Sunne kommun

Styrdokument

Riktlinje för informationssäkerhetsarbetet Sunne kommun

SUNNE | VÄRMLAND

Dokumenttyp	Riktlinje
Diarienummer	KS/2024:570
Beslutad av	Kommunstyrelsen 2026-03-12, § 38
Reviderad av	
Dokumentansvarig	Informationssäkerhetssamordnare

Innehåll

1. Inledning 4

2. Organisation och ansvarsfördelning 5

2.1 Grundprincip 5

2.2 Ledning och ansvar 5

2.3 Roller och ansvar 6

2.3.1 Informationsägare 6

2.3.2 Systemägare 6

2.3.3 Systemförvaltare 7

3. Roller och ansvar för stöd, samordning och kontroll 7

3.1 Styrgrupp för informationssäkerhetsarbetet 7

3.2 Informationssäkerhetsforum 7

3.3 Informationssäkerhetssamordnare 8

3.4 Kontaktpersoner 8

3.5 IT- funktion/ IT-säkerhetsansvar 8

4. Ledningssystem för informationssäkerhet (LIS) 9

4.1 Identifiera och analysera 9

4.2. Utforma och införa 10

4.3 Följa upp, utvärdera och förbättra 10

5. Informationsklassning 11

6. Riskanalys 13

7. Säkerhetsåtgärder 13

Bilaga 1. Begreppsförklaring 15

1. Inledning

Information är en grundläggande byggsten i en organisation, på samma sätt som medarbetare, lokaler och utrustning. Det är en av kommunens viktigaste tillgångar och behöver som sådan skyddas. Informationssäkerhet omfattar skydd av all information oavsett form och innebär en strävan att skydda information så att följande grundprinciper upprätthålls:

- Endast behöriga personer får ta del av informationen **(konfidentialitet)**
- Informationen går att lita på, att den är korrekt och inte manipulerad **(riktighet)**
- Informationen finns tillgänglig när den behövs **(tillgänglighet)**
- Bearbetning av informationen ska kunna härledas till vem och när **(spårbarhet)**

Cybersäkerhet utgör en del av informationssäkerheten och avser särskilt skydd av digital information samt de nätverks- och informationssystem som används för att lagra, behandla och överföra information. Krav enligt cybersäkerhetslagstiftningen hanteras därför inom ramen för kommunens samlade informationssäkerhetsarbete.

Arbetet med informations- och cybersäkerhet har sin utgångspunkt i kommunens Policy för informationssäkerhet. Denna riktlinje syftar till att konkretisera informationssäkerhetspolicyn vad avser hur informations- och cybersäkerhetsarbetet bedrivs i kommunen. Den anger vilka roller som ingår i organisationen, fastställer ansvarsfördelningen, och beskriver hur arbetet för att initiera, bibehålla och förbättra går till. Det övergripande målet med riktlinjen är att tillse att det operativa informationssäkerhetsarbetet bedrivs i enlighet med vad som är fastställt samt relaterar till gällande lagstiftning.

Riktlinjen gäller för alla kommunens verksamheter och förvaltningar. Kommunstyrelsen ska med stöd av denna riktlinje kunna styra kommunens informationssäkerhetsarbete i enlighet med Myndigheten för civilt försvars rekommendationer för kommuners informationssäkerhet samt med beaktande av kraven i informationssäkerhetsstandarden ISO/IEC 27000, där så anges i tillämpningsanvisningarna.

Riktlinjen omfattar all information oavsett format. I de fall informationen hanteras digitalt omfattas samtliga verksamhetssystem, appar och tjänster. Om information behandlas i en extern miljö ska behandlingen vara reglerad i avtal i enlighet med denna riktlinje.

Riktlinjen förvaltas av informationssäkerhetssamordnare och revideras vid behov.

2. Organisation och ansvarsfördelning

2.1 Grundprincip

Arbetet med informationssäkerhet ska vara systematiskt, riskbaserat och integrerat med befintliga sätt att leda och styra.

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret och sträcker sig på så sätt från den politiska ledningen och ner till varje enskild medarbetare. Den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt etcetera) är också formellt ansvarig för informationssäkerheten i verksamheten.

