Kommunstyrelsen

§234 Dnr KS 2020-1899

Antagande av policy och riktlinje för systematiskt säkerhetsarbete

Beslut

Kommunstyrelsen föreslår:

1. Kommunfullmäktige beslutar att anta Policy för systematiskt säkerhetsarbete.
2. Kommunfullmäktige beslutar att upphäva Informationssäkerhetspolicy för Norrtälje kommun, KF § 61, antagen av kommunfullmäktige 2012-04-02,.

Kommunstyrelsen beslutar för egen del, under förutsättning att kommunfullmäktige beslutar om upphävande av ”Informationssäkerhetspolicy för Norrtälje kommun” KF § 61 samt antagande av Policy för systematiskt säkerhetsarbete, att anta Riktlinje för systematiskt säkerhetsarbete.

Sammanfattning av ärendet

Ny policy och riktlinje för systematiskt säkerhetsarbete syftar till implementering av ett koncept som skapar förutsättningar för att leva upp till de laga krav som i dag ställs på områdena informationssäkerhet, säkerhetsskydd, fysisk säkerhet, säkerhet vid upphandling, säkerhet vid rekrytering samt incidentrapportering. Norrtälje kommun uppnår inte laga efterlevnad avseende flera av ovan nämnda områden i dagsläget. Ambitionen att sammanställa en policy och en riktlinje som omfattar flera olika ämnesområden inom säkerhetsområdet bygger på att dessa områden är ömsesidigt beroende av samstämmighet för att bygga en fungerande helhet.

Beslutsunderlag

§161 KSAU protokollsutdrag avseende Antagande av policy och riktlinje för systematiskt säkerhetsarbete
Tjänsteutlåtande avseende Antagande av policy och riktlinje för systematiskt säkerhetsarbete
Riktlinje för systematiskt säkerhetsarbet1
Policy för systematiskt säkerhetsarbete

Beslutande sammanträde

Beslutsgång

Ordföranden frågar om kommunstyrelsen kan besluta i enlighet med kommunstyrelsens arbetsutskotts förslag, och finner att kommunstyrelsen beslutar i enlighet med förslaget.

Beslutet ska skickas till

Samtliga kontor/förvaltningar i Norrtälje kommun.
Författningssamlingen

Kommunstyrelsens arbetsutskott

Allmänkommunala ärenden

§161 Dnr KS 2020-1899

Antagande av policy och riktlinje för systematiskt säkerhetsarbete
Beslut

Kommunstyrelsens arbetsutskott föreslår:
Kommunstyrelsen föreslår:

1. Kommunfullmäktige beslutar att anta Policy för systematiskt säkerhetsarbete.
2. Kommunfullmäktige beslutar att upphäva Informationssäkerhetspolicy för Norrtälje kommun, KF § 61, antagen av kommunfullmäktige 2012-04-02,.

Kommunstyrelsen beslutar för egen del, under förutsättning att kommunfullmäktige beslutar om upphävande av ”Informationssäkerhetspolicy för Norrtälje kommun” KF § 61 samt antagande av Policy för systematiskt säkerhetsarbete, att anta Riktlinje för systematiskt säkerhetsarbete.

Sammanfattning av ärendet

Ny policy och riktlinje för systematiskt säkerhetsarbete syftar till implementering av ett koncept som skapar förutsättningar för att leva upp till de laga krav som i dag ställs på områdena informationssäkerhet, säkerhetsskydd, fysisk säkerhet, säkerhet vid upphandling, säkerhet vid rekrytering samt incidentrapportering. Norrtälje kommun uppnår inte laga efterlevnad avseende flera av ovan nämnda områden i dagsläget. Ambitionen att sammanställa en policy och en riktlinje som omfattar flera olika ämnesområden inom säkerhetsområdet bygger på att dessa områden är ömsesidigt beroende av samstämmighet för att bygga en fungerande helhet.

Beslutsunderlag

Tjänsteutlåtande avseende Antagande av policy och riktlinje för systematiskt säkerhetsarbete
Policy för systematiskt säkerhetsarbete
Riktlinje för systematiskt säkerhetsarbet1

Beslutande sammanträde

Beslutsgång

Ordföranden frågar om kommunstyrelsens arbetsutskott kan besluta i enlighet med kommunstyrelsekontorets tjänsteutlåtandes förslag, och finner att kommunstyrelsens arbetsutskott beslutar i enlighet med förslaget.

Beslutet ska skickas till

Samtliga kontor/förvaltningar i Norrtälje kommun.
Författningssamlingen

NORRTÄLJE KOMMUN

TJÄNSTEUTLÅTANDE

Datum: 2020-09-22
Diarienummer: KS 2020-1899

Förvaltning och avdelning

Handläggare: Olof Sigfrid
Titel: Säkerhetschef
E-post: olof.sigfrid@norrtalje.se

Till: Kommunstyrelsens arbetsutskott

Antagande av policy och riktlinje för systematiskt säkerhetsarbete

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår:
Kommunstyrelsen föreslår:

1. Kommunfullmäktige beslutar att anta Policy för systematiskt säkerhetsarbete.
2. Kommunfullmäktige beslutar att upphäva Informationssäkerhetspolicy för Norrtälje kommun, KF § 61, antagen av kommunfullmäktige 2012-04-02,.

