Bilaga 4: Informationssystem

Innehåll

1 Inledning

Med informationssystem avses ett system av sammansatt mjuk- och hårdvara som behandlar information[1], hädanefter benämns dessa enbart informationssystem.

Denna bilaga förtydligar krav och ansvar för informationssystem som är avsedda att behandla säkerhetsskyddsklassificerade uppgifter eller uppgifter av betydelse för säkerhetskänslig verksamhet i Göteborgs Stads förvaltningar och bolag.

För berörda bolag gäller enbart kapitel 1. Inledning och kapitel 2. Generella krav i denna bilaga. För berörda förvaltningar gäller bilagan i sin helhet.

Med förvaltningsgemensamt informationssystem avses system som används av två eller fler förvaltningar inom samma driftgodkännande.

Med förvaltningsspecifikt informationssystem avses system som endast används av och är driftgodkänt för en förvaltning.

2 Generella krav

Kraven i detta avsnitt är generella och gäller för samtliga typer av informationssystem, inklusive signalskyddssystem som också är informationssystem.

I Göteborgs Stad förekommer tre typer av informationssystem:

- Informationssystem avsedda för behandling av säkerhetsskyddsklassificerade uppgifter.
- Informationssystem av betydelse för säkerhetskänslig verksamhet, dvs. informationssystem som är kritiska för att kunna bedriva säkerhetskänslig verksamhet.
- Signalskyddssystem av sådan typ att de även anses vara informationssystem enligt 1 kap. 3 § Säkerhetsskyddsförordningen (2021:955).

Ett informationssystem utgör i sig ett eget skyddsvärde och ska tas upp i den förvaltnings-/bolagsspecifika säkerhetskyddsanalysen.

Berörda förvaltningar och bolag ska löpande identifiera behov av informationssystem och signalskyddssystem i den säkerhetskänsliga verksamheten. Behov ska förankras och dokumenteras i verksamhetens säkerhetsskyddsanalys.

Förvaltningar ska informera Göteborgs Stads säkerhetskyddschef i samband med att process för driftsättningsbeslut av ett förvaltningsspecifikt säkerhetskänsligt informationssystem påbörjas.

2.1 Beslut om driftgodkännande

För förvaltningsgemensamma informationssystem fattar Göteborgs Stads säkerhetsskyddschef beslut om driftgodkännande. För förvaltningsspecifika

[1] 1 kap. 3 § Säkerhetsskyddsförordning (2021:955)

informationssystem fattar säkerhetsskyddsansvarig i respektive förvaltning beslut om driftgodkännande.

I bolag fattar bolagets säkerhetsskyddchef, eller den som hen delegerar till, beslut om driftgodkännande för informationssystem.

Beslut om driftgodkännande ska dokumenteras.

2.2 Samråd med Säkerhetspolisen

Innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen 3. konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren skriftligen samråda med Säkerhetspolisen. Samrådsskyldigheten gäller även i fråga om andra informationssystem än sådana som anges i första stycket, om obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig.

För förvaltningsgemensamma informationssystem ansvarar Göteborgs Stads säkerhetsskyddschef för att samråd genomförs med Säkerhetspolisen. För förvaltningsspecifika informationssystem ansvarar säkerhetsskyddsansvarig i respektive förvaltning för att samråd genomförs med Säkerhetspolisen.

I bolag ansvarar bolagets säkerhetsskyddschef, eller den som hen delegerar till, för att samråd genomförs med Säkerhetspolisen.