All information som behandlas i Sunne kommun ska vara identifierad, informationsklassad och förtecknad samt ha genomgått en riskanalys. Av förteckningen ska det framgå vem som är informationsägare. Verksamhetssystem, appar och tjänster som används för att behandla information ska vara förtecknade, informationsklassade, ha genomgått en riskanalys samt ha en utsedd systemägare och systemförvaltare.

2.2 Ledning och ansvar

I Sunne kommun är ansvaret för informationssäkerhet fördelat på följande sätt.

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhetsarbete och ansvarar för att kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet utarbetas och hålls aktuella. Kommunstyrelsen ansvarar även för övergripande styrning och uppföljning av att beslutade åtgärder genomförs och att målen för informationssäkerhetsarbetet uppnås.

Varje nämnd och kommunalägt bolag ansvarar för informationssäkerheten inom sitt verksamhetsområde och ska löpande planera, genomföra och följa upp åtgärder för att upprätthålla tillräcklig intern kontroll. Ansvaret för informationssäkerheten följer på det viset verksamhetsansvaret.

Varje chef ansvarar för att det i deras område/ enhet/ avdelning finns förutsättningar att bedriva informationssäkerhetsarbete. Vidare ansvarar de för att säkerställa att medarbetare har ett säkerhetstänk och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet ska kunna uppnås. Ansvaret omfattar även att tillgängliga verksamhetssystem, appar, tjänster används på avsett sätt.

Alla medarbetare har ett ansvar att följa gällande bestämmelser kring informationssäkerhet. Varje medarbetare är ska rapportera informationssäkerhetsrelaterade brister och incidenter.

2.3 Roller och ansvar

Informationssäkerhetsarbetet kräver en tydlig ansvarsbeskrivning där det framkommer vad varje roll förväntas och ska göra. Ansvar och ansvarsområden som står i konflikt med varandra ska åtskiljas. Detta görs bland annat genom att definiera rollerna informationsägare, systemägare och systemförvaltare.

2.3.1 Informationsägare

Informationsägare är den som äger och ansvarar för informationens riktighet och tillförlitlighet samt hur informationen får spridas och användas. Informationsägaren ska:

- säkerställa att informationen är identifierad och klassad,
- säkerställa att riskanalyser genomförs och att proportionerliga säkerhetsåtgärder beslutas och följs upp,
- säkerställa att verksamhetssystem/tjänster som hanterar information har utpekad systemägare.

2.3.2 Systemägare

Är den som har utpekat ansvar för ett eller flera verksamhetssystem, appar eller tjänster. Systemägaren ska:

- säkerställa att systemet uppnår en skyddsnivå som motsvarar skyddsbehovet hos den information som hanteras, inkluderat kontinuerlig kontroll av leverantörskedjerisker och att nödvändiga uppdateringar görs,
- utse systemförvaltare för det aktuella systemet och säkerställa att systemförvaltaren har rätt kompetens och resurser i rollen som systemförvaltare,
- tillsammans med systemförvaltare säkerställa att nödvändiga klassningar och riskanalyser genomförs med lämplig regelbundenhet samt vid införande och större förändringar,
- ha styrning för behörigheter (roll- och behovsstyrt, minsta privilegium) samt säkerställa att behörigheter avslutas vid byte/ avslut av tjänst,
- säkerställa att säkerhetskrav ställs i avtal och följs upp inom systemets livscykel,
- vid externa incidenter hantera dessa i samråd med och/eller på rekommendation av leverantör, genomföra åtgärder på kort och lång sikt,
- vid interna incidenter genomföra åtgärder på kort och lång sikt i samråd med informationssäkerhetssamordnare och dataskyddsombud om tillämpligt.

2.3.3 Systemförvaltare

Systemförvaltaren bistår användare och stödjer förvaltningen av systemet i syfte att upprätthålla en hög informationssäkerhet. Systemförvaltaren ska:

- stödja användare och medverka till att rutiner och arbetssätt i systemet främjar säker hantering,
- medverka i arbete med förändringar, uppföljning och dokumentation enligt systemägarens styrning,
- bidra till att identifierade brister, risker och incidenter rapporteras och omhändertas.

3. Roller och ansvar för stöd, samordning och kontroll

3.1 Styrgrupp för informationssäkerhetsarbetet

Styrgruppen utgörs av kommunledningsgruppen och ansvarar för att:

- strategiskt styra, stödja och leda arbetet med informationssäkerhet,
- besluta om genomförande av övergripande utbildning,
- vara vägledande vid allvarligare incidenter.