Kommunstyrelsen beslutar för egen del, under förutsättning att kommunfullmäktige beslutar om upphävande av ”Informationssäkerhetspolicy för Norrtälje kommun” KF § 61 samt antagande av Policy för systematiskt säkerhetsarbete, att anta Riktlinje för systematiskt säkerhetsarbete.

Sammanfattning av tjänsteutlåtandet

Ny policy och riktlinje för systematiskt säkerhetsarbete syftar till implementering av ett koncept som skapar förutsättningar för att leva upp till de laga krav som i dag ställs på områdena informationssäkerhet, säkerhetsskydd, fysisk säkerhet, säkerhet vid upphandling, säkerhet vid rekrytering samt incidentrapportering. Norrtälje kommun uppnår inte laga efterlevnad avseende flera av ovan nämnda områden i dagsläget. Ambitionen att sammanställa en policy och en riktlinje som omfattar flera olika ämnesområden inom säkerhetsområdet bygger på att dessa områden är ömsesidigt beroende av samstämmighet för att bygga en fungerande helhet.

Ärendet

Beskrivning

Den interna säkerheten är viktig för att skydda såväl Norrtälje kommun som de personer och organisationer som är beroende av att kommunen kan fortsätta bedriva sin verksamhet. Att vi har ett ändamålsenligt och väl fungerande internt säkerhetsarbete är avgörande för att vi ska kunna upprätthålla förtroendet för kommunen och den kommunala verksamheten.
Med säkerhetsarbete avses det systematiska, förebyggande arbete som Norrtälje kommun bedriver för att minimera risken för negativa händelser och begränsa skadan av inträffade negativa händelser inom den kommunala verksamheten. Utan en beslutad policy och riktlinje som ser till helheten av ett systematiskt och långsiktigt säkerhetsarbete kommer Norrtälje kommun fortsätta att vara kravunderskridande i förhållande till de laga krav som styr kommunens interna säkerhetsarbete.

Målet med Policy för systematiskt säkerhetsarbete är att Norrtälje kommun ska anta ett inriktningsbeslut i syfte att Norrtälje kommun ska kunna bedriva ett ändamålsenligt och kostnadseffektivt säkerhetsarbete.

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

I Mål och budget 2020-2022 har kommunen, med målsättningen ”En trygg och säker kommun – i både vardag och kris”, antagit en bred ansats i arbetet med trygghet och säkerhet. En del i detta är den interna kommunsäkerheten vilken består av informationssäkerhet, säkerhetsskydd, fysisk säkerhet, säkerhet vid upphandling, säkerhet vid rekrytering, incidentrapportering samt skydd mot hot och våld. Den nya policyn och riktlinjen omfattar inte området skydd mot hot och våld då detta område har sin egen beslutade policy och riktlinje som inte är i behov av uppdatering. I dagsläget är Norrtälje kommun kravunderskridande i förhållande till flera av de laga krav som existerar, i synnerhet inom områdena informationssäkerhet och säkerhetsskydd. Ambitionen att sammanställa en policy och en riktlinje, som omfattar flera olika ämnesområden inom säkerhetsområdet, bygger på att dessa områden är ömsesidigt beroende av samstämmighet för att bygga en fungerande och kostnadseffektiv helhet.

Även säkerhetsrelaterade krav som följer av den europeiska dataskyddsförordningen (GDPR/DSF) har inarbetats i kommunens säkerhetsarbete och de inriktande, styrande och stödjande dokument som reglerar kommunens säkerhetsarbete. De mest noterbara förändringar som sker, och som kommer påverka samtliga kommunens verksamheter, är det nya koncept för informationssäkerhet som den nya policyn och riktlinjen utgör ett fundament för. Policy och riktlinje kommer att kompletteras med utbildningar och pedagogiska instruktioner för att en ny systematik och nya arbetsmetoder ska kunna upprätthållas. Implementering av ett koncept för systematiskt säkerhetsarbete skapar förutsättningar för att leva upp till de laga krav som i dag ställs på ovan nämnda områden.

Det interna säkerhetsarbetet ska baseras på genomförda analyser (t.ex. de lagstadgade analyserna säkerhetsskyddsanalys och risk- och sårbarhetsanalys) och vara väl avvägt utifrån förekomsten av skyddsvärda tillgångar och den dimensionerande hotbilden för Norrtälje kommuns verksamhet vilka ska framgå av genomförda analyser.

Det interna säkerhetsarbetet är utformat för att åstadkomma ett ändamålsenligt skydd för Norrtälje kommuns skyddsvärda tillgångar, vilka indelas i följande kategorier:

- Kommunens medarbetare och övriga personer som deltar i vår verksamhet
- Förtroendet för Norrtälje kommun och vårt varumärke
- Kommunens information och den information som vi hanterar för våra kunders räkning
- Kommunens egendom (i form av lokaler och utrustning m.m.) och egendom som vi nyttjar
- Kommunens ekonomiska tillgångar
- Kommunens kulturhistoriska värden

Ansvaret för den interna säkerheten är uppdelat på ett antal roller, enligt följande:

Kommundirektör	Är ytterst ansvarig för säkerheten inom Norrtälje kommun och ansvarar för att resurser avdelas för säkerhetsarbetet utifrån fastställda målsättningar. Kommundirektören beslutar i säkerhetsfrågor som inte delegerats.
Säkerhetsskyddschef	Beslutar i frågor som rör kommunens säkerhetsskydd efter delegering från kommundirektören.
Säkerhetschef	Leder och följer upp säkerhetsarbetet och ger stöd till ledning och medarbetare i säkerhetsfrågor. Säkerhetschefen beslutar i säkerhetsfrågor efter delegering från kommundirektören.

