KUNGÄLVS KOMMUN

# Riktlinjer för informationssäkerhet

**Riktlinje**

Diarie-/dokumentnummer: KS2023/1938
Beslut: 2023-12-13, Kommunstyrelsen §353/2023
Beredande politiskt organ: Kommunstyrelsen
Ersätter tidigare beslut 2021-05-26, Kommunstyrelsen, §20/2021
Giltighetstid: 2026-12-31
Dokumentansvarig: Säkerhetschef
Senast uppdaterad av: Martin Holm

KUNGÄLVS KOMMUN

# Innehållsförteckning

KUNGÄLVS KOMMUN

## 1. Inledning

Riktlinjerna ska säkerställa kommungemensamma regler för hantering av informationssäkerhet som inte hanteras i informationssäkerhetspolicyn. Riktlinjerna är övergripande och ska appliceras på all informationshantering inom samtliga nämnder. Enskilda informationstillgångar eller system kan vara i behov av individuella riktlinjer eller rutiner och ska i så fall ses som komplement till dessa riktlinjer.

## 2. Relation till andra styrdokument

- Informationssäkerhetspolicy
- Program för digitalisering av Kungälvs kommun

## 3. Syfte

Riktlinjerna ska säkerställa en hög gemensam säkerhet med bibehållen effektivitet i kommunens informationshantering i enlighet med Informationssäkerhetspolicyn. Kommunens information ska behandlas likvärdigt och lagligt utifrån informationens skyddsvärde oavsett i vilken verksamhet eller informationstillgång den behandlas.

## 4. Mål och viljeinriktning

Riktlinjerna ska tillse att information får ett adekvat skydd utifrån laglighet och lämplighet i syfte att uppfylla rättsliga krav samt de mål som fastställts av kommunfullmäktige i Informationssäkerhetspolicyn.

## 5. Definition av informationssäkerhet

Informationssäkerhet definieras i enlighet med SIS-TR 50:2015 som *bevarande av informationens konfidentialitet, riktighet och tillgänglighet.*

Ovanstående kan även uttryckas på följande sätt:

- Information finns endast tillgänglig för de som är behöriga (Konfidentialitet)
- Information skyddas mot oavsiktlig eller avsiktlig förvanskning (Riktighet)
- Information skall kunna nås och användas när den behövs (Tillgänglighet).

## 6. Principer för informationssäkerhetsarbetet

- Informationssäkerhetsarbetet baseras på SS-EN ISO/IEC 27000:2022 standarden.
- Informationssäkerhetssamordnare ska en gång per år rapportera det gångna årets informationssäkerhetsarbete till kommunstyrelsen.
- Det ska finnas en informationssäkerhetsgrupp som stöttar informationssäkerhetssamordnaren i sitt arbete.

## 7. Ansvar och roller för informationssäkerhetsarbetet

Följande roller och ansvar finns i kommunens informationssäkerhetsarbete

- **Kommunstyrelsen** Ansvarar ytterst för informationssäkerhetsarbetet.
- **Övriga nämnder** Har övergripande ansvar för att informationssäkerhetsarbetet bedrivs inom nämndens verksamhetsområde.

- **Systemägare** Ansvarar för säkerheten i informationstillgångar, klassning av informationstillgångar samt för genomförande av riskåtgärder.
- **Systemförvaltare** Stödjer Systemägaren i arbetet med informationssäkerhet, ofta ansvarig för riskåtgärd.
- **Säkerhetsskyddschef** Ansvarar för informationssäkerhetsarbetet med säkerhetsskyddsklassad information.
- **Enskilda medarbetare** Ansvarar för att följa rutiner, policys, riktlinjer och tillämpningsanvisningar.
- **Informationssäkerhetssamordnare** Ansvarar för att leda och samordna informationssäkerhetsarbetet.
- **Informationssäkerhetsgrupp** Stöttar informationssäkerhetssamordnaren.

## 8. Hantering av avvikelser och undantag

Kommunfullmäktige beslutar om undantag av principiell karaktär från styrdokument inom informationssäkerhetsområdet. Kommunstyrelsen beslutar om undantag av icke-principiell karaktär från styrdokument inom informationssäkerhetsområdet.

Större avvikelser rapporteras så snart som möjligt till förvaltningsledningen och vid behov till kommunstyrelsen. Mindre avvikelser sammanfattas i den årliga rapporten till kommunstyrelsen.

