Riktlinje för säkerhet

Diarienummer	Senast uppdaterad	Beslutsinstans	Ansvarig processägare
KS 2019/0057	2019-11-25	KS	Säkerhetschef

Dokumentets syfte

Syftet med riktlinjen är att på ett samlat och enhetligt sätt reglera samtliga krav på kommunens säkerhetsarbete och tillhandahålla ett tydligt och fastställt underlag för framtagande av enkla, och konkreta anvisningar och rutiner som stödjer medarbetare och leverantörer i det dagliga arbetet med säkerhet.

Dokumentet gäller för

Dokumentet gäller för hela kommunens verksamhet.

Innehållsförteckning

1. Inledning

Detta dokument utgör kommunens riktlinje för säkerhet. Riktlinjen följer beslutade policys som beskriver kommunens övergripande målsättningar för säkerhetsarbetet.

Med säkerhetsarbete avses det systematiska, förebyggande arbete som kommunen bedriver för att minimera risken för negativa händelser och begränsa skadan av inträffade negativa händelser inom den kommunala verksamheten.

Kommunens säkerhetsarbete syftar till att säkerställa kommunens förmåga att bedriva den verksamhet som regleras i kommunallagen genom att skydda de tillgångar i form av personer, förtroende, information och egendom samt ekonomiska och kulturhistoriska värden som kommunen ansvarar för och är beroende av.

Riktlinjen ingår i den struktur av styrande och stödjande dokument som reglerar kommunens säkerhetsarbete. Riktlinjen reglerar VAD som ska åstadkommas, till vilken nivå i relevanta fall och i viss mån, på en övergripande nivå, HUR detta ska åstadkommas.

Utöver policys och riktlinjer förekommer även analyser och planer som beskriver säkerhetsläget och planerade åtgärder samt anvisningar och rutiner som i detalj beskriver hur arbetet med att upprätthålla en ändamålsenlig säkerhet för kommunens verksamhet ska bedrivas.

Samtliga styrande dokument som reglerar kommunens säkerhetsarbete är framtagna för att stödja kommunens uppdrag och övergripande verksamhetsmål. I slutändan är syftet med kommunens säkerhetsarbete att skydda verksamheten så att kommunen kan uppfylla sina åtaganden mot medborgarna och övriga delar av samhället i olika nivåer av beredskap.

1.1. Riktlinjens uppbyggnad och innehåll

En målsättning för riktlinjen har varit att samla samtliga krav som reglerar kommunens säkerhetsarbete på ett ställe i syfte att förtydliga kraven för medarbetare och leverantörer samt underlätta löpande revidering.

Riktlinjens uppbyggnad har även anpassats så att de överensstämmer med kommunens riktlinjer för beredskap vad gäller övergripande struktur i syfte att åstadkomma igenkänning och därmed underlätta för användarna.

Riktlinjen för säkerhet inkluderar krav inom ett stort antal områden såsom exempelvis säkerhetsskydd, informationssäkerhet, fysisk säkerhet och personsäkerhet samt säkerhet vid upphandling och rekrytering. Även säkerhetsrelaterade krav som följer av den europeiska dataskydds-förordningen (GDPR/DSF) har inarbetats i riktlinjen.

Riktlinjen fokuserar på att beskriva de konkreta krav på säkerhetsåtgärder som gäller inom kommunens verksamhet och pedagogiska beskrivningar av de principer som styr säkerhetsarbetet har begränsats till korta inledande texter för varje delområde. För mer generell information om säkerhetsarbete rekommenderas kommunens anvisningar, rutiner och säkerhetsutbildningar (se Säkerhetsutbildning och informationsinsatser nedan).

2. Styrande regelverk

2.1. Författningskrav på kommunens säkerhetsarbete

Det finns en mängd författningskrav i lagar, förordningar och föreskrifter som reglerar kommunens säkerhetsarbete. Förutom krav som innebär att kommunen ska vidta säkerhetsåtgärder så förekommer krav som säkerställer att kommunen inte vidtar alltför långtgående säkerhetsåtgärder (det senare gäller exempelvis krav på allmänna handlingars offentlighet som begränsar kommunens möjligheter att skydda information från åtkomst).

Författningskraven kommer dels från EU-rätten och dels från svenska grundlagar, lagar och förordningar samt föreskrifter som myndigheter meddelar med stöd av lag eller förordning.

I tabellen nedan sammanställs ett urval av de författningar som bedöms ha störst påverkan på kommunens säkerhetsarbete. Antingen på grund av att de innebär direkta krav på kommunens säkerhetsarbete (exempelvis säkerhetsskyddslagstiftningen eller dataskyddsförordningen) och dels författning som begränsar kommunen att vidta för långtgående säkerhetsåtgärder (exempelvis tryckfrihetsförordningen eller lagen om offentlig upphandling).

Typ	**Benämning**	**Förkortas**	**Beteckning**
EU-rätt	General Data Protection Regulation/Dataskyddsförordningen	GDPR/DSF	2016/679
EU-rätt	Network and Information Security directive	NIS	2016/1148
Grundlag	Tryckfrihetsförordningen	TF	1949:105
Grundlag	Yttrandefrihetsgrundlagen	YGL	1991:1469
Lag	Brottsbalk	BrB	1962:700
Lag	Offentlighets- och sekretesslag	OSL	2009:400
Förordning	Offentlighets- och sekretessförordning	OSF	2009:641
Lag	Säkerhetsskyddslag		2018:585
Förordning	Säkerhetsskyddsförordning		1996:633
Lag	Lag om informationssäkerhet för samhällsviktiga och digitala tjänster		2018:1174
Förordning	Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster		2018:1175
Lag	Lag med kompletterande bestämmelser till EU:s dataskyddsförordning		2018:218
Lag	Skyddslag		2010:305
Förordning	Skyddsförordning		2010:523
Lag	Kamerabevakningslag		2018:1200
Lag	Lag om skydd för geografisk information		2016:319