3 Särskild säkerhetsskyddsbedömning

Inför driftsättning av ett informationssystem ska en särskild säkerhetsskyddsbedömning genomföras. Utöver det som framgår av Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1) och denna anvisnings bilaga 1, ska den särskilda säkerhetskyddsbedömningen även innehålla beskrivningar av minst följande områden:

- Tilltänkt användningsområde och vilken verksamhet som ska nyttja informationssystemet
- Skyddsvärden
  - Informationssystemets säkerhetsskyddsklassificering alternativt signalskyddsgrad
  - Informationssystemets konsekvensnivå vid bristande tillgänglighet/riktighet
- Dimensionerande hotbild för informationssystemet
- Informationssystemets sårbarheter
  - Teknikval och arkitektur
  - Informationssystemets exponering mot andra informationssystem
  - Rådighet över informationssystemet (Utveckling, förvaltning och drift)
- Gällande säkerhetskrav för informationssystemet (Författningsreglerade krav samt egna krav)
- Säkerhetsskyddsåtgärder

- Systemdokumentation
- Resultat av genomförda tester av skyddsåtgärder (Tekniska och administrativa)

4 Informationssystem

Vad som anges i detta avsnitt gäller för samtliga typer av informationssystem, exklusive signalskyddssystem. Signalskyddssystem regleras istället, utöver vad som angivits i avsnitten ovan, av Försvarsmaktens föreskrifter samt verksamhetens signalskyddsinstruktion.

4.1 Styrande och stödjande dokument

Det ska finnas nödvändiga och tillräckliga styrande och stödjande dokument för varje informationssystem.

Sådana styrande och stödjande dokument ska utgå från de säkerhetskrav och de säkerhetskyddsåtgärder som framkommit i den särskilda säkerhetsskyddsbedömningen.

Styrande och stödjande dokument bör normalt minst omfatta följande områden:

- Organisation för förvaltning av informationssystemet
- Användning av informationssystemet
- Administration och logghantering
- Import och export av information till informationssystemet
- Godkänd utrustning och dess hantering
- Autentisering och tilldelning av behörigheter
- Hantering av avvikelser, fel och säkerhetshotande händelser

4.2 Organisation

Det ska finnas en utpekad systemägare samt en systemförvaltare för varje informationssystem. För systemförvaltare ska det även finnas en utpekad ersättare. Denne kan vid behov utgöras av personal utanför den egna verksamheten. Systemägare ansvarar för att utse systemförvaltare samt ersättare.

Systemägaren har ett överordnat ansvar för att administration, drift och säkerhet i informationssystem upprätthålls. Systemägaren ska tillse att det för varje informationssystem finns en resurssatt och utbildad organisation samt fastställda styrande dokument och i övrigt ta principiella beslut som rör informationssystemet.

Systemförvaltare ansvarar för löpande drift av informationssystem bland annat genom att ta fram styrande dokument, genomföra utbildning samt bereda och genomföra ändringar av systemet.

I övrigt ska de roller finnas som krävs för att förvalta systemet och upprätthålla säkerhetsskyddet.

4.2.1 Rollfördelning i Göteborgs Stad

- För förvaltningsgemensamma informationssystem är Göteborgs Stads säkerhetsskyddschef, eller den hen delegerar till, systemägare.
- För förvaltningsspecifika informationssystem är säkerhetsskyddsansvarig i respektive förvaltning, eller den hen delegerar till, systemägare.

4.3 Åtkomst och behörigheter

Säkerhetsskyddsansvarig vid förvaltning eller den som denne delegerar till, beslutar om tilldelning av behörigheter avseende åtkomst till informationssystem. Åtkomst och behörighet till informationssystem ska ges restriktivt utifrån ett uttryckligt behov kopplat till individens arbetsuppgifter.

Åtkomst till informationssystem får endast ges personal som genomgått godkänd säkerhetsprövning och vid behov inplacerats i säkerhetsklass i enlighet med det aktuella informationssystemets krav. Personalen ska även ha genomgått systemspecifik utbildning innan åtkomst till informationssystemet ges.

Innan åtkomst till informationssystem ges till personal utanför den egna verksamheten ska en säkerhetsskyddsöverenskommelse, alternativt ett säkerhetsskyddsavtal, tecknas.

För varje driftsatt informationssystem ska det finnas en uppdaterad förteckning över tilldelade behörigheter till informationssystemet.

Behörigheter som ger åtkomst till informationssystem ska bygga på personliga användaridentiteter och vara spårbara till en fysisk person.

Behörigheter som inte går att koppla till en specifik användare ska användas synnerligen restriktivt och godkännas av säkerhetsskyddschef. Beslutet ska motiveras och dokumenteras.