För rapportering gällande efterlevnad av Dataskyddsförordningen ansvarar Dataskyddsombud.

## 9. Tekniska krav

### a. Dokumentation av IT-miljö

Kommunstyrelsen ska tillse att det finns uppdaterad dokumentation över:

1. hård- och mjukvara som används i varje enskilt informationssystem.
2. beroenden mellan olika interna informationssystem respektive beroenden av informationssystem hos externa aktörer.
3. vilka informationssystem som behandlar information som har behov av utökat skydd, exempelvis enligt säkerhetsskyddslagen, känsliga personuppgifter, NIS-direktivet.
4. vilka informationssystem som är centrala för kommunens förmåga att utföra sitt uppdrag.

### b. Utveckling, anskaffning och utkontraktering

Systemägare ska, vid utveckling, anskaffning eller utkontraktering av informationssystem, identifiera krav på säkerhet avseende:

1. uppdelning i nätverkssegment
2. filtrering av nätverkstrafik
3. behörigheter, digitala identiteter och autentisering
4. krav på dokumentation av mjuk- och hårdvara
5. kryptering
6. säkerhetskonfigurering
7. säkerhetstester och granskningar
8. ändringshantering, uppgradering och uppdatering
9. spårbar och korrekt tid
10. säkerhetskopiering

11. säkerhetsloggning och tillhörande analys
12. övervakning av nätverkstrafik
13. övervakning av informationssystem inklusive säkerhetsfunktioner
14. Möjlighet till intrångsdetektering
15. skydd mot skadlig kod
16. skydd av utrustning
17. redundans och återställning
18. kontinuitet under fredstida krissituation samt inför och vid höjd beredskap
19. arkivering
20. avveckling

Systemägare ska, innan driftsättning och inför förändring som kan påverka säkerheten i informationssystemen,

1. genom säkerhetstester och granskning kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet
2. verifiera att det finns nödvändig dokumentation för drift och förvaltning.

Nödvändig dokumentation för drift och förvaltning bör omfatta arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation. Av dokumentationen bör även framgå vem som är systemägare samt om och till vilken extern aktör informationssystemet är utkontrakterat.

I de fall brister identifieras ska systemägare riskbedöma och hantera dessa brister innan driftsättning eller inför förändring som kan påverka säkerheten i informationssystemen.

### c. Utvecklings-, test- och utbildningsmiljöer

Systemägarens arbete med utveckling och tester som kan påverka informationssäkerheten i produktionsmiljön ska ske i en från produktionsmiljön avskild del av IT-miljön.

Systemägaren ska identifiera och hantera behovet av en utbildningsmiljö som är avskild från produktionsmiljön.

### d. Uppdelning i nätverkssegment och filtrering av nätverkstrafik

Kommunstyrelsen ska tillse att spridning av incidenter och konsekvenser av angrepp minskas genom att placera informationssystem med olika funktioner i separata nätverkssegment i sin produktionsmiljö. Följande funktioner i produktionsmiljön ska placeras i separata nätverkssegment:

1. Klienter för användare
2. Klienter för administration
3. Servrar
4. Centrala systemsäkerhetsfunktioner i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande
5. Centrala stödfunktioner i form av skrivare, scanner och liknande
6. Trådlösa nätverk
7. Gästnätverk
8. Externt åtkomliga tjänster
9. Informationssystem som sammankopplas med informationssystem hos extern aktör
10. Industriella informations- och styrsystem
11. System som innehåller sårbarheter som inte kan hanteras

Nätverkstrafiken ska filtreras så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.

Verksamhetssystem som hanterar säkerhetsklassificerade uppgifter skall följa säkerhetspolisens riktlinjer för skyddsåtgärder.

## e. Behörigheter, digitala identiteter och autentisering

Kommunstyrelsen ska tillse att endast behöriga användare och informationssystem har åtkomst till IT-miljön och utforma sin behörighetshantering på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver.
Behörighetshanteringen bör säkerställa att:

1. digitala identiteter i produktionsmiljön är unika.
2. digitala identiteter och behörigheter är godkända innan de kopplas till en användare eller ett informationssystem.
3. tilldelade behörigheter kan vara tidsbegränsade och ska kontrolleras en gång per år eller vid ändring i tjänst.
4. behovet av att använda olika kataloger för digitala identiteter och behörigheter är identifierat och hanterat.

En digital identitet ska endast användas av en individ.