Chefen för IT-avdelningen	Ansvarar för implementation av säkerhetsåtgärder för kommunens IT-miljö och kommunikationslösningar utifrån fastställda krav i styrande dokument.
Dataskyddsombudet	Leder arbetet med att säkerställa Norrtälje kommuns efterlevnad av dataskyddsförordningen och utgör kontaktperson mot Datainspektionen och ger stöd till ledning och medarbetare i frågor rörande behandling av personuppgifter.
Medarbetare och andra som deltar i Norrtälje kommuns verksamhet	Ansvarar för att efterleva styrande dokument och se till att det dagliga arbetet utförs i enlighet med gällande regler samt rapportera säkerhetsincidenter enligt fastställd rutin.

Säkerhetsarbetet inom Norrtälje kommun styrs av följande inriktande, styrande och stödjande dokument:

- Kommunens Policy för systematiskt säkerhetsarbete utgör inriktande dokument för det interna säkerhetsarbetet.
- Kommunens Riktlinje för systematiskt säkerhetsarbete utgör styrande dokument för säkerhetsarbetet.
- Anvisningar och rutiner utgör stödjande dokument för säkerhetsarbetet.

I slutändan utgör medarbetarens kunskap om-, och förståelse för, det interna säkerhetsarbetet det bästa skyddet för verksamheten. Norrtälje kommun ska sträva efter ständig kompetensutveckling inom säkerhetsområdet för samtliga medarbetare och tillhandahåller återkommande internutbildningar i säkerhetsfrågor.

Ambitionen att sammanställa en policy och en riktlinje som omfattar flera olika ämnesområden inom säkerhetsområdet bygger på att dessa områden är ömsesidigt beroende av samstämmighet för att bygga en fungerande helhet. Som exempel är informationssäkerhet en del i ett fungerande säkerhetsskydd samtidigt som fysisk säkerhet, säkerhet vid upphandling och säkerhet vid rekrytering är delar i ett fungerande koncept för säkerhetsskydd och informationssäkerhet. Av denna anledning har vi samlat de sammanlänkade säkerhetsområdena i ett övergripande koncept för säkerhet som syftar till att på ett överskådligt sätt reglera de komplexa sambanden mellan dessa områden som grundar sig på laga krav, standarder, praxis och analysverksamhet.

Många av de laga krav som ställs på dessa områden är även väldigt detaljspecifika i hur lagstiftningen bör tillämpas vilket innebär att även Norrtälje kommuns riktlinje för dessa ämnesområden behöver ha en relativt hög detaljupplösning. För att vidare kunna implementera ett koncept för systematiskt säkerhetsarbete behöver riktlinjen innehålla all handläggning som våra medarbetare behöver tillämpa för att vi som kommun ska klara att leva upp till de laga kraven. Då riktlinjen är utformad som ett dokument som ser till helheten av det systematiska långsiktiga säkerhetsarbetet, samt är utformad utifrån vilken information som det föreligger ett behov av politiskt beslut bakom, och inte enbart utifrån pedagogisk lättillgänglighet, kommer riktlinjen att kompletteras med instruktioner och annat pedagogiskt material för att underlätta efterlevnaden avseende t.ex. kraven på informationssäkerhet som omfattar samtliga medarbetare i Norrtälje kommun.

Kommunen har sedan tidigare en informationssäkerhetspolicy beslutad i kommunfullmäktige 2012-04-02. Innehållet i den policyn har uppdaterats och inkorporerats inom förslaget för ny policy och riktlinje för systematiskt säkerhetsarbete. Därmed kan nuvarande informationssäkerhetspolicy upphävas.

Lagkrav

Det finns en mängd författningskrav i lagar, förordningar och föreskrifter som reglerar Norrtälje kommuns säkerhetsarbete. Förutom krav som innebär att kommunen ska vidta säkerhetsåtgärder förekommer också krav som förhindrar att kommunen vidtar alltför långtgående säkerhetsåtgärder (det senare gäller exempelvis krav på allmänna handlingars offentlighet som begränsar Norrtälje kommuns 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. Författningarna innebär dels direkta krav på Norrtälje kommuns säkerhetsarbete (exempelvis säkerhetsskyddslagstiftningen eller dataskyddsförordningen) och dels begränsningar i Norrtälje kommuns möjligheter att vidta för långtgående säkerhetsåtgärder (exempelvis tryckfrihetsförordningen eller lagen om offentlig upphandling).