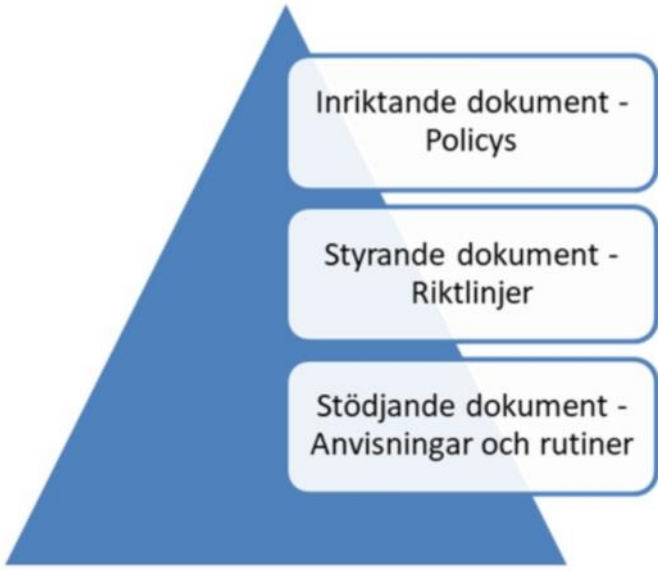
Typ	Benämning	Förkortas	Beteckning
Förordning	Förordning om skydd för geografisk information		2016:320
Lag	Lag om totalförsvar och höjd beredskap		1992:1403
Lag	Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap	LEH	2006:544
Förordning	Förordning om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap		2006:637
Lag	Lag om offentlig upphandling	LOU	2007:1091
Lag	Lag om upphandling på försvars- och säkerhetsområdet	LUFS	2011:1029
Lag	Lag om offentlig anställning[1]	LOA	1994:260
Föreskrift[2]	Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd		PMFS 2015:3
Föreskrift	Myndigheten för samhällsskydd och beredskaps föreskrifter om kommuners risk- och sårbarhetsanalyser		MSBFS 2015:5
Föreskrift	Myndigheten för samhällsskydd och beredskaps föreskrifter om civila myndigheters kryptoberedskap		MSBFS 2009:11

2.2. Inriktande, styrande och stödjande dokument avseende säkerhet

Kommunfullmäktige inriktar kommunens systematiska säkerhetsarbete genom att fastställa policys inom olika områden som de förtroendevalda bedömer vara särskilt viktiga att lyfta fram. Som exempel kan nämnas kommunens policy avseende informationssäkerhet och dataskydd som fastställdes under 2018.

De konkreta kraven på säkerhet inom kommunens verksamhet regleras i riktlinjen för säkerhet och utöver dessa, förekommer även ett antal anvisningar och rutiner som syftar till att stödja verksamhetens säkerhetsarbete genom att tydliggöra hur riktlinjen ska tillämpas. Se bild nedan.

[1] I tillämpliga delar
[2] Myndighetsföreskrift som utfärdats med stöd i lag eller förordning



En sammanställning av inriktande, styrande och stödjande dokument inom kommunens säkerhetsarbete presenteras på intranätet.

2.3. Revidering av inriktande, styrande och stödjande dokument för kommunens säkerhetsarbete

Nedan sammanställs kraven på intervall för regelbunden revidering av inriktande, styrande och stödjande dokument som reglerar kommunens säkerhetsarbete.

Dokumenttyp	Ansvarig	Beslutas av	Intervall
Policy - Inriktande dokument	Säkerhetschef	Kommun-fullmäktige	1 gång per mandatperiod
Riktlinje - Styrande dokument	Säkerhetschef	Kommun-styrelsen	1–2 gånger per mandatperiod
Kommunövergripande anvisningar och rutiner – Stödjande dokument	Säkerhetschef	Kommun-direktör	Vid behov
Lokala rutiner	Kontaktombud	Ansvarig chef	Vid behov

3. Kommunens behov av säkerhet

Säkerheten syftar till att skydda kommunens verksamhet och ytterst till att skydda den samhällsviktiga och säkerhetskänsliga verksamhet som är kritisk för medborgare och organisationer samt, i förlängningen, för Sverige. Kommunens behov av säkerhet styrs bara delvis av föreliggande författnings-krav.

Även de krav som föreligger på kommunens säkerhetsarbete (exempelvis inom ramen för säkerhetsskyddslagstiftningen) baseras på att kommunen ska ha det skydd som krävs utifrån den egna verksamheten.

Därför är det viktigt att poängtera att kommunens säkerhetsarbete ska dimensioneras utifrån de skyddsvärda tillgångar som kommunen är beroende av för att kunna bedriva sin verksamhet samt föreliggande hotbild mot dessa skyddsvärda tillgångar. I slutändan är det konsekvenserna för verksamheten

om, en skyddsvärd tillgång görs otillgänglig för verksamheten, som styr vilka säkerhetsåtgärder som ska vidtas.[3]

3.1. Kommunens skyddsvärda tillgångar

De skyddsvärda tillgångar som finns i kommunens verksamhet definieras nedan.

3.1.1. Personer

De personer i form av medarbetare, förtroendevalda, leverantörer, besökare m.fl. som på något sätt deltar i kommunens verksamhet utgör en skyddsvärd tillgång och den kunskap och erfarenhet som dessa personer besitter är avgörande för att kommunens verksamhet ska kunna fortgå.

3.1.2. Förtroende

Att upprätthålla förtroendet för kommunens verksamhet är en skyddsvärd tillgång då mycket av kommunens verksamhet är beroende av ett förtroende från medborgare, förtroendevalda, andra myndigheter med flera för att kunna fortgå. Detta gäller särskilt då kommunen är beroende av ett stort antal samarbeten med andra aktörer för at kunna upprätthålla olika samhällsviktiga funktioner.