Digitala identiteter som ger systemadministrativ behörighet ska endast användas för systemadministration och tilldelas restriktivt. Flerfaktorsautentisering ska användas vid

1. egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk
2. systemadministrativ åtkomst till informationssystem
3. åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd.

## f. Kryptering

Kommunstyrelsen ska tillse att behovet av kryptering identifieras för att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring.

Kryptering bör användas för att skydda

1. säkerhetsloggar mot obehörig åtkomst och obehörig förändring
2. autentiseringsuppgifter mot obehörig åtkomst och obehörig förändring
3. information i behov av utökat skydd mot obehörig åtkomst och obehörig förändring vid överföring till informationssystem utanför kommunens kontroll.

Det skall även finnas möjlighet att kryptera e-postmeddelanden både mellan enskilda användare och även vid överföring av e-post till och från andra statliga myndigheter och kommuner.

Kommunen skall alltid kunna verifieras som avsändare respektive mottagare av e-post.

DNSSEC (Domain Name System Security Extensions) skall alltid användas avseende samtliga domännamn som kommunen registrerat i domännamnssystemet (DNS).

Kommunstyrelsen ska tillse att interna regler för kryptering finns med krav på

1. hantering av krypteringsnycklar
2. godkännande och förvaltning av krypteringslösningar
3. hur krypteringsalgoritmer, krypteringsprotokoll och nyckellängder ska väljas.

## g. Användning av AI

Användandet av AI (Artificiell Intelligens) skall alltid utvärderas innan ett nytt system börjar användas eller att en ny funktion i ett befintligt system införs. Det är viktigt att genomföra en riskanalys av:

- Vilken information som kan komma att hanteras, får den hanteras av AI?
- Vad riskeras att lämnas ut oavsiktligt om regelverk för AI inte är komplett?
- Vad skulle en injektion av illasinnad kod kunna medföra för det egna och andra system?
- Kan informationen, grunddata, som AI använder manipuleras?
- Kan komplexa eller illasinnade frågor till AI medföra att tjänsten blir otillgänglig, en typ av Denial off Service?
- Kan en leverantör av AI utgöra en svaghet och ingång av attackerare? (Supply chain attack)
- Vilka behörigheter kommer AI att ha, kan de medföra att systemet kan utföra andra åtgärder än önskat?
- Finns risk för att AI kommer publicera eller skapa information som inte är korrekt?
- Finns risk för att AI kommer stjäla upprättskyddad information ifrån andra system?

## h. Säkerhetskonfigurering

Systemägaren ska, för att skydda informationssystem mot obehörig åtkomst:

1. byta ut förinställda autentiseringsuppgifter
2. stänga av, ta bort eller blockera (härda) systemfunktioner som inte behövs
3. i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet som krävts genom klassning av systemet och informationen i det.

## i. Säkerhetstester och granskningar

Kommunstyrelsen ska tillse att säkerhetstester och granskningar utförs och möjliggör identifiering av sårbarheter. Det ska finnas interna regler för hur kontroll görs av att:

1. informationssystemen är uppdaterade
2. valda säkerhetsåtgärder är införda på korrekt sätt
3. genomförda säkerhetskonfigurationer är tillräckliga

## j. Ändringshantering, uppgradering och uppdatering

Systemförvaltare ska säkerställa att förändringar i informationssystem genomförs på ett strukturerat och spårbart sätt. Det ska finnas interna regler för ändringshantering med krav på:

1. vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning
2. hur risker för incidenter och avvikelser i samband med förändring i produktionsmiljön ska identifieras och hanteras
3. hur mjukvara, utan onödigt dröjsmål, ska uppdateras till av utvecklare stödd version, inklusive säkerhetsuppdateringar
4. hur utbyte eller uppgradering av hård- och mjukvara som inte längre uppdateras eller stöds av leverantören ska säkerställas utan onödigt dröjsmål

5. hur risker ska hanteras när uppdatering eller uppgradering enligt punkt 3 och 4 inte kan genomföras.

## k. Korrekt och spårbar tid

Systemägaren ska tillse att tidstjänsten Swedish Distributed Time Service används.

## l. Säkerhetskopiering

Systemägaren ska tillse att information som förlorats eller förvanskats kan återställas. Detta genom att regelbundet säkerhetskopiera viktig information i systemet.