Typ	**Benämning**	**Beteckning**
EU-rätt	General Data Protection Regulation	2016/679
EU-rätt	Network and Information Security directive	2016/1148
Grundlag	Tryckfrihetsförordningen	1949:105
Grundlag	Yttrandefrihetsgrundlagen	1991:1469
Lag	Brottsbalk	1962:700
Lag	Offentlighets- och sekretesslag	2009:400
Lag	Säkerhetsskyddslag	2018:585
Lag	Lag om informationssäkerhet för samhällsviktiga och digitala tjänster	2018:1174
Lag	Lag med kompletterande bestämmelser till EU:s dataskyddsförordning	2018:218
Lag	Skyddslag	2010:305
Lag	Kamerabevakningslag	2018:1200
Lag	Lag om skydd för geografisk information	2016:319
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	2006:544
Lag	Lag om offentlig upphandling	2016:1145
Lag	Lag om upphandling på försvars- och säkerhetsområdet	2011:1029
Lag	Lag om offentlig anställning[1]	1994:260
Föreskrift[2]	Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd	PMFS 2019:2
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

Koppling till gällande styrdokument

I Mål och budget 2020-2022 anges att ett av kommunfullmäktiges mål är att Norrtälje ska vara En trygg och säker kommun – i både vardag och kris. Övergången till ett systematiskt säkerhetsarbete, vilket antagandet av den nya policyn och riktlinjen skulle innebära, är en förutsättning för att vi ska kunna leva upp till att vara en säker kommun i både vardag och kris. De laga krav som ställs till vardags såväl som i krissituationer kräver att vissa fundamentala arbetsmetoder kopplade till bl.a. säkerhetsskydd och informationssäkerhet finns på plats för att arbetet med säkerhet och krisberedskap ska kunna bedrivas.

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

I Verksamhetsplan och budget 2020 för kommunstyrelsen har Kontoret för räddning och säkerhet (numera Trygghets- och säkerhetskontoret) tillskrivits ansvar för verksamhetsprocesserna informationssäkerhet och säkerhetsskydd. Den konkreta uppgiften är ”Ta fram och implementera systematik för kommunens informationssäkerhetsarbete.” Denna uppgift ombesörjs inom ramen för det koncept för systematiskt säkerhetsarbete som den nya policyn och riktlinjen styr.

Ekonomiska konsekvenser och riskanalys

Ett beslut om antagande av policy och riktlinje för systematiskt säkerhetsarbete får inga direkta ekonomiska konsekvenser förutom den arbetstid som nyttjas för arbete med nya handläggningsförfaranden, dock kan det tillkomma vissa kostnader i arbetet med att eftersträva laga efterlevnad i form av utbildning för kommunens medarbetare och eventuell anpassning av tekniska system. Samtidigt är det okänt vilka kostnader kommunen har i dagsläget som en konsekvens av bristen på ett systematiskt säkerhetsarbete. För vidare resonemang om hur ekonomiska risker minimeras genom ett systematiskt säkerhetsarbete, se konsekvens/riskanalys nedan.

Målet med Policy för systematiskt säkerhetsarbete är att Norrtälje kommun ska anta ett inriktningsbeslut i syfte att Norrtälje kommun ska kunna bedriva ett ändamålsenligt och kostnadseffektivt säkerhetsarbete. Målet med Riktlinje för systematiskt säkerhetsarbete är att reglera samtliga krav på Norrtälje kommuns säkerhetsarbete på ett samlat och enhetligt sätt. Syftet med riktlinjen är att tillhandahålla ett tydligt och fastställt underlag för framtagande av enkla, och konkreta anvisningar och rutiner som stödjer medarbetare och leverantörer i det dagliga arbetet. Den nya strukturen och systematiseringen av kommunens samlade säkerhetsarbete kommer innebära synergieffekter och effektivisering i form av minskad risk för:

- stöld av kommunens egendom som följd av för dåligt utvecklat fysiskt skydd
- röjande av sekretessreglerad information som följd av brister i en icke heltäckande informationssäkerhet vilket leder till kostnader och kan orsaka oåterkalleliga informationsförluster
- IT-incidenter som leder till kostnader och kan orsaka oåterkalleliga informationsförluster
- parallella motsägelsefulla arbetsmetoder och systematik som orsakar missförstånd
- höga kostnader till följd av ostrukturerade upphandlingar
- kravunderskridande leverantörer av säkerhetsrelaterade tjänster till följd av ostrukturerade upphandlingar samt avsaknad av kravställningar
- att någon av ovan nämnda risker orsakar minskat förtroende för kommunen hos andra myndigheter, företag eller allmänheten.

Vidare finns det en risk att avsaknaden av ett systematiskt arbetssätt inom säkerhetsområdet skapar en ojämn säkerhetsnivå mellan de olika underliggande delområdena. Detta riskerar att leda till att även om kommunen gör ekonomiskt kostsamma men effektiva och bra lösningar inom ett område, så kan de vara till ingen nytta då vi samtidigt inte har identifierat brister inom ett annat område, vilket kan göra de kostsamma satsningar som gjorts verkningslösa. Som exempel kan man vidta stora mängder kostsamma åtgärder för att undvika IT-säkerhetsincidenter och informationsförluster, men om kommunen samtidigt inte har gjort bakgrundskontroller på de personer som ska ta del av känslig information, eller inte har byggt ett fullt ut fungerande fysiskt skydd kring IT-systemen, riskerar vi ha byggt kostsamma IT-säkerhetslösningar till ingen nytta.