Behörigheter ska vara tidsbegränsade, följas upp och omprövas löpande, minst årligen. Vid byte eller förändring av tjänst ska behörigheter och åtkomst till informationssystem alltid och skyndsamt ses över.

4.4 Godkänd utrustning

Endast godkänd utrustning får anslutas till informationssystem och användas inom den säkerhetskänsliga verksamheten och/eller för behandling av säkerhetsskyddsklassificerade uppgifter. Vilken utrustning som ingår i respektive informationssystem ska framgå av en förteckning.

Utrustning som inte ingår i respektive systems driftgodkännande får ej anslutas till informationssystemet.

All i informationssystemet ingående hårdvara ska alltid märkas med vilken säkerhetsskyddsklass den är godkänd för. Märkning ska regleras i respektive systems styrande dokument.

4.5 Förändringshantering

Alla förändringar avseende mjukvara eller hårdvara i informationssystem ska godkännas av systemägaren eller den som denne delegerar till, innan ändringen genomförs.

Beslut om godkänd förändring ska beakta om motsvarande säkerhetsnivå bibehålls enligt tidigare driftgodkännande och särskild säkerhetsskyddsbedömning.

Systemägare ansvarar för att bedöma om planerande ändringar är av sådan karaktär att de kräver ett nytt driftgodkännande eller samråd, enligt 3 kap. 2 § säkerhetskyddsförordningen, med Säkerhetspolisen.

4.6 Användning av informationssystem

Informationssystem får endast användas inom ramen för systemets driftgodkännande (användningsområde, behörig personal, lokaler, mm.).

4.6.1 Förvaring och nyttjande

Förvaltningar ska för samtliga driftställen och platser där informationssystem nyttjas, fastställa lokala regler för arbete i informationssystemet samt dess förvaring.

Reglerna ska utgå från informationssystemets särskilda säkerhetskyddsbedömning, den förvaltningsspecifika säkerhetskyddsanalysen samt i förekommande fall dimensionerande antagonistisk förmåga (DAF) från Säkerhetspolisen.

Lagringsmedia i informationssystemet som har innehållit eller innehåller säkerhetsklassificerad information ska förvaras på samma sätt som verksamhetens övriga säkerhetsklassificerade handlingar. Övrig utrustning (t.ex. skärmar och dockningsstationer) i informationssystem ska vara under ständig uppsikt eller förvaras så att manipulation förhindras.

4.6.2 Hantering av konton och autentiseringsuppgifter

Personligt tilldelade uppgifter (lösenord) och materiel som utgör del av autentiseringen (aktiva kort eller enhet för multifaktorautentisering) till informationssystem får ej delas med andra eller röjas på något sätt. Utlämnande av sådan uppgift och materiel ska kvitteras och dokumentationen sparas i minst tio år.

Lösenord ska vara unika för varje system och användare. Användare ska byta lösenord vid första tilldelningen när så är tekniskt möjligt.

Lösenordspolicy ska finnas och framgå av varje systems styrande dokument.

Lösenord och koder får endast dokumenteras i form av fysisk anteckning. Sådan fysisk anteckning ska förvaras i ett för säkerhetsskyddsklassificerade handlingar godkänt förvaringsutrymme[2] och får inte vara samma förvaringsutrymme som det aktuella informationssystemet förvaras i.

[2] 5 kap. 10 § PMFS 2022:1

Konton och behörigheter som ger åtkomst till informationssystem ska skyndsamt avaktiveras så snart de inte längre behövs. Avaktiveringen ska genomföras så att kraven på historisk spårbarhet (loggar) bibehålls.

4.6.3 Utlämning och återlämning av utrustning

Utlämnande av utrustning ingående i informationssystem ska kvitteras och dokumentationen sparas i minst tio år.

När användare inte längre har behov av att nyttja informationssystemet, ska all utrustning återlämnas. Återlämningen dokumenteras och dokumentationen sparas i minst tio år.

Med utlämnande avses tiden från det tillfälle som personal tilldelas utrustningen eller till exempel får access till förvaringsutrymme där sådan utrustning förvaras.