För att säkerställa att styrgruppen kan fullgöra sitt ansvar att strategiskt styra, stödja och leda informationssäkerhetsarbetet sammankallar informationssäkerhetssamordnare styrgruppen vid behov. Detta sker när frågor kräver strategiska ställningstaganden, vägledning eller beslut på ledningsnivå. Informationssäkerhetssamordnare ansvarar då för att:

- ta fram och presentera det underlag styrgruppen behöver för att kunna utöva sin styrande funktion och fatta informerade beslut i enlighet med styrgruppens uppdrag.

3.2 Informationssäkerhetsforum

Frågor relaterat till informations- och cybersäkerhet diskuteras, utreds, analyseras och bereds även i andra relevanta forum inom kommunen. Dessa forum är icke-beslutsfattande och agerar stödjande samt lyfter ärenden till styrgruppen vid behov.

- **Strategiska digitaliseringsgruppen**, ska med ett kommunövergripande perspektiv arbeta proaktivt och bidra till samsyn kring större digitala frågor,
- **Forum för säkerhet och beredskap**, verkar för att säkerhetsarbetet inom kommunen bedrivs sammanhållet och konsekvent.

3.3 Informationssäkerhetssamordnare

Informationssäkerhetssamordnaren leder, utvecklar och samordnar kommunens informationssäkerhetsarbete. Utgör strategiskt stöd till ledning och operativt stöd till verksamheterna och medarbetare så att de i sin tur kan ta ansvar för informationssäkerheten i sitt arbete.

- ge metodstöd och vägledning i informationssäkerhetsfrågor,
- arbeta med kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom kommunen, exempelvis genom utbildning,
- vid behov och som minst årligen följa upp och sammanställa lägesbild för informationssäkerheten,
- vara kontaktpunkt vid frågor från externa parter/ tillsyn,
- ta emot och utreda informationssäkerhetsincidenter samt rekommendera åtgärder,
- ansvara för omvärldsbevakning inom informationssäkerhetsområdet,

3.4 Kontaktpersoner

Samordnar arbetet med informationssäkerhet i den egna verksamheten/bolaget. Ska ges resurser för att kunna utföra uppdraget och ansvarar för att:

- driva på arbetet med informationssäkerhet i den egna verksamheten,
- i dialog med informationssäkerhetssamordnare vägleda verksamheten i frågor relaterade till informationssäkerhet,

Kontaktpersonerna möts fyra gånger per år för att diskutera olika frågor kring informationssäkerhet. De ska på träffarna också få den utbildning de behöver för att kunna utföra sitt uppdrag. Informationssäkerhetssamordnare är sammankallande för träffarna.

3.5 IT- funktion/ IT-säkerhetsansvar

IT-funktionen ansvarar för att möjliggöra och stödja genomförandet av tekniska och driftsrelaterade säkerhetsåtgärder. Systemägaren ansvarar dock fortsatt för *vilka* krav som ska gälla utifrån informationens behov.

- samordnar arbetet med säkerheten i Sunne kommuns IT-miljö,
- agerar stödjande vid eskalering av IT- och IT-säkerhetsincidenter,
- bedriver omvärldsbevakning för IT-miljön.

4. Ledningssystem för informationssäkerhet (LIS)

Ett ledningssystem är ett strukturerat ramverk av processer, rutiner och riktlinjer som ska användas för att styra, följa upp och kontinuerligt förbättra verksamheten mot uppsatta mål. Sunne kommuns ledningssystem för informationssäkerhet (LIS) utgör ramen för hur kommunen systematiskt ska skydda och hantera information, och ska tillsammans med tillhörande tillämpningsanvisningar och rutiner konkretisera och reglera informationssäkerhetsarbetet i kommunen.

LIS omfattar alla verksamheter, all information och alla system som behandlas i kommunen. Hantering av säkerhetsskyddsklassificerade uppgifter regleras separat enligt säkerhetsskyddslagen (2018:585).