Systemägaren ska tillse att:

1. en gång per dygn säkerhetskopiera information som behövs för kommunens förmåga att utföra sitt uppdrag
2. en gång per år, eller vid större förändringar av produktionsmiljön, verifiera förmågan att, inom för kommunen godtagbar tidsperiod, återställa information från säkerhetskopior

Säkerhetskopior ska förvaras skilda från produktionsmiljön och skyddas mot skada, obehörig åtkomst och obehörig förändring.

## m. Säkerhetsloggning och övervakning

Systemägaren ska tillse, för att säkerställa spårbarhet i informationssystem, att följande säkerhetsrelaterade händelser loggas:

1. Obehörig åtkomst och försök till obehörig åtkomst till IT-miljö och enskilda informationssystem.
2. Förändringar av konfigurationer och säkerhetsfunktioner som förutsätter priviligierade rättigheter.
3. Förändringar av behörighet för användare och informationssystem.
4. Åtkomst till information som bedömts ha behov av utökat skydd.

Man ska analysera innehållet i säkerhetsloggarna i ett för ändamålet avsett informationssystem för att upptäcka och hantera incidenter och avvikelser. Säkerhetsloggarna ska:

1. möjliggöra utredning av intrång, tekniska fel och brister i säkerheten
2. utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar
3. vara tillgängliga för analys under fastställd bevarandetid

Man ska dokumentera hur säkerhetsloggarna ska användas samt var loggningsuppgifter hämtas och lagras, hur de skyddas och hur länge de ska bevaras.

Systemägaren ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd.

Systemägaren ska identifiera och hantera behovet av realtidsövervakning av informationssystem.

## n. Skydd mot skadlig kod

Systemägare ska tillse att mjukvara som ger skydd mot skadlig kod används. För informationssystem där sådan mjukvara inte finns tillgänglig ska andra åtgärder vidtas som ger motsvarande skydd.

### o. Skydd av utrustning

Systemägaren ska tillse att skydd finns för den utrustning som informationssystem består av mot skador och obehörig åtkomst, genom att:

1. placera centrala servrar och central nätverksutrustning i särskilda it-utrymmen
2. tilldela behörighet till särskilda it-utrymmen restriktivt
3. identifiera och hantera behovet av övervakning och larm i särskilda it-utrymmen
4. registrera tillträde till särskilda it-utrymmen på individnivå och spara dokumentationen under fastställd bevarandetid
5. ha interna regler för hur mobil utrustning ska skyddas

### p. Redundans och återställning

Systemägare ska, för att säkerställa tillgänglighet till information och informationssystem vid incidenter och avvikelser:

1. ha interna regler för återställning av produktionsmiljön i sin helhet och för enskilda informationssystem
2. öva återställning av informationssystem som är centrala för kommunens förmåga att utföra sitt uppdrag
3. placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika särskilda it-utrymmen

## 10. Administrativa krav

### a. Lösenordsregler

Kommunstyrelsen ska tillse att lösenord är minst tolv tecken långa där det är möjligt. Lösenordet kan innehålla specialtecken eller siffror samt stora och små bokstäver. Lösenordet bör ändras med jämna intervaller.
Lösenord ska alltid bytas vid misstanke om att det läckts eller avslöjats.

### b. Säkerhetsskyddssklassificerade handlingar

Kommunstyrelsen ska tillse att rutiner för hantering av säkerhetsskyddsklassificerade handlingar och verksamheter upprättas.

Kommunstyrelsen ska minst vartannat år aktualisera säkerhetsskyddsanalys för sin egen och andra nämnder verksamheter.

Kommunstyrelsen ska tillse att endast säkerhetsskyddsklassificerad personal har tillgång till informationssystem, handlingar eller verksamheter placerade i säkerhetsklass.

### c. Informationssäkerhetsgruppens sammansättning

Informationssäkerhetsgruppen ska bestå av:

1. Informationssäkerhetssamordnare
2. IT-strateg
3. Dataskyddsombud
4. Kontaktpersoner ifrån de olika sektorerna och staben

### d. Sekretessmarkering

Upprättade eller inkommande handlingar som kan antas innehålla uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen ska tillföras en sekretessmarkering. Sekretessmarkeringen ska innehålla:

- tillämplig sekretessbestämmelse
- datum då sekretessmarkeringen gjordes
- den nämnd som har gjort anteckningen

Systemägare ska tillse att mallar i verksamhetssystem innehåller funktionalitet för att tillföra sekretessmarkering på upprättade handlingar.

För handlingar i informationssystem där anteckning inte är möjlig ska filnamn eller liknande innehålla uppgifter om sekretessmarkering.