3.1.3. Information

Den information som förekommer inom kommunens verksamhet (i IT-system, på papper och hos personer) utgör en skyddsvärd tillgång. Kommunens verksamhet är i mycket hög grad beroende av tillgång till information. Att informationen är korrekt och tillgänglig när den behövs, samtidigt som den skyddas mot obehörig åtkomst, är avgörande för kommunens verksamhet. Felaktig hantering av information skulle kunna skada såväl kommunen som enskilda individer och organisationer och kunna leda till att förtroendet för kommunen skadas allvarligt.

3.1.4. Egendom och utrustning

Kommunens egendom och utrustning i form av exempelvis fastigheter, fordon och teknisk infrastruktur samt IT-utrustning utgör en skyddsvärd tillgång. Tillgång till egendom och utrustning kan dels vara avgörande för att bedriva verksamhet till vardags och dels för att förebygga eller hantera inträffade krissituationer.

3.1.5. Ekonomiska och kulturhistoriska värden

Kommunen ansvarar även för en mängd skyddsvärden som inte är av operativ betydelse för verksamheten, men som utgör betydande ekonomiska eller kulturhistoriska värden. Det gäller exempelvis konst och kulturhistoriskt viktiga dokument i arkiv m.m. men även de tilldelade ekonomiska medel som kommunen förfogar över. Även dessa ekonomiska och kulturhistoriska värden utgör skyddsvärda tillgångar för kommunen.

[3] Konsekvensstyrt säkerhetsarbete. När en konsekvens inte kan accepteras ska säkerhetsåtgärder sättas in för att begränsa konsekvenserna eller sannolikheten för att den oönskade händelsen ska inträffa.

4. Kommunens förutsättningar att bedriva säkerhetsarbete

Säkerhetsarbetet inom kommunen ska säkerställa att kommunen uppfyller gällande författningskrav och i övrigt stödja de övergripande verksamhetsmålen.

Arbetet ska bedrivas kostnadseffektivt och säkerhetsrelaterade frågor ska så långt som möjligt, hanteras i linjeorganisationen och inarbetas i ordinarie huvudprocesser, riktlinjer och rutiner.

Säkerhetsarbetet inom Danderyds kommun ska bedrivas i nära samarbete med övriga närliggande kommuner och så långt som möjligt, samordnas inom ramen för samverkansorganisationer för att uppnå synergieffekter.

5. Organisation av kommunens säkerhetsarbete

Kommunens säkerhetsarbete inriktas på en övergripande policy- och riktlinjenivå av kommunfullmäktige. Kommunstyrelsen säkerställer budgeten för säkerhetsarbetet. Kommundirektören är under kommunstyrelsen, med stöd av ledningsgruppen, ytterst ansvarig på tjänstemannanivå~~Kommundirektören är, med stöd av ledningsgruppen, ytterst ansvarig~~ för säkerheten i kommunen och kommunens säkerhetsarbete. Kommunens säkerhetschef leder och följer upp kommunens säkerhets- och beredskapsarbete.

Säkerhetschefen är tillika kommunens säkerhetsskyddschef[4] och är direkt underställd kommundirektören i säkerhetsskyddsfrågor. För övriga roller se anvisning säkerhet.

6. Handlingssekretess och tystnadsplikt

Den som är anställd i kommunen eller på annat sätt bedriver kommunens verksamhet (exempelvis i egenskap av anställd hos leverantör till kommunen) omfattas av förbudet mot att röja uppgifter som omfattas av sekretess, som framgår av offentlighets- och sekretesslagen

Sekretessen gäller mot enskilda (personer och företag) och andra myndigheter[5] (om det inte föreligger undantag i lagen). Sekretessen gäller även mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra. Sekretessen gäller även på motsvarande sätt mot utländska myndigheter och mellanfolkliga (internationella) organisationer.

Tystnadsplikt innebär att en person inte har rätt att delge uppgifter som omfattas av sekretess till obehöriga. Tystnadsplikten innebär begränsningar i yttrandefriheten enligt regeringsformen samt, i vissa särskilt angivna fall, även begränsningar i rätten att meddela och offentliggöra uppgifter som följer

[4] Säkerhetsskyddschef utgör den befattning som har ansvar enligt säkerhetsskyddslag och som bedriver tillsyn i dessa frågor. Säkerhetsskyddslagen omhändertar frågor som rör Sveriges säkerhet och säkerhetskänslig verksamhet.
[5] Observera att Danderyds kommun består av flera separata myndigheter.

av tryckfrihetsförordningen och yttrandefrihetsgrundlagen (den så kallade meddelarfriheten). Bestämmelser om tystnadsplikt regleras i Offentlighets- och sekretesslag.

Handlingssekretess innebär att en person inte har rätt att lämna ut handlingar som innehåller uppgifter som omfattas av sekretess till obehöriga[6]. Handlingssekretessen innebär begränsningar i den rätt att ta del av allmänna handlingar som följer av tryckfrihetsförordningen.

Av offentlighets- och sekretesslagen framgår även att i de fall då det råder förbud mot att röja en uppgift, så får uppgiften inte heller i övrigt utnyttjas utanför den verksamhet för vilken den är sekretessreglerad.

6.1. Sekretessförbindelse

Samtliga personer som bedriver kommunens verksamhet ska informeras om tystnadsplikten och handlingssekretessen och teckna en sekretessförbindelse som tydligt visar att de har delgivits informationen. Sekretessförbindelsen för anställda i Danderyds kommun sparas i personalakten hos respektive förvaltning. Tecknande av sekretessförbindelse ska ske innan en person ges behörighet att ta del av uppgifter som omfattas av sekretess (informationssäkerhetsklass INTERN eller högre).

7. Informationsklassning

Samtliga informationstillgångar som hanteras inom kommunens verksamhet ska klassas utifrån behov av konfidentialitet, riktighet och tillgänglighet för informationen enligt de klasser som beskrivs nedan.

Klassningen ska ske under informationens hela livscykel. Ofta klassas den om, exempelvis från INTERN under arbete till ÖPPEN vid publicering.

