Bilaga 3: Informationssäkerhet

Innehåll

1 Inledning

Informationssäkerhet ska:

(1) förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och
(2) förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.

Denna bilaga reglerar informationssäkerhet inom ramen för säkerhetsskydd. Den avser säkerhetsskyddsklassificerade uppgifter, säkerhetskänsliga uppgifter och handlingar, samt lagringsmedia som innehåller eller innehållit sådana uppgifter.

Bilagan omfattar säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass 4. Begränsat hemlig, 3. Konfidentiell och 2. Hemlig. Uppgifter i säkerhetsskyddsklass 1. Kvalificerat hemlig regleras inte i denna bilaga.

Denna bilaga omfattar säkerhetskänsliga uppgifter i konsekvensnivå D, C och B. Uppgifter i konsekvensnivå A regleras inte i denna bilaga.

Uppgifter som rör externa aktörers säkerhetskänsliga verksamhet och vars hantering kravställs i säkerhetsskyddsavtal eller säkerhetsskyddsöverenskommelser ska istället hanteras i enlighet med dessa krav.

Säkerhetsskyddsåtgärder inom informationssäkerhet ska integreras med säkerhetsskyddsåtgärderna inom personalsäkerhet och fysisk säkerhet.

1.1 Informationsklassificering

Uppgifter som är skyddsvärda ur ett konfidentialitetsperspektiv och omfattas av sekretess utgör säkerhetsskyddsklassificerade uppgifter. Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen i säkerhetsskyddsklasser görs enligt Säkerhetsskyddslag (2018:585) 2 kap. 5§ (se tabell 1 nedan).
Säkerhetsskyddsklassificeringen ska utgå ifrån aktuell förvaltnings eller bolags säkerhetsskyddsanalys, Göteborgs stads säkerhetsskyddsanalys (för förvaltningar) och särskilda säkerhetsskyddsbedömningar.

Om en förvaltning bedömer att en viss uppgift ska klassificeras som kvalificerat hemlig eller får kännedom om sådana uppgifter ska Göteborgs Stads säkerhetsskyddschef kontaktas omgående. Stadens säkerhetsskyddschef ska i sin tur informera stadsdirektören som beslutar om vidare hantering av uppgifterna.

Uppgifter som enbart ska skyddas ur ett riktighets- och/eller tillgänglighetsperspektiv ska inte säkerhetsskyddsklassificeras. Dessa ska delas in i konsekvensnivå utifrån den skada exempelvis ett sabotage kan orsaka Sveriges säkerhet i enlighet med Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1) 2 kap 5§. Dessa uppgifter benämns inom Göteborgs Stad säkerhetskänsliga uppgifter.

Säkerhetsskydds-klass	Den skada som ett röjande av uppgifterna kan medföra för Sveriges säkerhet	Värdeord till stöd för bedömningen om en viss typ av skada föreligger
Kvalificerat hemlig	Ett röjande kan medföra en synnerligen allvarlig skada.	Synnerligen allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa.
Hemlig	Ett röjande kan medföra en allvarlig skada.	Allvarliga/betydande negativa konsekvenser, av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funktioner. Svårt att återställa.
Konfidentiell	Ett röjande kan medföra en inte obetydlig skada	Påtagliga negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott.
Begränsat hemlig	Ett röjande kan medföra endast ringa skada	Ringa negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning.

Tabell 1: Från Säkerhetspolisens vägledning ”Informationssäkerhet”

1.2 Befattningar och funktioner

1.2.1 Säkerhetsskyddsregistratur

Vid förvaltningar som hanterar säkerhetsskyddsklassificerade uppgifter ska det finnas en säkerhetsskyddsregistratur om det inte är uppenbart obehövligt. Med uppenbart obehövligt avses i detta fall att förvaltningen genom avtal kan samnyttja säkerhetsskyddsregistratur tillhörande annan förvaltning inom staden.

Säkerhetsskyddsregistratur behöver inte vara en separat funktion, utan kan exempelvis vara en del av verksamhetens ordinarie registratur.

1.2.1.1 Säkerhetsskyddsregistrator

Säkerhetsskyddsregistraturen ska bemannas av minst en utsedd, behörig säkerhetsskyddsregistrator. Säkerhetsskyddsregistrator kan vara en tillikauppgift och innebär inte krav på en enskild befattning.

