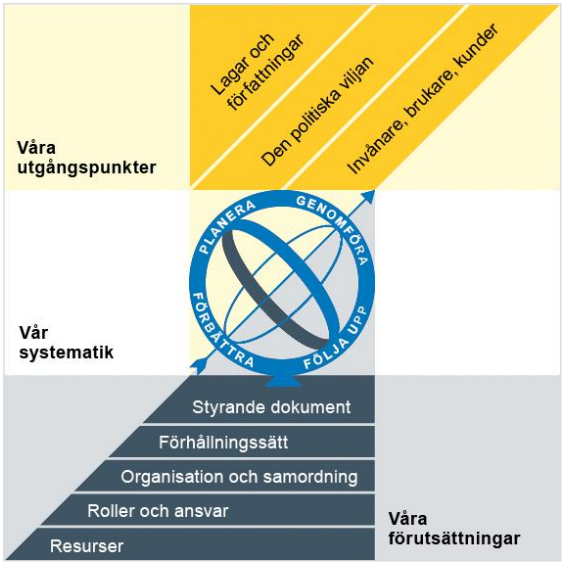
Göteborgs Stad

Göteborgs Stads riktlinje för informationssäkerhet

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



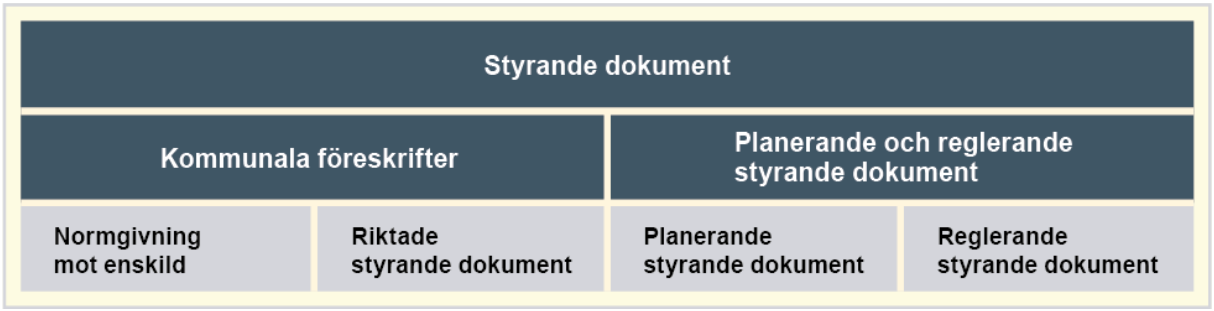
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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	0160/23	2023-05-25, § 7
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	2023-05-25	Säkerhetschef

Bilagor:
Göteborgs Stads klassificeringsmodell
Göteborgs Stads klassificeringsmodell - beskrivning av konsekvensnivåer
Begreppsdefinition

Innehåll

Inledning

Syftet med denna riktlinje

Syftet med Göteborgs Stads riktlinje för informationssäkerhet är att 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.

Säkerhetsskyddsklassificerad information med betydelse för Sveriges säkerhet hanteras utanför denna riktlinje. Se Göteborgs Stads riktlinje för säkerhetsskydd.

Vem omfattas av riktlinjen

Denna riktlinje gäller tillsvidare för Göteborgs Stads nämnder och styrelser.

Koppling till andra styrande dokument

Denna riktlinje konkretiserar Göteborgs Stads säkerhetspolicy avseende informationssäkerhet.

Stödjande dokument

Göteborgs Stads klassificeringsmodell inklusive beskrivning av konsekvensnivåer. Utöver stödjande dokument finns även ett nätverk för informationssäkerhet med representanter från stadens nämnder och styrelser som syftar till kunskaps- och erfarenhetsutbyte.

Riktlinje

Inledning

Denna riktlinje anger hur Göteborgs Stad ska arbeta med informationssäkerhet.

Information är viktig för Göteborg Stad och behöver skyddas efter behov. Ett bra informationssäkerhetsarbete skapar förtroende både inom och utanför organisationen.

Information är värdefull för Göteborg Stad. Information inhämtas, bearbetas, lagras och kommuniceras på olika sätt. Information som går förlorad eller hanteras felaktigt kan leda till allvarliga konsekvenser både för organisationer och för den enskilda människan.