### e. Destruktion av fysiska handlingar och lagringsmedia

Pappershandlingar innehållandes sekretessuppgifter ska vid gallring förstöras genom förbränning. Handlingarna placeras i särskilda sekretesskärl utplacerade på varje våningsplan. Även digital media så som USB-minnen eller CD-skivor ska placeras här.

För destruktion av säkerhetsskyddsklassificerade handlingar se ”Tillämpningsanvisning för hantering av säkerhetsklassificerade uppgifter”.

## 11. Klassningsmodell

För att veta vilken information som behandlas inom kommunens verksamhet, hur viktig den är för verksamheten samt vilka risker som finns så klassas den. Detta är en del i det systematiska informationssäkerhetsarbetet. Detta sker genom kartläggning, riskanalys och klassning enligt gällande anvisning.

### a. Kartläggning

För att kunna genomföra klassningen måste informationen kartläggas vilket görs ihop med systemägare, systemförvaltare, informationssäkerhetssamordnare med flera som känner till vilken information som finns i det IT-system som kartläggs.

### b. Riskanalys

Nästa del är att identifiera vilka risker som finns mot informationen och vilka åtgärder som kan göras för att minska konsekvenserna av dessa.

### c. Klassning

Efter riskanalysen så skall själva klassningen av informationen ske och då utgår man ifrån fyra aspekter (Konfidentialitet, Riktighet, Tillgänglighet samt Spårbarhet) för att bedöma hur viktig informationen är för verksamheten. Vid klassningen använder man olika kategorier och nivåer för att precisera varför och på vilket sätt informationen är viktig.

#### I. Konsekvenskategorier

Konsekvenskategorier utgår från de värden som är viktiga för Kungälvs kommun att upprätthålla eller undvika. Konsekvenskategorierna kopplas till aspekterna konfidentialitet, riktighet och tillgänglighet och vilka konsekvenser ett bortfall av dessa kan få.

Konsekvenskategorier för Kungälvs kommun är

1. **Samhälle**. Vilka konsekvenser får bortfall av konfidentialitet, riktighet och tillgänglighet för samhällsviktig verksamhet eller samhället i stort. Exempel: kan samhällsviktig verksamhet med kommunal eller icke-kommunal huvudman upprätthålla sin verksamhet?
2. **Ekonomi**. Vilka konsekvenser får bortfall av konfidentialitet, riktighet och tillgänglighet för kommunens ekonomi. Exempel: uppstår större kostnader vid ett bortfall för kommunen eller någon annan?
3. **Verksamhet**. Vilka konsekvenser får bortfall av konfidentialitet, riktighet och tillgänglighet för den kommunala verksamheten? Exempel: är informationstillgången så kritisk att en större del av kommunens verksamhet inte kan fortgå vid exempelvis bortfall?
4. **Individ**. Vilka konsekvenser får bortfall av konfidentialitet, riktighet och tillgänglighet för enskild? Exempel: röjs känsliga personuppgifter eller kan ett bortfall av tillgänglighet påverka digitala vårdtjänster på ett negativt sätt?

### II. Konsekvensnivåer

Konsekvensnivåer avser uppdelning av allvarlighetsgrad vid påverkan på konfidentialitet, riktighet och tillgänglighet. Kommunen delar upp sina informationstillgångar i 5 nivåer där nivå 1 innebär försumbar påverkan och nivå 5 innebär synnerligen allvarlig påverkan. Se klassningsmatris nedan för definitioner av de olika nivåerna.

### III. Klassningsmatris

*Konfidentialitet*

| | | |
|---|---|---|
| Synnerligen allvarlig skada (5). Säkerhetsskydd | Skada för Sveriges säkerhet som inte endast är ringa. Kontakta säkerhetsskyddschef. | Röjande av informationen medför skada för Sveriges säkerhet som inte endast är ringa.<br>• Systemet behandlar information som omfattas av sekretess och rör Sveriges säkerhet där röjande av information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Uppgifter av bäring för totalförsvaret.<br>• Informationen omfattas av säkerhetsskyddslagen. |
| Allvarlig skada (4) | Allvarlig skada - ex massiv informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, eller fara för liv och hälsa | Röjande av information medför allvarlig skada.<br>• Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.<br>• Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt.<br>• Allvarlig kränkning av den personliga integriteten |
| Betydande skada (3) | Betydande skada - ex tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, eller förlust av skapat förtroende | Röjande av informationen medför betydande skada.<br>• Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).<br>• Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte.<br>• Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. |

| | | |
|---|---|---|
| Måttlig skada (2) | Måttlig skada - ex minskad förmåga att genomföra verksamhetens uppdrag, effektiviteten är påvisbart reducerad | Röjande av informationen medför måttlig skada.<br>• Inga märkbara större svårigheter för verksamheten att nå målen.<br>• Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.<br>• Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. |
| Försumbar skada (1) | Ingen eller försumbar skada | Röjande av informationen medför ingen eller försumbar skada.<br>• Inga svårigheter för verksamheten att nå målen.<br>• Ingen eller endast försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation. |