Säkerhetsskyddsregistrator ansvarar för registratorsuppgifter avseende säkerhetsskyddsklassificerade handlingar och lagringsmedia i enlighet med denna anvisning och framtagna metodstöd.

Säkerhetsskyddsregistrator har särskilda befogenheter och undantas från vissa krav på säkerhetsskyddsåtgärder. Detta gäller exempelvis krav på kvittering när säkerhetsskyddsregistrator tar emot en säkerhetsskyddsklassificerad handling för registrering, kopiering, distribution, arkivering eller förstöring, om inte den som överlämnar handlingen begär det. Det vill säga när registratorn hanterar handlingen i

egenskap av registrator och inte själv har behov av att ta del av uppgifterna handlingen innehåller. Detsamma gäller för lagringsmedia.

1.3 Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter

Medarbetare vid förvaltningar och bolag som tar del av säkerhetsskyddsklassificerade uppgifter ska vara säkerhetsprövade och utbildade i enlighet med bilaga 6 till denna anvisning.

Medarbetare ska endast ta del av uppgifter som är nödvändiga för befattningsutövandet. Medarbetare ska endast ta del av säkerhetsskyddsklassificerade uppgifter i den säkerhetsskyddsklass som omfattningen på deras säkerhetsprövning tillåter.

Beslut om behörighet att ta del av säkerhetsskyddsklassificerade uppgifter ska fattas av säkerhetsskyddsansvarig vid förvaltning eller säkerhetsskyddschef vid bolag.

Berörda förvaltningar och bolag ska ha en uppdaterad förteckning över de medarbetare som är behöriga att ta del av säkerhetsskyddsklassificerade uppgifter samt i vilken säkerhetsskyddsklass. Förteckning över beslutade behörigheter ska delges säkerhetsskyddsregistratur.

2 Hantering av säkerhetsskyddsklassificerade uppgifter

Säkerhetsskyddsklassificerade uppgifter och lagringsmedia[1] innehållande säkerhetsskyddsklassificerade uppgifter ska hanteras enligt de krav som framgår nedan. För berörda bolag gäller enbart följande stycken:

- 2.2 Inkommande
- 2.3 Anteckning
- 2.10 Elektronisk kommunikation
- 2.11 Delgivning
- 2.12 Distribution
- 2.14 Lagringsmedia

2.1 Upprättande av arbetsdokument och handlingar

Med säkerhetsskyddsklassificerad handling avses en handling som innehåller en säkerhetsskyddsklassificerad uppgift. Med säkerhetsskyddsklassificerad uppgift avses uppgift som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt

[1] Med lagringsmedia avses här även utrustning innehållande lagringsmedia.

offentlighets- och sekretesslagen (OSL 2009:400). Innan en handling är färdigställd anses den vara ett arbetsdokument.

Förvaltningar ska säkerställa att spårbarhet upprätthålls för både arbetsdokument och upprättade handlingar som innehåller säkerhetsskyddsklassificerade uppgifter.

Om en elektronisk handling bedöms kunna omfattas av säkerhetsskydd ska handlingen upprättas i av staden eller förvaltningen godkänt informationssystem i enlighet med denna anvisnings bilaga 4. Säkerhetsskyddsklassificerade uppgifter i en viss säkerhetsskyddsklass får endast behandlas i informationssystem eller på lagringsmedium som verksamhetsutövaren godkänt för lägst den säkerhetsskyddsklass som uppgifterna har.

2.2 Inkommande

När en handling inkommer till en berörd förvaltning eller bolag ansvarar denne (mottagaren) för att handlingen hanteras korrekt utifrån dess säkerhetsskyddsklassificering.

2.3 Anteckning

En säkerhetsskyddsklassificerad handling ska förses med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har. Första sidan stämplas med säkerhetsskyddsklass och stämpeln fylls i med tillämplig sekretessbestämmelse i offentlighets- och sekretesslagen (OSL 2009:400), datum samt verksamhetsutövare. För förvaltningar ska både aktuell förvaltning samt verksamhetsutövare anges. Exempelvis stadsledningskontoret, Göteborgs Stad. Om handlingen innehåller uppgifter med olika säkerhetsskyddsklass avgör den högsta säkerhetsskyddsklassen vilken anteckning (stämpel) handlingen ska ha.

Efterföljande sidor stämplas med information om handlingens säkerhetsskyddsklass och en hänvisning till första sidan.

