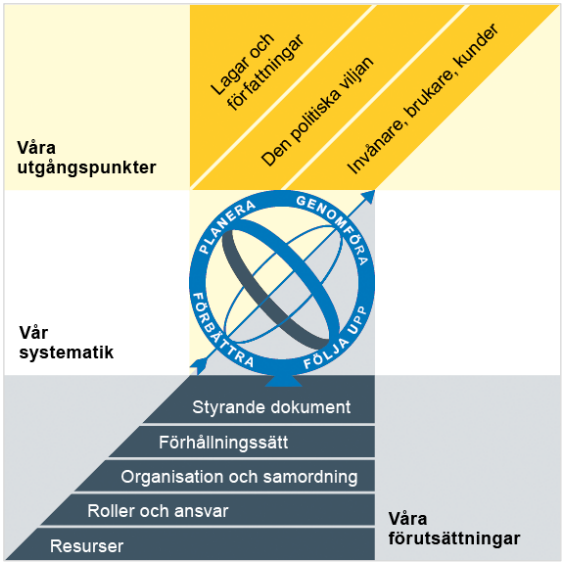
Göteborgs Stad

Grundskoleförvaltningens rutin för informationsklassning

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



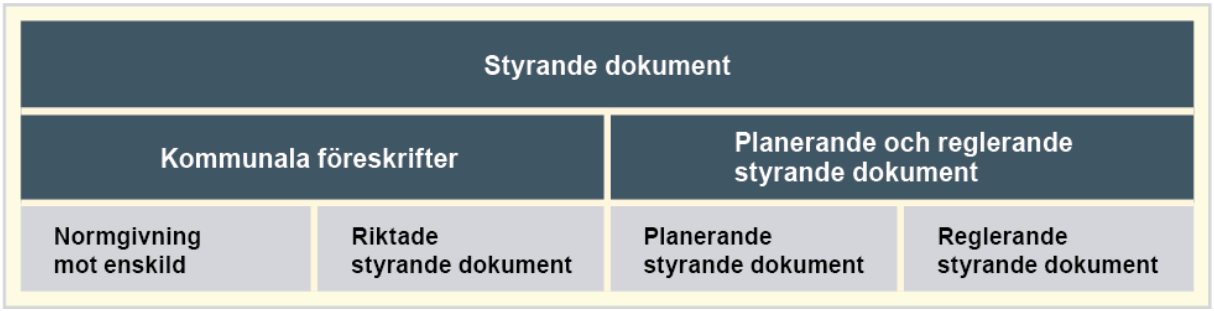
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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:**
Enhetschef kansli och säkerhet	Grundskoleförvaltningens anställda	GSF-2025-04978	2026-02-11
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Rutin	Datum 2026-02-11 Tillsvidare	2026-02-11	Informationssäkerhetssamordnare

Bilagor:
Mall för informationsklassning

Innehåll

Inledning

Syftet med denna rutin

Rutinen med tillhörande mall för informationsklassning utifrån Göteborgs Stads riktlinje för informationssäkerhet anger varför och hur grundskoleförvaltningen ska arbeta med informationsklassning.

Vem omfattas av rutinen

Denna rutin gäller tillsvidare för grundskoleförvaltningens anställda. Rutinen vänder sig till alla som ska genomföra eller delta i en informationsklassning, exempelvis klassningsledare, representanter från verksamheten, informationssäkerhetssamordnare (ISAM) och arkivarie. Rutinen vänder sig även till de funktioner som har ett ansvar kopplat till informationsklassning, exempelvis informationsägare och systemägare.

Bakgrund

Göteborgs Stads riktlinje för informationssäkerhet anger att förvaltningar och bolag ska arbeta med informationsklassning. Nämnder och styrelser ansvarar för att säkerställa att informationen klassificeras utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.

Koppling till andra styrande dokument

Styrande dokument	Koppling till denna rutin
Göteborgs stads riktlinje för informationssäkerhet, beslutad av kommunfullmäktige 2023-05-25 § 7	Fördelar ansvar för och ställer krav på informationsklassning.

Stödjande dokument

Grundskoleförvaltningens klassificeringsstruktur, version 2.0, diarienummer N609-2359

Grundskoleförvaltningens dokumenthanteringsplan, version 1.7, diarienummer GSK-2024-04490

Mall för informationsklassning (bilaga 1)

Rutin

Inledning

Stadens riktlinje för informationssäkerhet föreskriver att stadens informationstillgångar ska vara informationsklassade. För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska det finnas ett riskbaserat förhållningssätt i arbetet. Klassning är en riskbaserad metod som hjälper verksamheten att välja rätt säkerhetsåtgärder för att skydda sin information och se till att den får det skydd som motsvarar dess betydelse för verksamheten.