4.6.4 Import och export av information

Varje informationssystem ska ha regler för import och export av information. Reglerna ska omhänderta både risken för skadlig kod såväl som verksamhetens krav på informationssäkerhet.

4.6.5 Säkerhetskopiering

Säkerhetskopiering och testning av säkerhetskopiorna för att återskapa information ska utföras regelbundet, minst en gång per år.

Krav på tidsintervall mellan säkerhetskopieringar ska regleras i de systemspecifika styrande dokumenten.

4.6.6 Medförande

Medförande av utrustning ett informationssystem utanför verksamhetens lokaler får endast ske efter godkännande av säkerhetskyddschef eller den som denne delegerar till.

Utrustning som medförs utanför verksamhetens lokaler ska vara under ständig uppsikt eller förvaras i av verksamheten godkänt förvaringsutrymme.

4.6.7 Avslutande av behörigheter

Behörigheter ska avslutas så fort som en användare inte längre har behov av att nyttja informationssystem eller av annan anledning inte längre ska ha åtkomst till dessa.

Beslut om avslutande av behörighet ska tas av samma roll som beslutade om tilldelning av behörigheten.

Uppgifter om vilka behörigheter som avslutats och när ska framgå i förteckning som sparas i tio år.

4.7 Avveckling och förstöring

4.7.1 Avveckling av informationssystem

Avveckling av informationssystem ska ske på ett sådant sätt att säkerhetsskyddet upprätthålls under avvecklingsprocessen.

Planeringen inför en avveckling ska dokumenteras i en avvecklingsplan. Planen ska tas fram innan avveckling påbörjas och utgör en del i avvecklingsbeslutet.

Göteborgs Stads säkerhetsskyddschef beslutar om avveckling av förvaltningsgemensamma informationssystem.

För förvaltningsspecifika informationssystem fattar säkerhetsskyddsansvariga beslut om avveckling.

4.7.2 Återanvändning

Lagringsmedia som innehållit information på högst nivån begränsat hemlig (BH) får återbrukas om följande förutsättningar uppfylls:

- Godkänd mjukvara för överskrivning används. Beslut om godkänd mjukvara tas av säkerhetskyddsansvarig i förvaltning eller den som denne delegerar till.
- Lagringsmediet får endast återbrukas inom förvaltningens egna säkerhetsskyddsorganisation.
- Lagringsmediet hanteras och förstörs som om det innehåller säkerhetsklassificerad information.

4.7.3 Förstöring

Elektroniska datamedia t. ex. USB-minnen, aktiva kort, SSD hårddiskar, CD/DVD som innehåller eller har innehållit säkerhetsskyddsklassificerade uppgifter ska förstöras så att informationen på dem inte går att återskapa.

Datamedia som innehåller eller har innehållit säkerhetsskyddsklassificerade uppgifter ska alltid förstöras genom mekanisk destruktion vid beslut om end-of-life.

Övrig hårdvara, exempelvis arbetsminnen (RAM), från informationssystem som i någon grad vid något tillfälle kan ha lagrat säkerhetsklassificerade uppgifter ska behandlas som om de har innehållit säkerhetsklassificerade uppgifter avseende krav på förstöring.

Säkerhetsskyddsöverenskommelse eller avtal ska ingås om destruktörstjänster anlitas genom samverkan med förvaltning eller annan aktör.

Vid mekanisk destruktion ska den använda destruktionsmetoden uppfylla kraven enligt standarden DIN 66399	
Lagringsmedia	**Destruktionskrav**
Optiska lagringsmedier, t. ex CD och DVD (O)	Ska förstöras enligt lägst destruktionsklass O-6.

Mekaniska hårddiskar (H)	Ska förstöras enligt lägst destruktionsklass H-5. Destruktion ska föregås av avmagnetisering med degausser, med minst ”Single Pass Pulse”
Elektroniska datamedia (E) t. ex. USB-minnen, kort, SSD, mobiltelefoner, läsplattor	Ska förstöras minst enligt lägst destruktionsklass E-5.