De identifierade riskerna av att implementera ett koncept för systematiskt säkerhetsarbete bör ställas emot det faktum att dagens avsaknad av ett koncept för systematiskt säkerhetsarbete även innebär avsaknad av samtliga ovan nämnda riskminimerande effekter. Identifierade risker är:

Risk	**Kommentarer/Åtgärder**
Medarbetare följer inte de nya anvisningarna och riktlinjerna till följd av tidigare inarbetade rutiner och oförståelse för det nya konceptet.	Kontrollplan ska tas fram för att säkerställa efterlevnad. En kommunikationsplan har tagits fram för att förankra det nya konceptet inom samtliga verksamheter.
Eventuellt ökade kostnader för kommunens IT-verksamhet	De nya riktlinjerna ställer krav på kommunens upphandling och drift av kommunens IT-system. SKRs verktyg KLASSA, baserat på ISO 27 000-serien, sätter standarden för kravställningen, vilket är det verktyg som

	kommunen redan idag använder sig av, men inte alltid tillämpar.
Klassificering av information upplevs av medarbetare som omständligt och tidskrävande.	Alternativet till att inte klassificera information är att inte ha någon systematisk informationssäkerhet och ingen laga efterlevnad, vilket är fallet i kommunen idag.

Samberedning

Ärendet har tagits fram av Trygghets och Säkerhetskontoret i samråd med Kommunkoncernledningen, Kommunstyrelsekontoret, HR-avdelningen, IT-avdelningen, Upphandling, Arkiv/Registratur Kommunjurist, Dataskyddsombud, Socialkontoret, Barn- och Utbildningskontoret, Tekniska kontoret, Bygg- & Miljökontoret, KSON samt säkerhetsexpertis hos Secana AB.

Samberedning har skett genom diverse workshops samt utbildningstillfällen.

Ärendet har även samberetts med fackliga parter via CESAM.

Förvaltningens analys och slutsatser

För att Norrtälje kommun ska har förutsättningar att följa svensk lagstiftning, nå kravnivåer utifrån uppbyggnaden av civilt förvar samt skydda sina skyddsvärda tillgångar bedömer Trygghets och säkerhetskontoret det nödvändigt att kommunen antar en uppdaterad policy och riktlinje för kommunens systematiska säkerhetsarbete. I dagsläget når inte Norrtälje, likt många andra kommuner, den nivå som egentligen krävs inom området. Detta tydliggjordes bl.a. vid den nyligen genomförda revisionen av kommunens informationssäkerhetsarbete. Vid ett antagande av förslaget till policy och riktlinjer ges dock förutsättningar för att genom ett kontinuerligt och systematiskt säkerhetsarbete nå dessa nivåer på ett bra sätt och på sikt bli ett nationellt exempel på en hög kommunal säkerhetsnivå. Vissa kostnader i form av bland annat utbildning för medarbetare samt anpassning av tekniska system kan tillkomma, men dessa bedöms som små i förhållande till de risker, såväl verksamhetsmässiga som ekonomiska, som kommunen har vid avsaknad av ett ändamålsenligt och effektivt systematiskt säkerhetsarbete.

Alternativet att inte anta den föreslagna policyn och riktlinjerna bedömer Trygghets- och säkerhetskontoret som olyckligt, då kommunen då inte har de styrdokument som krävs för att nå tillräckligt god nivå på det interna säkerhetsarbetet. Det i sin tur riskerar att äventyra kommunens skyddsvärda tillgångar.

Tidplaner

Kommunfullmäktige behandlar ärendet 2020-12-14, och vid positivt beslut kan den nya policyn och riktlinjen tillämpas omgående.

Charlotta Tillbom
Tf direktör Trygghets- och säkerhetskontoret
Trygghets- och säkerhetskontoret

Olof Sigfrid
Säkerhetschef
Trygghets- och säkerhetskontoret

Bilagor

Bilaga 1, Policy för systematiskt säkerhetsarbete, 2020-10-22
Bilaga 2, Riktlinje för systematiskt säkerhetsarbete, 2020-10-22

Beslut skickas till

Samtliga kontor/förvaltningar i Norrtälje kommun.
Författningssamlingen

NORRTÄLJE KOMMUN

2020-10-22
Diarienummer: KS 2020-1901

Avdelningen för säkerhet och krisberedskap
Namn: Olof Sigfrid

Riktlinje för systematiskt säkerhetsarbete

Innehåll

1 Inledning

Detta dokument utgör Norrtälje kommuns riktlinjer för systematiskt säkerhetsarbete. Riktlinjerna följer beslutade policys som beskriver Norrtälje kommuns övergripande målsättningar för säkerhetsarbetet.

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

Organisationens säkerhetsarbete syftar till att säkerställa Norrtälje kommuns 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 Norrtälje kommun ansvarar för och är beroende av.

Riktlinjerna ingår i den struktur av styrande och stödjande dokument som reglerar Norrtälje kommuns säkerhetsarbete. Riktlinjerna 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 Norrtälje kommuns verksamhet ska bedrivas.

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

1.1 Mål och syfte

Målet med riktlinjerna är att på ett samlat och enhetligt sätt reglera samtliga krav på Norrtälje kommuns säkerhetsarbete.