För att kunna göra en klassning av information behöver vi veta vilken information vi har, vilket värde den har och vilka risker som kan påverka informationen negativt.

Vad är informationsklassning

Informationsklassning är grundläggande för informationssäkerhetsarbetet. Klassning är en riskbaserad metod som hjälper verksamheten att välja rätt säkerhetsåtgärder för att skydda sin information.

Genom att klassa information utifrån kriterierna konfidentialitet, riktighet och tillgänglighet görs ett ställningstagande som visar verksamhetens syn på hur skyddsvärd informationen är och hur den behöver skyddas. Genom att bedöma konsekvenserna utifrån dessa tre kriterier går det att identifiera brister. Dessa ligger i sin tur till grund till vilka skyddsåtgärder som tas fram.

Det är viktigt att inte ge informationen för högt skydd vilket kan ge onödiga kostnader. Klassning av information sker utifrån rättsliga krav i form av lagar och föreskrifter och verksamhetens interna krav på informationens värde, känslighet och vilken betydelse informationen har för organisationens verksamheter.

När ska informationsklassning göras

Det finns olika tillfällen då en informationsklassning behöver genomföras,

- inför en upphandling,
- anskaffning eller utveckling av en IT-tjänst
- en förändring av en personuppgiftsbehandling,
- verksamheten ska se över sina klassningar minst en gång per år eller vid större förändring. Det kan vara vid exempelvis byte av leverantör eller organisationsförändringar.

En genomförd klassning ska ses över årligen och revideras vid behov. Ibland kan det vara tillräckligt att dokumentera att en klassning fortfarande gäller.

Processorienterad informationsklassning

Informationsklassningen syftar till att skydda den information som skapas och hanteras inom förvaltningens verksamhet. Denna information är inom staden strukturerad utifrån de processer där informationen skapas. Dessa går att finna i förvaltningens klassificeringsstruktur och är indelade i verksamhetsområden och underliggande processer. Processerna är kompletterade med vilken information som uppstår och hanteras i processerna och detta beskrivs i förvaltningens dokumenthanteringsplan.

Grunden för att inventera den information som ska skyddas utgörs därmed av förvaltningens klassificeringsstruktur och dokumenthanteringsplan. I staden kallas detta för processorienterad informationsredovisning.

Ett processorienterat klassningsförfarande startar med en inventering av den informationshantering som ingår i en verksamhetsprocess, inklusive personuppgifter. Förutom att inventeringen utgör underlag för klassning utgör den också underlag för verksamhetens registerförteckning. Det ska finnas en samstämmighet mellan dokumenthanteringsplan, registerförteckning och förteckning över informationsklassningar. Genom att utgå från processperspektivet i klassningsarbetet kan verksamheten informationsklassa all information som hanteras inom en process, det vill säga både digital och manuell informationshantering.

Ansvar för en informationsklassning

Ansvaret för informationssäkerheten följder det ordinarie verksamhetsansvaret. Det kan vara exempelvis avdelning, enhet, process eller projekt.

Informationsägaren ansvarar för att informationsklassning genomförs och att skyddsåtgärder från informationsklassningen kommuniceras och ställs till rätt part.

Informationsägaren är också den som godkänner informationsklassningens resultat.

Det är vanligt att information från flera informationsägare samlas i samma IT-tjänst, exempelvis i förvaltningens diarium. Detta ökar i normala fall även skyddsvärdet för informationen.

Deltagare vid en klassning

Informationsägaren tillhandahåller resurser för utförandet. ISAM ansvarar för tillhandahållande av metod och stöd.

De funktioner som bör delta när en informationsklassklassning ska göras är:

Informationsägare/representant för informationsägaren

Representanter från verksamheten som är väl bekant med den information och personuppgiftsbehandlingar som ska klassas.

Juridisk kompetens som till exempel jurist och arkivarie.

En person med kunskap om hur man genomför en informationsklassning. Exempelvis ISAM. ISAM kan ingå i klassningsarbetet som klassningsledare eller som sakkunnig och ge stöd till informationsägaren eller klassningsledaren.

Metod

Innan klassningen startar

Använd förvaltningens mall för informationsklassning (se bilaga till detta dokument)

Kartläggning av den information som ska klassas görs med hjälp av förvaltningens klassificeringsstruktur, dokumenthanteringsplan och behandlingsregister. Den kartlagda informationen fungerar som grund till att identifiera vilka informationsbärare som hanterar informationen. Exempel på informationsbärare är papper, verksamhetssystem, e-post, databas och molntjänst.