7.1. Konfidentialitet

Med konfidentialitet avses informationens behov av skydd mot obehörig åtkomst. Till skillnad från riktighet, tillgänglighet och spårbarhet, som huvudsakligen hanteras genom inbyggda funktioner i kommunens IT-miljö, så är konfidentialitet en angelägenhet för alla som kommer i kontakt med kommunens informationstillgångar. Varje medarbetare, leverantör och övriga som hanterar kommunens skyddsvärda informationstillgångar måste beakta behovet av konfidentialitet i det dagliga arbetet, exempelvis då man avgör huruvida en viss informationsmängd får skickas med e-post.

- Informationssäkerhetsklass ÖPPEN

  Med ÖPPEN information avses uppgifter som inte omfattas av några krav på konfidentialitet och därför inte behöver skyddas från obehörig insyn. Uppgifterna kan dock fortfarande vara av stor betydelse för kommunen och omfattas av krav på riktighet och tillgänglighet.

- Informationssäkerhetsklass INTERN

[6] Observera att meddelarfriheten inte omfattar utlämnande av handlingar, utan endast meddelande av uppgifter.

Med INTERN information avses uppgifter som behöver ges ett grundläggande skydd mot obehörig åtkomst. All information som förekommer i kommunens IT-miljö och som inte är ÖPPEN eller KÄNSLIG eller högre är att betrakta som INTERN. Hit räknas uppgifter som omfattas av svag sekretess (rakt skaderekvisit: huvudregel offentlighet). Hit räknas även personuppgifter som i normalfallet inte är att betrakta som känsliga[7].

- Informationssäkerhetsklass KÄNSLIG

  Med KÄNSLIG information avses uppgifter som behöver ges ett särskilt skydd då obehörig åtkomst till uppgifterna kan innebära allvarliga konsekvenser för kommunen eller enskilda. Hit räknas uppgifter som omfattas av stark sekretess (omvänt skaderekvisit: huvudregel sekretess) eller absolut sekretess och uppgifter som bedöms vara av särskilt intresse för obehöriga. Hit räknas även personuppgifter som i normalfallet är att betrakta som känsliga[7].

- Informationssäkerhetsklass BEGRÄNSAT HEMLIG[8]

  Med begränsat hemlig information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400 kap 15) kan medföra ringa skada för Sveriges säkerhet.

- Informationssäkerhetsklass KONFIDENTIELL[8]

  Med konfidentiell information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen. Ett röjande kan medföra en inte obetydlig skada för Sveriges säkerhet.

- Informationssäkerhetsklass HEMLIG[8]

  Med hemlig information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen. Ett röjande av informationen kan medföra en allvarlig skada för Sveriges säkerhet.

- Informationssäkerhetsklass KVALIFICERAT HEMLIG[8]

  Med kvalificerat hemlig information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen. Ett röjande kan medföra en synnerligen allvarlig skada för Sveriges säkerhet.

7.2. Riktighet

Informationens riktighet är avgörande för såväl kommunens verksamhet som allmänheten och medias förtroende för kommunen. Riktigheten säkerställs främst genom en strikt tillämpning av behörighet att påverka informations-

[7] Observera att bedömning av huruvida en personuppgift är känslig alltid måste ske från fall till fall. En uppgift som i normalfallet inte är känslig, såsom en gatuadress, kan exempelvis vara känslig om den avser bostadsadress för en person med skyddad identitet.
[8] Regleras i säkerhetsskyddslagstiftningen

mängder i kommunens IT-miljö[9] och åtgärder för att säkerställa spårbarhet (och därmed möjlighet att utkräva ansvar) då åtgärder vidtas i IT-miljön (se även rubriken Spårbarhet nedan).

7.3. Tillgänglighet

Krav på informationens tillgänglighet utgår ifrån vilka konsekvenser det kan innebära för verksamheten om en viss informationsmängd är otillgänglig för behöriga användare. Konsekvensernas omfattning, gällande lagstiftning och hur tidskritisk informationen är för verksamheten är avgörande för vilka åtgärder som måste vidtas för att säkerställa tillgängligheten.

Tillgänglighet till den information som hanteras inom kommunens verksamhet hanteras främst genom åtgärder som vidtas för att garantera viss tillgänglighet till information i kommunens IT-miljö. Det är dock inte möjligt att garantera absolut tillgänglighet varför det finns anledning att implementera reservrutiner för att säkerställa att den mest verksamhets-kritiska informationen hålls tillgänglig även om IT-miljön är otillgänglig (exempelvis genom att tillhandahålla utskrifter av viss information).

Ett SLA (Service Level Agreement) som reglerar tillgänglighetskrav ska tecknas för varje nytt system, oavsett om det förvaltas och driftas internt, eller av en leverantör. Vid tecknande av ett SLA ska särskilt fokus läggas vid krav på säkerhetskopiering och återställande av säkerhetskopior.

För att underlätta kravställning och uppföljning av tillgänglighet så indelas IT-system och molntjänster i följande klasser[10]:

- Begränsad tillgänglighet

  System och tjänster som inte är verksamhetskritiska. Åtgärder för att avhjälpa avbrott ska vidtas inom två arbetsdagar.

- Hög tillgänglighet

  System och tjänster som är verksamhetskritiska för verksamhet som bedrivs dagtid på vardagar. Exempelvis ärende- och arkivsystem samt ekonomi- och personalsystem m.m. Åtgärder för att avhjälpa avbrott ska vidtas inom 4 timmar då fel inträffar mellan 08:00 och 17:00 på vardagar. Avbrott som inträffar övriga tider ska avhjälpas inom fyra timmar räknat från 08:00 nästkommande vardag.