Syftet med riktlinjerna är att tillhandahålla ett tydligt och fastställt underlag för framtagande av enkla, och konkreta anvisningar och rutiner som stödjer medarbetare och leverantörer i det dagliga arbetet.

1.2 Riktlinjernas uppbyggnad och innehåll

En målsättning för riktlinjerna är att samla samtliga krav som reglerar Norrtälje kommuns säkerhetsarbete på ett ställe i syfte att förtydliga kraven för medarbetare och leverantörer samt underlätta löpande revidering.

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

Riktlinje för systematiskt säkerhetsarbete inkluderar krav inom ett stort antal områden: informationssäkerhet, säkerhetsskydd, fysisk säkerhet, säkerhet vid upphandling,

säkerhet vid rekrytering samt incidentrapportering. Även säkerhetsrelaterade krav som följer av den europeiska dataskydds-förordningen (GDPR/DSF) har inarbetats i riktlinjerna.

Riktlinjerna fokuserar på att beskriva de konkreta krav på säkerhetsåtgärder som gäller inom Norrtälje kommuns verksamhet och pedagogiska beskrivningar av de principer som styr säkerhetsarbetet har begränsats till korta inledande texter för varje delområde. För mer information om säkerhetsarbete rekommenderas Norrtälje kommuns säkerhetsutbildningar (se avsnitt 10.2 Säkerhetsutbildning och informationsinsatser för medarbetare samt 11.2 Säkerhetsutbildning och informationsinsatser för leverantörer nedan).

2 Styrande regelverk

2.1 Författningskrav på Norrtälje kommuns säkerhetsarbete

Det finns en mängd författningskrav i lagar, förordningar och föreskrifter som reglerar Norrtälje kommuns säkerhetsarbete. Förutom krav som innebär att kommunen ska vidta säkerhetsåtgärder så förekommer också krav som förhindrar att kommunen vidtar alltför långtgående säkerhetsåtgärder (det senare gäller exempelvis krav på allmänna handlingars offentlighet som begränsar Norrtälje kommuns 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 Norrtälje kommuns säkerhetsarbete (exempelvis säkerhetsskyddslagstiftningen eller dataskyddsförordningen) och dels författning som begränsar Norrtälje kommuns möjligheter att vidta säkerhetsåtgärder (exempelvis tryckfrihetsförordningen eller lagen om offentlig upphandling).

Typ	Benämning	Förkortas	Beteckning
EU-rätt	General Data Protection Regulation	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		2018:658

Typ	Benämning	Förkortas	Beteckning
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
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	2016:1145
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 2019:2
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

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

2.2 Inriktande, styrande och stödjande dokument avseende säkerhet

Kommunfullmäktige inriktar Norrtälje kommuns systematiska säkerhetsarbete genom att fastställa policys inom olika områden som de förtroendevalda bedömer vara särskilt viktiga att lyfta fram.

De konkreta kraven på säkerhet inom Norrtälje kommuns verksamhet regleras i riktlinjerna för säkerhet. Utöver dessa förekommer även ett antal anvisningar och rutiner som syftar till att stödja verksamhetens säkerhetsarbete genom att tydliggöra hur riktlinjerna ska tillämpas.

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

2.3 Revidering av inriktande, styrande och stödjande dokument för Norrtälje kommuns säkerhet

Nedanstående sammanställs kraven på intervall för regelbunden revidering av inriktande, styrande och stödjande dokument som reglerar Norrtälje kommuns säkerhetsarbete.

Dokumenttyp	Ansvarig	Beslutas av	Intervall
Policy - Inriktande dokument	Säkerhetschef	Kommunfullmäktige	1 gång per mandatperiod
Riktlinje - Styrande dokument	Säkerhetschef	Kommunstyrelsen	2 gånger per mandatperiod
Kommunövergripande rutiner och anvisningar – Stödjande dokument	Säkerhetschef	Säkerhetschef	Vid behov
Lokala rutiner och anvisningar	Säkerhets- och beredskaps-samordnare	Ansvarig chef	Vid behov

3 Kommunens behov av säkerhet

Kommunens behov av säkerhet styrs bara delvis av föreliggande författningskrav. Säkerheten syftar till att skydda Norrtälje kommuns verksamhet och ytterst till att skydda den samhällsviktiga och säkerhetskänsliga verksamhet som är kritisk för kommunens invånare och organisationer samt, i förlängningen, för Sverige.

Även de krav som föreligger på Norrtälje kommuns säkerhetsarbete (exempelvis inom ramen för säkerhetsskyddslagstiftningen) baseras på att Norrtälje kommun 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 Norrtälje kommun är beroende av för att kunna bedriva verksamhet samt föreliggande risker och 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.

3.1 Organisationens skyddsvärda tillgångar

De skyddsvärda tillgångar som Norrtälje kommuns verksamhet är beroende av kan insorteras i någon av nedanstående kategorier.