Innan klassningen startar behöver den information som ska klassas finnas beskriven. Till hjälp för att identifiera vilken information som ska klassas bör kartläggningen utgå från de processer som stödjer verksamheten i att utföra sitt uppdrag. Förvaltningens klassificeringsstruktur och dokumenthanteringsplan är till god hjälp. Den kartlagda informationen ska även stämma överens med verksamhetens behandlingsregister där verksamhetens personuppgiftsbehandlingar finns dokumenterade.

Om det i samband med kartläggningen uppkommer ny information som hanteras av verksamheten som inte redan finns dokumenterad i dokumenthanteringsplanen eller i behandlingsregistret, så ska dessa uppdateras.

Informationsklassning görs i två steg.

Steg 1 - Bestäm informationens värde

I det första steget ska informationen som ska klassas värderas. Klassningen sker utifrån de tre perspektiven konfidentialitet, riktighet och tillgänglighet (KRT). Resultatet blir ett klassningsvärde för KRT som visar hur skyddsvärd informationen är för verksamheten. Klassningen ska dokumenteras i förvaltningens mall för informationsklassning.

- Konfidentialitet (K), att information inte tillgängliggörs eller avslöjas för obehöriga.
- Riktighet (R), att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
- Tillgänglighet (T), att information är tillgänglig och användbar när den behövs.

Ett av de viktigaste momenten i informationsklassningen är att bestämma hur skyddsvärd informationen är för verksamheten och ur ett integritetsperspektiv. Värderingen sker genom att gruppen tillsammans bedömer konsekvenserna som kan uppstå när det brister i konfidentialitet, riktighet och tillgänglighet utifrån de olika perspektiven övergripande, verksamhet, samhälle, individ (perspektivet omfattar även gruppen individer), ekonomi och varumärke.

Gruppen behöver ta ställning till följande klassningsnivåer:

0- Försumbar skada (ingen skyddsnivå)

1- Måttlig (grundläggande nivå)

2- Betydande (utökad skyddsnivå)

3- Allvarlig skada (hög skyddsnivå)

4- Sveriges Säkerhet Säkerhetsskydd (Information som omfattas av Säkerhetsskyddslagstiftningen Särskild hantering - Riktlinje för säkerhetsskydd)

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

Olika konsekvensperspektiv

- *Övergripande*: Hur stor skadan är för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet*: Hur stora svårigheterna är för verksamheten att fullfölja en eller flera av sina uppdrag. Hur omfattande skadorna är på verksamhetens tillgångar. Hur stor påverkan är på andra myndigheter och organisationer (ekonomiskt eller genom extraordinära åtgärder).
- *Samhälle*: Hur påverkan är på samhällsviktiga funktioner i egen eller annans organisation.
- *Individ*: Hur stor påverkan är på enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi*: Hur stor den ekonomiska förlusten är (exempelvis minskade intäkter, ökade kostnader, skada på tillgångar)
- *Varumärke*: Hur stor påverkan är på varumärke och förtroende.

För beskrivning av de olika konsekvensnivåerna, se Göteborgs Stads riktlinje för informationssäkerhet.

Steg 2 - Definiera skyddsåtgärder

En grundläggande princip är att ju högre skyddsvärde informationen har desto mer omfattande åtgärder behövs för att skydda informationen. Det kan röra sig om vilken nivå av informationsklassning ett IT-stöd behöver för att ge rätt skydd för informationen.

Skyddsåtgärder omfattar både verksamhetsnära och tekniska åtgärder. Verksamhetsnära åtgärder innebär sådana som ska utföras av verksamheten, exempelvis en rutin för uppföljning av medarbetarnas behörigheter i en IT-tjänst. Tekniska åtgärder innebär sådana som gäller för den IT-tjänst som hanterar informationen i fråga, exempelvis kryptering för att skydda konfidentialitet.

Efter genomförd informationsklassning

Efter att informationsägaren har godkänt informationsklassningens resultat ansvarar klassningsledaren för att klassningsexcelarket diarieförs.

Informationsägaren ansvarar för att framtagna skyddsåtgärder åtgärdas och följs upp som en del av det systematiska informationssäkerhetsarbetet.

När klassningsarbetet är färdigt är nästa steg att ta fram en riskanalys för informationssäkerhet. I riskanalysen ska verksamheten fördjupa analysen kring de tekniska och organisatoriska säkerhetskrav som har definierats i klassningens steg 2 *Definiera skyddsåtgärder*.