- Mycket hög tillgänglighet

  System och tjänster som är verksamhetskritiska för verksamhet som måste kunna fortgå under kvällar och helger. Exempelvis system som är kritiska för hemtjänsten, socialtjänsten, överförmyndare eller kommunalteknisk försörjning eller system som är kritiska för kommunens IT-infrastruktur alternativt för intern/extern kommunikation m.m. Åtgärder för att avhjälpa avbrott ska vidtas inom fyra timmar.

[9] Här menas att spårbarhet i ändringar kopplas till unik användare för att på så sätt säkerställa spårbarhet.
[10] Klasserna syftar till att möjliggöra kravställning vid anskaffning av system samt också att skapa möjlighet för uppföljning av systemkrav mm.

7.4. Spårbarhet

Att säkerställa informationens konfidentialitet, riktighet och tillgänglighet i kommunens IT-miljö förutsätter att en ändamålsenlig nivå av spårbarhet upprätthålls. Spårbarhet åstadkoms huvudsakligen genom en strikt behörighetstilldelning i kombination med loggning av aktiviteter och granskning av loggar. Med detta menas att om kontroll finns över vem som tilldelats en behörighet så ger det också möjlighet till spårbarhet kopplat till hantering av informationen. Unika användaridentiteter som går att koppla till en fysisk användare är en förutsättning för att kunna påvisa att informationssäkerheten upprätthålls under informationstillgångens hela livscykel.

- Begränsad spårbarhet

  Kommunens basnivå för loggning av system och tjänster. Åtgärder som vidtas för att uppfylla krav på begränsad spårbarhet beskrivs i kommunens dokumentation av IT-säkerhetsåtgärder.

- Hög spårbarhet

  Särskild loggning och logguppföljning för system och tjänster som med högre krav på konfidentialitet, riktighet och tillgänglighet. Åtgärder som vidtas för att uppfylla krav på hög spårbarhet beskrivs i kommunens dokumentation av IT-säkerhetsåtgärder

8. Säkerhet i kommunens lokaler

Att kommunens lokaler har ändamålsenlig säkerhet är dels viktigt för att skydda kommunens verksamhet från skada, men även för att medarbetare, leverantörer, förtroendevalda, elever, vårdtagare och besökare m.fl. ska kunna känna sig trygga i lokalerna.

8.1. Tillträdesbegränsning

För att säkerställa att endast de som har behov av tillträde till en viss lokal ges tillträde så är kommunens lokaler indelade i tre olika behörighetzoner enligt nedan. En lokal kan bestå av en eller flera behörighetszoner.

8.1.1. Zon 1 – Grön zon

Grön zon avser lokal, eller del av lokal, dit allmänheten har tillträde. Grön zon kan exempelvis utgöras av en reception, eller en samlingslokal som är öppen för allmänheten under vissa tider.

8.1.2. Zon 2 – Gul zon

Gul zon avser lokal, eller del av lokal, dit kommunens personal och leverantörer som tilldelats allmän behörighet ges tillträde (inre zon). Behörighet ges baserat på befattning och tilldelas i samband med att anställning eller uppdrag påbörjas. Besökare som inte givits egen behörighet ska ledsagas av besöksmottagaren under hela besöket och får inte lämnas ensamma i zonen. Gul zon kan exempelvis utgöras av kontorslokaler och konferensrum.

8.1.3. Zon 3 – Röd zon

Röd zon avser lokal, eller del av lokal, dit endast viss personal och vissa leverantörer som tilldelats särskild behörighet ges tillträde (inre zon med särskilda behörighetskrav. Behörighet beslutas av verksamhetsansvarig chef eller den chefen delegerat beslutsrätten till och ska baseras på ett faktiskt behov av tillträde i tjänsten. Tilldelade behörigheter ska vara tidsbegränsade och omprövas årligen[11]. Röd zon kan exempelvis utgöras av datahallar, korskopplingsutrymmen (utrymmen avsedda för teknisk infrastruktur) eller kontorslokaler där särskilt skyddsvärd verksamhet bedrivs.

8.2. ID-kort och behörigheter till lokaler

Samtliga personer som tilldelas egen behörighet till kommunens lokaler ska bära kommunens ID-kort väl synligt då de vistas i kommunens lokaler. Detta gäller såväl egen personal och andra personer som ges tillträde till kommunens lokaler till följd av ett uppdrag eller liknande.

8.3. Säker arbetsplats

Det är viktigt att personal och leverantörer som utför arbete i kommunens lokaler har tillgång till säkra arbetsplatser som är anpassade efter verksamhetens art och de skyddsvärda tillgångar (exempelvis information som hanteras i arbetet).

8.3.1. Möjlighet att hantera skyddsvärda tillgångar

En arbetsplats där information som klassats som INTERN hanteras ska vara insynsskyddad mot Zon 1 – Grön zon och mot externa ytor.

En arbetsplats där information som klassats som KÄNSLIG eller högre hanteras ska vara insynsskyddad så att inte obehöriga personer kan ta del av den information som hanteras.

En arbetsplats där information som klassats som INTERN diskuteras ska vara skyddad mot överhörning från Zon 1 – Grön zon och från externa ytor.

En arbetsplats där information som klassats som KÄNSLIG eller högre hanteras ska vara i skyddad mot överhörning så att inte obehöriga personer kan ta del av den information som diskuteras.

8.3.2. Möjlighet att förvara skyddsvärda tillgångar

Vid en arbetsplats där information som klassats som KÄNSLIG hanteras ska det finnas tillgång till en låst förvaringsenhet där informationen lagras, dit endast behöriga personer har tillträde (exempelvis ett låst skåp).

Vid en arbetsplats där information som klassats som BEGRÄNSAT HEMLIG eller högre hanteras ska det finnas tillgång en förvaringsenhet där informationen lagras. Förvaringsenheten ska vara godkänd enligt normen SSF 3492 och endast behöriga personer får ha tillträde.

[11] Med omprövas menas att beslut om förlängning tas aktivt av behörig chef rörande röd zon.

8.3.3. Distansarbete

Motsvarande krav på säkra arbetsplatser som beskrivs ovan gäller även vid distansarbete.