3.1.1 Personer

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

3.1.2 Förtroende

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

3.1.3 Information

Den information som förekommer inom Norrtälje kommuns verksamhet utgör en skyddsvärd tillgång då Norrtälje kommuns verksamhet i mycket hög grad är beroende av tillgång till information. Att informationen är korrekt och tillgänglig när den behövs, samtidigt som den skyddas mot obehörig åtkomst, är avgörande för Norrtälje kommuns verksamhet. Felaktig hantering av information skulle kunna skada såväl kommunen som enskilda individer och organisationer och kunna leda till att förtroendet för Norrtälje kommun skadas allvarligt.

3.1.4 Egendom och utrustning

Organisationens 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

Organisationen 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 Norrtälje kommun förfogar över. Även dessa ekonomiska och kulturhistoriska värden utgör skyddsvärda tillgångar för Norrtälje kommun.

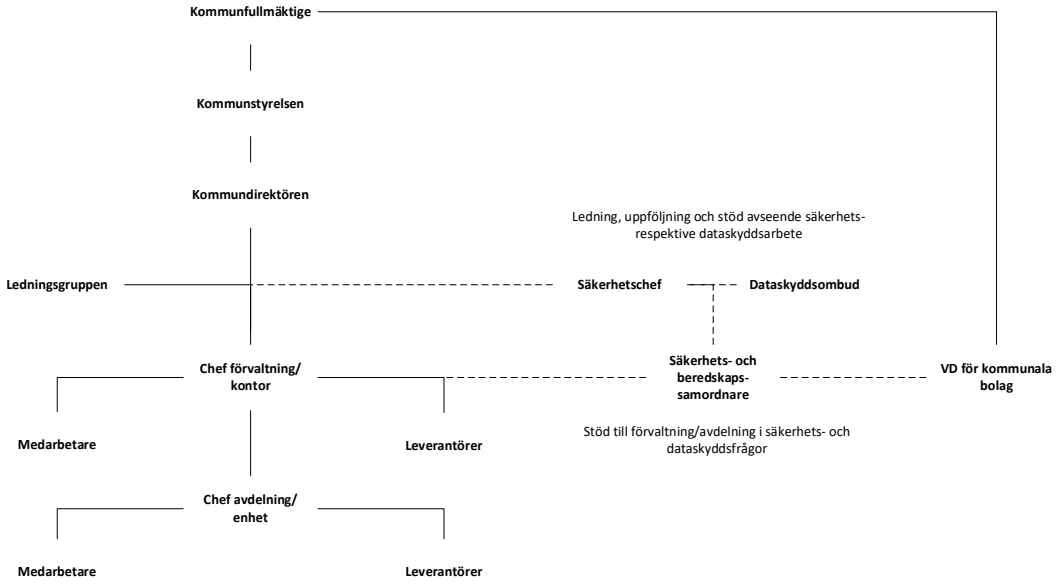
4 Kommunens förutsättningar för att bedriva säkerhetsarbete

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

Då Norrtälje kommun har begränsade resurser för att bedriva säkerhetsarbete så är det avgörande att arbetet bedrivs på ett kostnadseffektivt sätt och att säkerhetsrelaterade frågor, så långt som möjligt, hanteras i linjeorganisationen och inarbetas i ordinarie huvudprocesser, riktlinjer och rutiner.

Säkerhetsarbetet inom kommunens organisation ska bedrivas i nära samarbete med övriga närliggande kommuner och så långt som möjligt, samordnas inom ramen för samverkansorganisationer för att uppnå synergieffekter och hushålla med Norrtälje kommuns resurser.

5 Organisation av kommunens säkerhetsarbete



Figur 1: Principskiss - Fördelning av roller och ansvar för Norrtälje kommuns säkerhetsarbete.

5.1 Roller med säkerhetsansvar

5.1.1 Kommunfullmäktige

I egenskap av Norrtälje kommuns högsta beslutande organ inriktar kommunfullmäktige säkerhetsarbetet på en övergripande nivå genom beslut om fördelning av budget för säkerhetsarbetet. Kommunfullmäktige beslutar även om policys som inriktar Norrtälje kommuns säkerhetsarbete.

5.1.2 Kommunstyrelsen

Förutom att genomföra kommunfullmäktiges beslut har kommunstyrelsen till uppgift att leda och samordna Norrtälje kommuns angelägenheter, lämna förslag till budget och leda budgetarbetet samt att ha uppsikt över Norrtälje kommuns nämnder och egna bolag. Detta innebär att kommunstyrelsen har en viktig roll i arbetet med att säkerställa budgeten för Norrtälje kommuns säkerhetsarbete och förväntas utöva tillsyn även i säkerhetsfrågor.

5.1.3 Kommundirektören och Norrtälje kommuns ledningsgrupp

Kommundirektören är, med stöd av övriga ledningsgruppen, ytterst ansvarig för säkerheten i Norrtälje kommun och Norrtälje kommuns säkerhetsarbete.

Ledningsgruppen ska säkerställa att de resurser som krävs för att genomdriva beslut om Norrtälje kommuns säkerhetsarbete tillförs Norrtälje kommun samt ansvarar för att samordna de förändringar som krävs för att leva upp till styrdokument avseende säkerhet.

Ledningsgruppen utgör även det organ som dataskyddsombudet ska rapportera till och ansvarar för att följa upp dataskyddsarbetet i Norrtälje kommun genom den interna kontrollplanen.