En handling i säkerhetsskyddsklass 3. Konfidentiell eller högre ska i förekommande fall förses med anteckning om diarienummer, antal sidor och uppgift om bilagor. Utöver det ska handlingen exemplarnumreras även om det enbart finns ett exemplar.

Lagringsmedia som innehåller eller har innehållit säkerhetsskyddsklassificerade uppgifter ska vara märkta så att det framgår att de tillhör Göteborgs Stad samt förses med

anteckning om aktuell säkerhetsskyddsklass enligt ovan. Vidare ska lagringsmedia förses med identifieringsuppgift (PMFS 2022:1 3 kap. 11§).

Om lagringsmedia innehållande säkerhetsskyddsklassificerade uppgifter sitter fast monterade i IT-utrustning (exempelvis i en dator) så ska istället IT-utrustningen märkas på motsvarande sätt.

2.4 Diarieföring av säkerhetsskyddsklassificerade handlingar

I förvaltningar ska fysiska och digitala handlingar som innehåller säkerhetsskyddsklassificerade uppgifter registreras och diarieföras av säkerhetsskyddsregistrator. Registrering och diarieföring av säkerhetsskyddsregistrattor bör följa förvaltningen ordinarie rutiner, exempelvis genom en hänvisning i ordinarie system att handlingen förvaras på annan plats.

Lagringsmedia som innehåller eller har innehållit säkerhetsskyddsklassificerade uppgifter i ska vara registrerade i förteckning vid säkerhetsskyddsregistratur.

Säkerhetsskyddsregistrator ska säkerställa att register och förteckningar hålls uppdaterade.

2.5 Kvittering

Den som tar emot en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen 3. Konfidentiell eller 2. Hemlig ska kvittera mottagandet på ett kvitto. Mottagandet ska registreras i förteckning vid säkerhetsskyddsregistratur.

Den som tar emot lagringsmedia som innehåller, har innehållit, eller är avsedd att innehålla uppgifter i säkerhetsskyddsklassen 3. Konfidentiell eller 2. Hemlig ska kvittera mottagandet på ett kvitto. Mottagandet ska registreras i förteckning vid säkerhetsskyddsregistratur.

Samtliga fysiska handlingar och lagringsmedia som kvitterats ut ska återlämnas till säkerhetsskyddsregistratur. Återlämnandet ska kvitteras på kvitto och registreras i förteckning vid säkerhetsskyddsregistratur.

Samtliga kvittenser ska bevaras i 10 år vid säkerhetsskyddsregistratur.

2.6 Lokaler för hantering av handlingar och lagringsmedia

Handlingar och lagringsmedia innehållande säkerhetsskyddsklassificerade uppgifter ska hanteras i lokaler som är godkända för den säkerhetsskyddsklass som framgår av handlingen i enlighet med bilaga 5 i denna anvisning.

2.7 Förvaring

Handlingar och lagringsmedia innehållande säkerhetsskyddsklassificerade uppgifter ska hållas under ständig uppsikt eller förvaras i godkända förvaringsutrymmen i enlighet med bilaga 5 i denna anvisning.

2.8 Inventering

Inventering av samtliga säkerhetsskyddsklassificerade fysiska handlingar (inklusive utkvitterade) i säkerhetsskyddsklassen 3. Konfidentiell och 2. Hemlig ska ske minst en gång per år.

Lagringsmedia som innehåller uppgifter i säkerhetsskyddsklassen 3. Konfidentiell och 2. Hemlig ska inventeras minst en gång per år.

Inventering av utkvitterade säkerhetsskyddsklassificerade fysiska handlingar och lagringsmedia ska göras av säkerhetsskyddsregistrator och säkerhetsskyddsansvarig vid förvaltning.

Inventering ska ske mot diariet, förteckning och kvittenser.

2.9 Utskrift, skanning och kopiering av handlingar

Förvaltningar ska ha styrande dokument som säkerställer att spårbarhet upprätthålls för säkerhetsskyddsklassificerade uppgifter vid utskrift, skanning och kopiering. Exempelvis genom att handlingar endast får skrivas ut, skannas eller kopieras med hjälp av säkerhetsskyddsregistrator.

2.10 Elektronisk kommunikation

Säkerhetsskyddsklassificerade uppgifter får endast kommuniceras via av staden, förvaltningen eller bolaget godkända informationssystem eller signalskyddssystem. Se bilaga 4 i denna anvisning samt Göteborgs Stads anvisning för signalskydd (tillika signalskyddsinstruktion).