8.4. Rätt att fotografera, filma eller spela in ljud i kommunens lokaler

Syftet med att reglera vilka regler som gäller avseende fotografering, filmning och ljudinspelning i kommunens lokaler är att skapa en trygg miljö för allmänheten, anställda, leverantörer och förtroendevalda. Tydliga och förutsägbara regler ger möjlighet att sprida information om kommunens verksamhet utan att riskera att information som omfattas av sekretess, eller integritetskänsliga personuppgifter sprids.

Vilka krav som ställs på begränsning av rätten att fotografera, filma eller spela in ljud varierar beroende på i vilken zon verksamheten bedrivs enligt nedan.

Notera att inspelning får ske av enskild i samtal med handläggare. Detta ska beaktas i val av lokal.

- **Fotografering, filmning och ljudupptagning i Zon 1 – Grön zon**
  Fotografering, filmning och ljudupptagning får ske i zon 1 under förutsättning att det inte kränker någons personliga integritet eller riskerar att röja sekretessreglerade uppgifter eller på annat sätt bryter mot svensk lagstiftning. Den som fotograferar, filmar eller spelar in ljud ansvarar för att dataskyddsförordningen efterlevs i hanteringen av materialet.

- **Fotografering, filmning och ljudupptagning Zon 2 – Gul zon**
  Utöver eventuell kamerabevakning som utförs på uppdrag av kommunen bör fotografering, filmning eller ljudupptagning undvikas i zon 2. Fotografering, filmning eller ljudupptagning får ske inom den egna verksamheten (exempelvis fotografering av anteckningar på en whiteboard), men all fotografering, filmning eller ljudupptagning som kan komma att beröra andra verksamheter kräver tillstånd av den chef som är ansvarig för verksamheten som nyttjar lokalerna.

- **Fotografering, filmning och ljudupptagning Zon 3 – Röd zon**
  Utöver eventuell kamerabevakning som utförs på uppdrag av kommunen ska varken fotografering, filmning eller ljudupptagning förekomma i zon 3, förutom då den chef som ansvarar för verksamheten i lokalerna fattat ett skriftligt beslut om tillstånd för sådan verksamhet. Ett tillstånd för fotografering, filmning eller ljudupptagning i zon 3 ska vara tidsbegränsat, begränsat till en viss lokal och ett specifikt ändamål.

8.5. Skyltning av säkerhetskrav och säkerhetsåtgärder i lokaler

För att främja tydlighet och transparens så ska säkerhetskrav som påverkar allmänheten alltid anslås på lämpligt sätt i lokaler dit allmänheten har tillträde. Anslagen ska vara tydliga, informativa och upplevas som stödjande samt följa kommunens grafiska profil.

Det gäller exempelvis krav på som reglerar under vilka förutsättningar allmänheten får vistas i lokalerna samt i vilken omfattning tillträdes-begränsning, överbevakning och loggning sker samt eventuella begränsningar i rätten att fotografera, filma eller spela in ljud.

Information till medarbetare och leverantörer avseende säkerhetskrav ska tillhandahållas där det behövs för att säkerställa att kraven efterlevs (exempelvis i anslutning till en kopiator/multifunktionsskrivare).

8.6. Mekaniskt inbrottsskydd

För varje lokal som kommunen förfogar över ska det finnas ett beslut om vilken nivå av mekaniskt inbrottsskydd som lokalen ska vara försedd med. Nivån av mekaniskt inbrottsskydd beskrivs i någon av de skyddsklasser som framgår av svenska stöldskyddsföreningens norm ”Regler för inbrottsskydd – Byggnader och lokaler” (SSF200) med tillhörande dokumentation över eventuella undantag från normen eller tillägg till normen som kommunen beslutat om.

Tekniska kontoret ansvarar för att upprätthålla dokumentation avseende mekaniskt inbrottsskydd i kommunens lokaler.

8.7. Tekniska säkerhetssystem

Kommunen strävar efter ett säkert och effektivt nyttjande av tekniska säkerhetssystem för att komplettera det mekaniska inbrottsskyddet och upprätthålla ändamålsenlig säkerhet för kommunens fastigheter och lokaler.

De tekniska säkerhetssystem som nyttjas är inbrottslarmanläggningar,

Passerkontrollsystem (inkl. elektromekaniska låssystem) och system för kamerabevakning.

Vilka system som krävs och hur de nyttjas regleras[12] för respektive byggnad/lokal och anpassas efter verksamhetens behov av säkerhet.

Vid kravställning av tekniska säkerhetssystem ska Svenska stöldskydds-föreningens normer användas som referens så långt som möjligt för att säkerställa en långsiktigt hållbar kravställning och leverantörsoberoende.

Tekniska kontoret ansvarar för att upprätthålla dokumentation avseende tekniska säkerhetssystem i kommunens lokaler.

8.8. Ronderande bevakning

Kommunen använder sig av ronderande bevakning som ett komplement till tekniska säkerhetsåtgärder. För varje fastighet/lokal ska finnas ett beslut om huruvida ronderande bevakning krävs, och i vilken omfattning.

För varje bevakningsobjekt eller samling av objekt ska det finnas en bevakningsinstruktion som reglerar bevakningens omfattning[13].

Tekniska kontoret ansvarar för att upprätthålla dokumentation avseende ronderande bevakning i kommunens lokaler.

---

[12] Dessa beskrivs då i lokala rutiner eller anvisningar.
[13] Här avses en så kallad larminstruktion. Denna kan vara lokal eller övergripande för kommunens alla objekt.

8.9. Insats

För varje fastighet/lokal som försetts med inbrottslarmanläggning ska det finnas en insatsplan som reglerar hur larmcentral och väktare ska agera i händelse av larm.

Tekniska kontoret ansvarar för att upprätthålla dokumentation avseende insats vid larm i kommunens lokaler.