Kommunens informationssäkerhetsarbete ska vara långsiktigt och kontinuerligt samt utgå från tillämpliga delar av SS-ISO/IEC 27000-serien. Styrningen av arbetet sker genom dokument på olika nivåer som anger ansvar, krav och ramar:

- Informationssäkerhetspolicy, antas av kommunfullmäktige,
- Riktlinje för informationssäkerhetsarbetet, beslutas av kommunstyrelsen,
- Tillämpningsanvisningar, instruktioner och rutiner, beslutas av styrgruppen för informationssäkerhetsarbetet.

Dokumenten fungerar tillsammans som ett sammanhållet system för att säkerställa att informationssäkerhetsarbetet i kommunen bedrivs enhetligt och ändamålsenligt. LIS bygger på en strukturerad och återkommande arbetscykel där kommunen planerar, genomför, följer upp och förbättrar sitt informationssäkerhetsarbete. Arbetet genomförs löpande i verksamheterna och utgör kärnan i hur kommunen omsätter sitt ansvar enligt standarder och lagkrav i praktiken.

Nedan följer fyra steg som tillsammans beskriver hur LIS tillämpas. Respektive verksamhet, enhet eller avdelning ansvarar för att inom ramen för gällande styrande dokument genomföra nödvändiga analyser, bedömningar och åtgärder avseende information, system, tjänster och arbetssätt. På detta sätt fungerar LIS som det samlade verktyget för att konkretisera hur informationssäkerhetsarbetet ska bedrivas i kommunen.

4.1 Identifiera och analysera

Förutsättningar som påverkar informationssäkerheten ska kontinuerligt identifieras och analyseras. Detta inkluderar:

- externa krav så som lagar, avtal och nationella riktlinjer,
- interna krav på informationens värde, känslighet och betydelse för kommunens verksamheter,

- informations- och cybersäkerhetsrelaterade risker, inklusive risker relaterade till leverantörer och digitala tjänster,
- verksamhetskritisk information och system som underlag för prioritering av säkerhetsåtgärder.

Arbetet innefattar bland annat informationsklassning och riskanalyser. Bedömningar ska ta hänsyn till konsekvenser för verksamheten, förtroendet för kommunen samt risker för enskilda individer.

4.2. Utforma och införa

Utifrån de krav, behov och risker som identifierats ska verksamheterna, med stöd av centrala funktioner, utforma och införa lämpliga säkerhetsåtgärder och rutiner. Detta omfattar bland annat:

- behörighetsstyrning och principen om minsta behörighet,
- incidenthantering,
- personalsäkerhet, inklusive säkerhetsrelaterade moment före, under och vid avslut av anställning eller uppdrag,
- informationssäkerhetskrav vid anskaffning, utveckling och avveckling av system och digitala tjänster,
- kontinuitetsplanering, för att säkerställa att verksamhetskritisk information och funktioner kan upprätthållas eller återställas vid störningar.

Åtgärderna ska vara proportionerliga i förhållande till de risker som identifierats och bör därför föregås av aktiviteterna i 4.1 Identifiera och analysera.

4.3 Följa upp, utvärdera och förbättra

Arbetet med informations- och cybersäkerhet ska följas upp regelbundet för att säkerställa att:

- risker hanteras enligt plan,
- säkerhetsåtgärder fungerar och är ändamålsenliga,
- incidenter och avvikelser hanteras korrekt,
- lagar, krav och interna styrdokument efterlevs,
- utbildningsinsatser och medvetandehöjande åtgärder ger effekt,
- eventuella revisions- och tillsynsresultat tas om hand.

Informationssäkerhetsarbetet ska kontinuerligt förbättras baserat på:

- resultat från uppföljningar och revisioner,
- förändringar i hotbild, teknik och omvärld,
- erfarenheter från incidenter och avvikelser,
- förändringar i lagstiftning eller verksamhetsbehov.

Uppföljning ska ske vid behov, och som minst en gång årligen. Förändringsarbetet ska göras löpande och utgå från principen om ständig utveckling. Informationssäkerhetssamordnare ansvarar för den samlade kommunövergripande uppföljningen och rapporterar resultatet till kommunstyrelse och kommunledningsgrupp i form av ledningens genomgång och årsrapport.