2.11 Delgivning

Muntlig delgivning samt delgivning genom visning av säkerhetsskyddsklassificerade uppgifter får endast ske till behörig.

Innan delgivning sker ska den som avser delge säkerhetsskyddsklassificerade uppgifter inhämta information om att mottagaren är behörig att ta del av uppgifter i den aktuella säkerhetsskyddsklassen. Information om behörighet ska begäras från säkerhetsskyddsansvarig vid förvaltning eller säkerhetsskyddschef vid bolag.

Delgivning av säkerhetsskyddsklassificerade uppgifter får endast ske i lokaler eller på platser som är godkända för den säkerhetsskyddsklassen som informationen gäller i enlighet med bilaga 5 i denna anvisning.

2.12 Distribution

Förvaltningar och bolag ska ha styrande dokument som tydliggör hur intern och extern distribution av handlingar och lagringsmedia innehållande säkerhetsskyddsklassificerade uppgifter får ske.

Med intern distribution avses distribution inom förvaltningar och bolag samt mellan förvaltningar och bolag.

Med extern distribution avses distribution mellan staden och externa parter.

2.13 Medförande utanför stadens lokaler

En säkerhetsskyddsklassificerad handling eller lagringsmedia innehållande säkerhetsskyddsklassificerade uppgifter får endast medföras utanför godkända lokaler då det är nödvändigt för tjänsteutövningen.

Om en säkerhetsskyddsklassificerad handling eller lagringsmedia innehållande säkerhetsskyddsklassificerade uppgifter medförs utanför godkända lokaler ska den vara under ständig uppsikt eller förvaras i ett av staden godkänt förvaringsutrymme.

Innan en säkerhetsskyddsklassificerad handling eller lagringsmedia innehållande säkerhetsskyddsklassificerade uppgifter medförs utanför godkända lokaler ska skriftligt beslut fattas av säkerhetsskyddschef eller säkerhetsskyddsansvarig. Beslutet ska avse specifika uppgifter för ett visst ändamål och vara tidsbegränsat.

2.14 Lagringsmedia

2.14.1 Användning av lagringsmedia

Digitala säkerhetsskyddsklassificerade uppgifter och handlingar ska hanteras på för dessa godkända lagringsmedia (exempelvis USB-minnen, hårddiskar, CD, osv). För godkänd utrustning, se bilaga 4 i denna tillämpningsanvisning. Om digitala uppgifter behöver överlämnas mellan förvaltningar och/eller bolag ska i första hand CD användas. Alternativt kan en utsedd transport-USB upprättas mellan två förvaltningar och/eller bolag. Denna USB får då inte användas i något annat syfte än överföring av digitala säkerhetsskyddsklassificerade uppgifter mellan fristående system och mellan dessa förvaltningar. Detta för att undvika exempelvis manipulation av lagringsmedia och därmed av det fristående informationssystemet. Lämpliga åtgärder ska vidtas för att skydda informationen vid överlämning av information.

2.14.2 Återanvändning av lagringsmedia

Ett lagringsmedium som innehåller, eller har innehållit, säkerhetsskyddsklassificerade uppgifter får inte återanvändas.

2.15 Återlämning av säkerhetsskyddsklassificerade handlingar och lagringsmedia

Samtliga säkerhetsskyddsklassificerade handlingar och lagringsmedia ska återlämnas till säkerhetsskyddsregistraturen så snart innehavaren inte längre har behov av dem i tjänsten eller senast när anställning eller annat deltagande i den säkerhetskänsliga verksamheten avslutas.

2.16 Destruktion

Samtliga säkerhetsskyddsklassificerade handlingar och lagringsmedia som innehåller eller har innehållit säkerhetsskyddsklassificerade uppgifter och som inte längre behövs i stadens verksamhet ska destrueras av säkerhetsskyddsregistratur.

Destruering ska ske genom av staden godkänd destrueringsmetod.

Destruering av säkerhetsskyddsklassificerade handlingar samt lagringsmedia i säkerhetsskyddsklassen 3. Konfidentiell och 2. Hemlig ska dokumenteras. Av dokumentationen ska framgå vad som destruerats, när destrueringen genomfördes och vem som genomförde destrueringen.