8.10. Principer för inpassering

Inpassering till kommunens lokaler sker med behörigheter som lagts på kommunens ID-kort alternativt passertagg.

Vid inpassering under kontorstid krävs endast kort för inpassering till Zon 1 – Grön zon och Zon 2 – Gul zon. Övrig tid (kvällar, nätter och helger) krävs såväl kort som en personlig PIN-kod.

För inpassering till Zon 3 – Röd zon krävs alltid kort och PIN-kod för inpassering.

9. Personalsäkerhet

Med personalsäkerhet avses de åtgärder som vidtas för att personal inte ska utgöra ett hot mot kommunens verksamhet och att kommunens verksamhet inte ska utgöra ett hot mot personalen. För säkerhetsprövning av personal se anvisning säkerhet.

9.1. Säkerhetsutbildning och informationsinsatser för personal

9.1.1. Säkerhetsinformation till nyanställda

Alla medarbetare i kommunen ska, i samband med anställning, informeras om vilka säkerhetskrav som ställs inom den verksamhet som medarbetaren ska delta i och ges ett exemplar av broschyren ”Säkerhet för nyanställda” som, på övergripande nivå, sammanfattar de säkerhetskrav som regleras i denna riktlinje.

9.1.2. Introduktionsutbildning

Medarbetare som har en tillsvidareanställning, eller visstidsanställning som är längre än 6 månader, ska genomföra kommunens introduktionsutbildning i säkerhet. Utbildningen fokuserar på medarbetarens egna ansvar för att följa regler och upprätthålla säkerheten i verksamheten.

9.1.3. Återkommande utbildning

Introduktionsutbildningen i säkerhet ska repeteras minst vartannat år för att säkerställa att medarbetarnas kunskap om säkerhet vidmakthålls och uppdateras utifrån nya förutsättningar.

9.1.4. Specialiserad utbildning

Personer som har ett särskilt ansvar för säkerhet inom en viss verksamhet (exempelvis chefer, kontaktombud eller specialister) ska ges den utbildning som krävs för att de ska kunna utföra sitt arbete på ett säkert sätt i enlighet med gällande regelverk. Tillhandahållande av specialiserade säkerhets-utbildningar samordnas av säkerhetschefen utifrån verksamhetens behov.

9.1.5. Informationsinsatser

Personal ska ges regelbunden och löpande information om säkerhetsrelaterade frågor som är relevanta för det egna arbetet.

Det huvudsakliga ansvaret för att personal hålls informerade om säkerhetsfrågor ligger på närmaste chef med stöd av kontaktombud, kommunens säkerhetschef och dataskyddsombudet.

Återkommande information till personal inom en specifik verksamhet kan exempelvis ske som en stående punkt på agendan i samband med regelbundna personalsamlingar.

9.2. Förebyggande arbete mot hot och våld

Kommunen bedriver ett långsiktigt förebyggande arbete för att förhindra förekomsten av hot och våld riktat mot personal och förtroendevalda.

En del i arbetet består i att ta fram policys, riktlinjer och handlingsplaner som reglerar hur förekomst av hot och våld ska hanteras för att skydda de berörda.

För information om hantering av uppkomna incidenter omfattande hot eller våld, se hantering av säkerhetsincidenter.

För mer information om kommunens förebyggande arbete mot hot och våld, se information om systematiska arbetsmiljöåtgärder rörande hot och våld på intranätet.

10. Kontinuitet

Kommunens arbete för att kunna säkerställa förmåga att bedriva kontinuerlig verksamhet beskrivs huvudsakligen i riktlinjen för beredskap. Här regleras endast de delar som är specifika för säkerhetsberedskap, d.v.s. beredskap att hantera säkerhetshändelser och inträffade incidenter som påverkar säkerhetsarbetet.

Kommunens säkerhetsberedskap baseras främst på att den som tjänstgör som tjänsteman i beredskap (TiB) även ansvarar för att hantera säkerhetshändelser och inträffade incidenter som inträffar utanför ordinarie arbetstid. Övriga roller med ansvar för säkerhetsarbetet kan inkallas vid behov.

11. Incidenthantering

Med en säkerhetsincident avses alla säkerhetsrelaterade händelser som skadar, eller riskerar att skada, kommunens verksamhet. Även identifierade brister i kommunens säkerhetsarbete som potentiellt kan leda till en incident ska hanteras på motsvarande sätt som en inträffad incident vad gäller rapportering, hantering och dokumentation.

Säkerhetsincidenter indelas i 3 kategorier beroende på omfattning, potentiell skada och hur tidskritisk hanteringen av incidenten är enligt nedan. Säkerhetsincidenten ska hanteras på olika sätt beroende på vilken kategori säkerhetsincidenten placeras i.

- Mycket allvarlig incident

Med en mycket allvarlig incident avses en incident som potentiellt kan resultera i hot mot personers liv och hälsa, mycket allvarlig skada på kommunens verksamhet eller bortfall av kritiska förmågor[14] under en längre tid. Hit räknas incidenter som kan komma att påverka kommunens säkerhetsskydd eller civilförsvarsförmåga samt personuppgiftsincidenter som riskerar att leda till att känsliga personuppgifter om flera individer röjs, eller att personuppgifter som är skyddsvärda med hänsyn till en individs liv, hälsa eller säkerhet röjs.

- Allvarlig incident

  Med en allvarlig incident avses en incident som potentiellt kan resultera i allvarlig skada på kommunens verksamhet, bortfall av kritiska förmågor under en kortare tid och/eller bortfall av icke-kritiska förmågor under en längre tid. Hit räknas incidenter som kan komma att påverka kommunens säkerhets- eller beredskapsarbete (som inte är av betydelse för säkerhetsskyddet eller civilförsvars-förmågan) samt personuppgiftsincidenter som riskerar att leda till att känsliga personuppgifter om enskilda individer röjs, eller att personuppgifter som inte är känsliga om ett större antal individer röjs.

