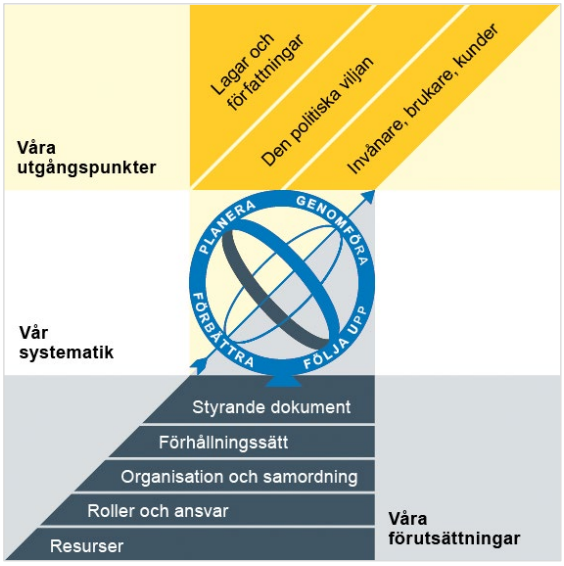
Göteborgs Stad

Göteborgs Stads riktlinje för informations- och cybersäkerhet

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



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

Om Göteborgs Stads styrande dokument

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

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

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

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

Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Kommunfullmäktige	Stadens nämnder och styrelser	SLK-2025-01130	2026-01-29 § 14
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	2026-01-29	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

Denna riktlinje gäller tillsvidare 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 , 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[1]. I anslutning till NIS2 finns även EU-kommissionens genomförandeförordning som preciserar direktivets tillämpning.

För de nämnder och styrelser som omfattas av cybersäkerhetslagen gäller utökade krav i enlighet med de specifika föreskrifter som gäller för respektive verksamhet.

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 både offentlig och privat sektor. Vidare finns EU-lagstiftning inom

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

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