Göteborgs Stads metod för säker informationshantering

Inom Göteborg Stad ska ett systematiskt och långsiktigt informationssäkerhetsarbete 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*, att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
- *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 informationssäkerhetsarbete

I takt med att omvärlden och den interna verksamheten förändras så förändras även behovet av informationssäkerhet. 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 informationssäkerhetsarbetet.

Ett riskbaserat förhållningssätt i informationssäkerhetsarbetet innebär att varje verksamhet ska identifiera, bedöma och följa upp informationssäkerhetsrisker och utifrån detta vidta lämpliga säkerhetsåtgärder.

Ansvar och roller i informationssäkerhet

I enlighet med vad som gäller för övrig verksamhet, är ansvaret för informationssäkerheten kopplat till ordinarie verksamhetsansvar. Det innebär att ansvarig nämnd/styrelse för en verksamhet också är ansvarig för att informationssäkerheten upprätthålls och efterföljs i denna verksamhet.

Informationsägare är den nämnd/styrelse som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten. Informationssägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.

Systemägare är den som har ett överordnat ansvar för administration, drift och säkerhet för ett 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.

Klassificering av information

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.

Nämnder och styrelser ansvarar för att:

- säkerställa att informationen klassificeras utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet och det är Göteborgs Stads klassificeringsmodell som ska användas (se bilaga 1). 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

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 allvarlig incident
- säkerställa att förteckningen minst omfattar ändamål för behandling eller lagring av information, informationsägare, systemägare och tillgångens informationsklass utifrån säkerhetsaspekterna konfidentialitet, riktighet 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.

Informationssäkerhet vid införande av nya system

Nämnder och styrelser ansvarar för att:

- säkerställa att informationssäkerhet integreras i projektledningen,
- säkerställa verifiering av leverantörens informationssäkerhet innan verksamheten inför ett nytt system. Leverantören kan åläggas att uppvisa verifiering.

Leverantörsrelationer

Nämnder och styrelser ansvarar för att:

- säkerställa att informationssäkerheten 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 leverantör behandlar personuppgifter på uppdrag av Göteborgs Stad.

Hantering av incidenter

Nämnder och styrelser ansvarar för att:

- säkerställa att inträffade incidenter hanteras och åtgärdas skyndsamt för att minimera skador i verksamheten
- säkerställa att informationssäkerhetsincidenter där anmälningsskyldighet finns enligt lag eller förordning, anmäls till ansvarig myndighet.

Informationssäkerhet vid störning - kontinuitetshantering

Nämnder och styrelser ansvarar för att:

- säkerställa att det finns en åtgärdsplan, så kallad kontinuitetsplan, för att kritisk verksamhet fortsatt kan bedrivas på en acceptabel nivå vid en allvarlig störning eller avbrott.

Personalrelaterade säkerhetsåtgärder

Nämnder och styrelser ansvarar för att:

Före anställning

- säkerställa att arbetssökandes referenser och formella meriter (såsom utbildning, yrkeslegitimation, etcetera), 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 informationssäkerhet.

Utbildning

- säkerställa att anställda inom Göteborgs Stad får den utbildning i informationssäkerhet 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 även vid förflyttning och omplacering av redan anställda och när tillfällig personal och externa konsulter anlitas.

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 driftdokumentationen 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 informationssäkerheten
- säkerställa att det finns rutiner och uppdaterad dokumentation för hantering av nätverksenheter.

Anskaffning, utveckling, underhåll och avveckling av IT-system

Informationssäkerhetskraven 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 informationssäkerheten.

Uppföljning av informationssäkerhet

Varje nämnd och styrelse ska följa upp informationssäkerheten och vidta de åtgärder som krävs för att säkerställa att styrande dokument, lagar och andra regelverk inom informationssäkerhet 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. Myndigheten för samhällsskydd och beredskap tillhandahåller en termbank för informationssäkerhet.

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.
Fysiskt skydd	Säkerhetsåtgärder relaterade till skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten.
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)
Skalskydd	Skalskydd är den gräns i ett utrymme, lokal eller fastighet som har ett fysiskt skydd vilket försvårar obehörigt tillträde
Spårbarhet	Möjlighet att kunna härleda utförda aktiviteter i systemet till en identifierad användare.
System	Informationssystem för att samla in, lagra, bearbeta och distribuera information för ett givet ändamål, innefattar såväl ett systems tekniska utrustning som dess mänskliga aktiviteter och rutiner.
Säkerhetsåtgärd	Identifierad uppsättning åtgärder för att möta en organisations risker