- Begränsad incident

  Med en begränsad incident avses en incident som potentiellt kan resultera i begränsad skada på kommunens verksamhet och/eller bortfall av icke kritiska förmågor under en kortare tid. Hit räknas även personuppgiftsincidenter som riskerar att leda till att personuppgifter som inte anses känsliga om enstaka individer röjs.

11.1. Rapportering av säkerhetsincidenter

Säkerhetsincidenter ska huvudsakligen rapporteras genom en anmälan via kommunens incidentrapporteringsportal som återfinns på intranätet. Om incidenter bedöms kunna påverka kommunens säkerhetsskydd ska incidenten istället endast och omedelbart rapporteras muntligen till kommunens säkerhetschef. Anledningen till detta är att systemet som hanterar incidentrapporter som inkommer via incidentrapporteringsportalen är inte godkänt för att hantera uppgifter som är säkerhetsskyddsklassade.

Vid tveksamhet avseende huruvida en viss information kan rapporteras via incidentrapporteringsportalen, kontakta kommunens säkerhetschef för råd.

- Mycket allvarlig incident

  Mycket allvarliga incidenter ska omgående rapporteras via telefonkontakt med kommunens tjänsteman i beredskap (TiB). Därefter ska kontakt tas med kommunens säkerhetschef och/eller dataskyddsombudet (beroende på typ av incident) samt berörda chefer. Då kontakter har tagits enligt ovan ska incidenten registreras i kommunens incidenthanteringsportal (under förutsättning att

[14] Med kritisk förmåga avses sådana förmågor verksamheten inte klarar sig utan. Vattenförsörjning och elförsörjning kan utgöra exempel på sådana förmågor. Även vissa system för till exempel larmning betecknas som kritiska.

incidenten inte rör kommunens säkerhetsskydd eller civilförsvarsförmåga).

- Allvarlig incident

  Allvarliga incidenter ska skyndsamt rapporteras via telefonkontakt med närmaste chef och säkerhetschefen eller dataskyddsombudet (beroende på typ av incident). Därefter ska incidenten rapporteras i kommunens incidenthanteringsportal.

- Begränsad incident

  Begränsade incidenter ska rapporteras genom registrering i kommunens incidenthanteringsportal. Från portalen kommer information att komma närmaste chef, säkerhetschefen och dataskyddsombudet tillhanda.

11.2. Hantering av säkerhetsincidenter

Säkerhetsincidenter och identifierade brister i kommunens säkerhetsarbete ska hanteras skyndsamt och är prioriterade. Ansvaret att hantera en säkerhetsincident, eller åtgärda en säkerhetsbrist, faller på verksamhetsansvarig chef förutom i de fall då incidenten/säkerhetsbristen påverkar hela, eller stora delar av kommunen, alternativt rör gemensamma IT-system eller säkerhetsfunktioner. I sådana fall ansvarar kommunens säkerhetschef för att samordna hanteringen.

Skadebegränsande åtgärder ska vid behov vidtas snarast av den som upptäcker en incident. Det gäller exempelvis bevakningspersonal som uppmärksammar brister i skalskyddet, eller egen personal som uppmärksammar en personuppgiftsincident.

11.3. Dokumentation och uppföljning av säkerhetsincidenter

Utöver den dokumentation om inträffade säkerhetsincidenter och identifierade säkerhetsbrister som framgår av kommunens incidenthanteringssystem så ska de åtgärder som vidtas för att hantera incidenter/brister dokumenteras så snart som möjligt av den som vidtar åtgärderna och en kopia på dokumentationen ska lämnas till kommunens säkerhetschef.

Syftet med dokumentationen är att kommunen systematiskt ska kunna utvärdera säkerhetsarbetet och vid denna utvärdering utgör kvalitativ information om inträffade incidenter och identifierade brister samt de åtgärder som vidtagits ett viktigt underlag.

11.4. Disciplinära åtgärder vid misskötsel och bristande efterlevnad

Alla som genom anställning, uppdrag eller av annan anledning utför arbete för kommunen är skyldiga att följa kommunens riktlinje för säkerhet.

Vid misskötsel eller bristande efterlevnad av riktlinjen kan olika disciplinära åtgärder komma att vidtas i syfte att skydda kommunen från vidare skada.

Misskötsel eller bristande efterlevnad kan resultera i omprövning och eventuell begränsning av tilldelade behörigheter till kommunens lokaler och IT-miljö. Därefter genomförs en intern utredning av det inträffade för att klarlägga vad som inträffat och rekommendera vidare hantering.

Om den interna utredningen ger anledning till det sker en anmälan till HR för vidare arbetsrättslig prövning, samt om det finns anledning att misstänka att ett brott har begåtts, en polisanmälan.

12. Uppföljning och utvärdering av kommunens säkerhetsarbete

För att säkerställa att kommunens säkerhetsarbete får avsedd effekt, och att kommunen följer gällande författningskrav och krav i ingångna avtal, så ska uppföljning och utvärdering av arbetet ske löpande. Respektive förvaltning/ avdelning och enhet ska genomföra interna kontroller i den omfattning som krävs för att kunna upprätthålla en lägesbild över säkerheten.

Vid kommunen ska det finnas en övergripande plan för säkerhetskontroller. Kommunens säkerhetschef ansvarar för kontrollplanen och rapporterar resultatet av genomförda kontroller till ledningsgruppen. Allvarlig misskötsel eller sårbarheter som upptäcks i samband med kontroller ska rapporteras omgående till ledningsgruppen. Övriga resultat av genomförda kontroller rapporteras kvartalsvis i samband med ledningens genomgång av säkerhets- och beredskapsarbetet inom kommunen.

Säkerhetschefen ansvarar för beredning inför ledningens genomgång och föredrar säkerhets- och beredskapsfrågor för ledningsgruppen kvartalsvis. Fokus för ledningens genomgång ska ligga på hantering av prioriterad verksamhet samt den långsiktiga effekten av kommunens säkerhets- och beredskapsarbete.