5. Informationsklassning

Informationsklassning är en grundläggande komponent i informationssäkerhetsarbetet. Genom att klassa information utifrån krav på dess konfidentialitet, riktighet, tillgänglighet och spårbarhet skapas förståelse för och möjlighet att styra vilket skydd som krävs för en viss information. Främst handlar det om att skyddet ska bli tillräckligt, men ibland också för att undvika överskydd med onödigt höga kostnader som följd. Klassning av information ska ske utifrån externa krav som lagar och föreskrifter, men även utifrån interna krav på informationens värde, känslighet och betydelse för verksamheten.

Informationsklassning ska genomföras för all kommunens information för att därefter kunna tilldela informationen lämpligt skydd. Samtliga bedömningar av skyddsbehov för information ska göras enligt kommunens modell för informationsklassning. Modellen består av fyra konsekvensnivåer vilka framgår av nedanstående tabell (nivå 0–3).

Tabell 1. Säkerhetsaspekter och konsekvensnivåer

Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
3 Allvarlig	Röjande av information medför allvarlig skada. Information där förlust av konfidentialitet kan leda till allvarliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust, kommunen eller annan part.	Information som om den inte är riktig och fullständig medför allvarlig konsekvens för verksamhetens förmåga, förtroende eller ekonomisk förlust, kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför allvarlig konsekvens för verksamhetens förmåga, förtroende eller ekonomisk förlust, kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför allvarlig konsekvens för verksamhetens förmåga, förtroende eller ekonomisk förlust, kommunen eller annan part.

2 Betydande	Röjande av information medför betydande skada. Information där förlust av konfidentialitet kan leda till betydande konsekvenser för verksamhetens förmåga, förtroenden eller ekonomisk förlust, kommunen eller annan part.	Information som om den inte är riktig och fullständig medför betydande konsekvens för verksamhetens förmåga, förtroenden eller ekonomisk förlust, kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför betydande konsekvens för verksamhetens förmåga, förtroenden eller ekonomisk förlust, kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför betydande konsekvens för verksamhetens förmåga, förtroenden eller ekonomisk förlust, kommunen eller annan part.
1 Måttlig	Röjande av information medför måttlig skada. Information där förlust av konfidentialitet kan leda till måttliga konsekvenser för verksamhetens förmåga, förtroenden eller ekonomisk förlust, kommunen eller annan part.	Information som om den inte är riktig och fullständig medför måttligt negativ konsekvens för verksamhetens förmåga, förtroenden eller ekonomisk förlust, kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför måttligt negativ konsekvens för verksamhetens förmåga, förtroenden eller ekonomisk förlust, kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför måttligt negativ konsekvens för verksamhetens förmåga, förtroenden eller ekonomisk förlust, kommunen eller annan part.
0 Obetydlig eller försumbar	Röjande av information medför ingen eller försumbar skada. Information där förlust av konfidentialitet inte medför någon negativ påverkan för kommunen eller annan part.	Information som ändrats medför ingen eller försumbar skada. Förlust av riktighet medför ingen negativ påverkan för kommunen eller annan part.	Information som om den inte är tillgänglig medför obetydlig eller försumbar skada för kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför obetydlig eller försumbar skada för kommunen eller annan part.

Med annan part avses annan organisation, extern aktör, medborgare eller enskild individ.

Observera att den lägsta skyddsnivån (0-Obetydlig eller försumbar) representerar information som skulle kunna ligga öppen, inte behöver något skydd mot insyn och som normalt inte har begränsad åtkomst. Däremot är det viktigt att informationen går att förstå, är korrekt och finns tillgänglig, därför kan även öppen information ha ett skyddsbehov vad gäller riktighet, tillgänglighet och spårbarhet. Gränsen mellan informationsklass 0 och 1 avseende konfidentialitet är om informationen är tänkt (eller möjlig) att spridas, exempelvis via intranät och webbplats.

För mer detaljerad beskrivning av informationsklassningsprocessen, se rutin för informationsklassning.

Informationsklassningar lagras där styrgruppen för informationssäkerhetsarbetet anser det lämpligt och kan vid behov beläggas med sekretess enligt offentlighets- och sekretesslagen (2009:400) 18 kap. 13 §.