*Riktighet*

| | | |
|---|---|---|
| Synnerligen allvarlig skada (5). Säkerhetsskydd | Skada för Sveriges säkerhet som inte endast är ringa. Kontakta säkerhetsskyddschef. | Manipulation av informationen medför skada för Sveriges säkerhet som inte endast är ringa.<br>• Systemet behandlar information som omfattas av säkerhetsskyddslagen och rör Sveriges säkerhet där manipulation av information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Uppgifter av bäring för totalförsvaret.<br>• Informationen omfattas av säkerhetsskyddslagen. |
| Allvarlig skada (4) | Allvarlig skada - ex massiv informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, eller fara för liv och hälsa | Röjande av information medför allvarlig skada.<br>• Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.<br>• Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt.<br>• Allvarlig kränkning av den personliga integriteten |
| Betydande skada (3) | Betydande skada - ex tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, eller förlust av skapat förtroende | Röjande av informationen medför betydande skada.<br>• Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).<br>• Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte.<br>• Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. |

| | | |
|---|---|---|
| Måttlig skada (2) | Måttlig skada - ex minskad förmåga att genomföra verksamhetens uppdrag, effektiviteten är påvisbart reducerad | Röjande av informationen medför måttlig skada.<br>• Inga märkbara större svårigheter för verksamheten att nå målen.<br>• Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.<br>• Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. |
| Försumbar skada (1) | Ingen eller försumbar skada | Röjande av informationen medför ingen eller försumbar skada.<br>• Inga svårigheter för verksamheten att nå målen.<br>• Ingen eller endast försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation. |

*Tillgänglighet*

| | | |
|---|---|---|
| Synnerligen allvarlig skada (5). Säkerhetsskydd | Skada för Sveriges säkerhet som inte endast är ringa. Kontakta säkerhetsskyddschef. | Ett avbrott som medför skada för rikets säkerhet som inte endast är ringa.<br>• Systemet behandlar information som omfattas av säkerhetsskyddslagen och rör Sveriges säkerhet där manipulation av information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Uppgifter av bäring för totalförsvaret.<br>• Informationen omfattas av säkerhetsskyddslagen. |
| Allvarlig skada (4) | Allvarlig skada - ex massiv informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, eller fara för liv och hälsa | Ett avbrott medför allvarlig skada.<br>• Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.<br>• Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. • Individers liv och hälsa äventyras.<br>• Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i en allvarlig/katastrofal omfattning av otillgänglighet i systemet. |
| Betydande skada (3) | Betydande skada - ex tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, eller förlust av skapat förtroende | Ett avbrott medför betydande skada.<br>• Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).<br>• Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner vid egen eller annan organisation påverkas troligen inte.<br>• Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen.<br>• Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i en betydande omfattning av otillgänglighet till systemet. |

| | | |
|---|---|---|
| Måttlig skada (2) | Måttlig skada - ex minskad förmåga att genomföra verksamhetens uppdrag, effektiviteten är påvisbart reducerad | Ett avbrott medför måttlig skada.<br>• Inga märkbara större svårigheter för verksamheten att nå målen. • Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation<br>• Externa individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.<br>• Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas endast i begränsad omfattning av otillgänglighet till systemet. |
| Försumbar skada (1) | Ingen eller försumbar skada | Ett avbrott medför ingen eller försumbar skada.<br>• Inga eller försumbara svårigheter för verksamheten att nå målen.<br>• Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.<br>• Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas inte eller i försumbar omfattning av otillgänglighet till systemet. |

## 12. Levandegöra

Kommuniceras till systemägare, systemadministratörer och systemförvaltare. Publiceras på kommunens hemsida under styrande dokument.

## 13. Uppföljning

Uppföljning av arbetet med informationssäkerheten skall ske årligen och resultatet rapporteras till kommunstyrelsen.