6. Riskanalys

Risker som har betydelse för informationssäkerheten i Sunne kommuns olika verksamheter ska identifieras, dokumenteras och hanteras. Riskerna ska identifieras och analyseras minst en gång och sedan följas upp kontinuerligt samt vid förändringar som har betydelse för informationssäkerheten. Efter den första riskanalysen kan eventuella ytterligare risker identifieras vid incidenter, uppmärksammade brister i informationssäkerhetsskyddet, omvärldsbevakning (generella hotbildstrender), anskaffning, utveckling och förändring av IT-stöd med mera. Alla riskanalyser som görs i ett informationssäkerhetssyfte ska göras enligt kommunens modell för riskanalys för informationssäkerhet. Riskanalysen ska alltid föranledas av en informationsklassning.

För varje risk bedöms eventuella konsekvenser av att en viss information inte har lämpligt skydd. Vid riskanalysen ska verksamheten, utifrån en konsekvens- och sannolikhetstabell, bedöma skyddsbehovet av en viss information genom att analysera, beskriva och värdera konsekvenserna och sannolikheten på en skala ett (1) till fyra (4) av att informationen i fråga:

- Sprids/görs tillgänglig för obehörig
- Inte är tillgänglig
- Inte stämmer
- Bearbetning av informationen inte går att härledas till vem och när.

För mer detaljerad beskrivning av riskhanteringsprocessen, se rutin för riskanalys av information.

Riskanalyser lagras där styrgruppen för informationssäkerhetsarbetet anser det lämpligt och kan vid behov beläggas med sekretess enligt offentlighets- och sekretesslagen (2009:400) kap. 18 § 13.

7. Säkerhetsåtgärder

Informationsklassningar och riskanalyser används som grund för att kunna fastställa lämpliga och proportionella säkerhetsåtgärder för hantering av information, system och tjänster. Säkerhetsåtgärderna ska utformas utifrån ett allriskperspektiv och ge en säkerhetsnivå som är lämplig i förhållande till identifierade risker och möjliga konsekvenser.

Säkerhetsåtgärder ska beaktas tidigt i processen vid upphandlingar, projekt och större förändringar i IT-miljö, systemstöd eller arbetssätt, så att krav kan integreras i planering, kravställning och avtal. Motsvarande bedömning ska göras vid personalrelaterade moment så som anställning, förändring i roller och behörigheter samt vid avslut av anställning eller uppdrag.

Säkerhetsåtgärder är antingen tekniska, driftsrelaterade eller organisatoriska. För att uppnå ett fullgott skydd krävs ofta en kombination av olika åtgärder. De ska alltid utformas i paritet med den eventuella konsekvens som kan uppstå om risken eller hotet realiseras. Det är därför viktigt att göra realistiska värderingar för att undvika att informationen får ett onödigt högt skydd, med höga kostnader som följd, eller för lågt skydd vilket innebär en för stor riskoptimering.

Bilaga 1. Begreppsförklaring

Behörighet – tilldelade rättigheter att använda information eller en IT-resurs på ett specificerat sätt.

Cybersäkerhet- Tekniker, metoder och processer för att bevara och skydda digitala tillgångar från skador, angrepp eller obehörig åtkomst.

Hot- Möjlig oönskad händelse med negativa konsekvenser för verksamheten.

Informationssäkerhet – Konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information.

Informationstillgång – Information som är av värde för organisationen och av de resurser som hanterar den. Exempelvis människor, mjukvara, hårdvara och immateriella tillgångar (till exempel rykte).

Incident – En eller flera händelser som har inneburit, eller kan tänkas innebära, konsekvenser för verksamheten eller enskild person och som hotar informationssäkerheten.

Informationsmängd - En gruppering av information, exempelvis i form av ett dokument, en databas eller liknande. En informationsmängd innehåller en eller flera informationstyper.

Informationsklassning - Att genom klassificering identifiera skyddsbehovet för en viss information.

Konfidentialitet - Att information inte tillgängliggörs eller avslöjas till obehörig.

Ledningssystem för informationssäkerhet (LIS) - En metod för att arbeta övergripande och systematiskt med informationssäkerhet.

Riktighet – Att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning.

Risk – Produkten av sannolikheten för och konsekvensen av att ett hot realiseras.

Spårbarhet - Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs.

Säkerhetsåtgärder - Identifierad uppsättning förebyggande åtgärder för att möta risker. Tillgänglighet - Att information är åtkomlig och användbar av behörig.

Verksamhetssystem – Kan även kallas informationssystem, IT-system eller systemstöd) De system som insamlar, lagrar, bearbetar eller distribuerar och presenterar information.