5.1.4 Chef för förvaltning/kontor och kommunala bolag

Chef för förvaltning/kontor eller kommunalt bolag ansvarar för säkerheten inom den egna förvaltningen, kontoret eller bolaget. Ansvaret består dels i att säkerställa att det arbete som bedrivs centralt på förvaltningen/kontoret eller bolaget utförs i enlighet med gällande policys, riktlinjer och anvisningar/rutiner och dels i att säkerställa att avdelnings- och enhetschefer vidtar de åtgärder som krävs för att upprätthålla säkerheten inom deras respektive avdelningar och enheter.

Chef för förvaltning/kontor eller kommunalt bolag har, genom sitt budget- och resursansvar, ett särskilt ansvar för att säkerställa att säkerhetsarbetet inom förvaltningen/kontoret eller bolaget tilldelas de resurser som krävs.

Chef för förvaltning/kontor eller kommunalt bolag ska:

- vid behov, säkerställa att förvaltnings-/bolagsgemensamma anvisningar och rutiner rörande säkerhet tas fram för att förtydliga hur Norrtälje kommuns policys och riktlinjer rörande säkerhet ska efterlevas inom förvaltningen/kontoret eller bolaget.

- i samråd med säkerhetschefen utse en säkerhets- och beredskapssamordnare per förvaltning/kontor eller bolag (se nedan).

- säkerställa att relevanta säkerhetskrav ställs vid upphandling/avrop av varor och tjänster då förvaltningen/kontoret eller bolaget står som beställare samt följa upp leverantörens efterlevnad av ställda krav under hela avtalstiden.

- säkerställa att inträffade säkerhetsincidenter, och uppmärksammade säkerhetsbrister rapporteras i enlighet med gällande policys och riktlinjer.

- säkerställa att säkerhetsarbetet inom förvaltningen/kontoret eller bolaget följs upp i enlighet med den interna kontrollplanen.

5.1.5 Avdelnings- och enhetschefer

Avdelnings- och enhetschefer ansvarar för säkerheten inom den egna avdelningen eller enheten. Ansvaret består dels i att säkerställa att det arbete som bedrivs inom avdelningen/enheten utförs i enlighet med gällande policys, riktlinjer och anvisningar/rutiner och dels i att säkerställa att medarbetare vidtar de åtgärder som krävs för att upprätthålla säkerheten i det dagliga arbetet.

Avdelnings- och enhetschefer ska:

- säkerställa att medarbetare inom avdelningen eller enheten får utbildning i säkerhetsfrågor och har den kunskap som krävs för att upprätthålla säkerheten i det dagliga arbetet.
- säkerställa att relevanta säkerhetskrav ställs vid upphandling/avrop av varor och tjänster då avdelningen/enheten står som beställare samt följa upp leverantörens efterlevnad av ställda krav under hela avtalstiden.
- säkerställa att inträffade säkerhetsincidenter, och uppmärksammade säkerhetsbrister rapporteras i enlighet med gällande policys och riktlinjer.
- säkerställa att säkerhetsarbetet inom avdelningen eller enheten följs upp i enlighet med den interna kontrollplanen.

5.2 Chefer med särskilt säkerhetsansvar

5.2.1 IT-chef

IT-chefen ansvarar för att verksamhet rörande anskaffning, utveckling, förvaltning, drift och avveckling av IT-system, IT-infrastruktur och enheter inom Norrtälje kommun utformas på ett sådant sätt att säkerhetsrelaterade krav hanteras och följs upp. Detta gäller särskilt vid framtagande av processer, rutiner och anvisningar samt övrig dokumentation av beslut och åtgärder. IT-chefen ska även informera och samråda med säkerhetschefen om identifierade behov av ytterligare säkerhetsåtgärder kopplat till Norrtälje kommuns IT-miljö.

5.2.2 HR-direktör

HR-direktören ansvarar för att processer för rekrytering och anställning inom Norrtälje kommun utformas på ett sådant sätt att säkerhetsrelaterade krav hanteras och följs upp. Detta gäller särskilt vid framtagande av processer, rutiner och anvisningar.

5.2.3 Chefen för upphandlingsenheten

Chefen för upphandlingsfunktionen ansvarar för att upphandlingsverksamheten inom Norrtälje kommun utformas på ett sådant sätt att säkerhetsrelaterade krav hanteras och följs upp. Detta gäller särskilt vid framtagande av processer, rutiner och anvisningar.

5.3 Styrande och stödjande roller

5.3.1 Säkerhetschef

Organisationens säkerhetschef har till uppgift att leda och följa upp Norrtälje kommuns säkerhets- och beredskapsarbete. Säkerhetschefen ska även stödja kommundirektören, ledningsgruppen, förvaltnings- och avdelningschefer samt de lokala säkerhets- och beredskapssamordnarna med rådgivning i säkerhetsfrågor.

Säkerhetschefen ska:

- ansvara för beredning vid framtagande och revidering av policys och riktlinjer avseende säkerhet. Gällande dataskydd sker detta i samråd med dataskyddsombudet.

- vid behov ta fram kommunövergripande anvisningar/rutiner i syfte att förtydliga hur policys och riktlinjer ska efterlevas. Gällande dataskydd sker detta i samråd med dataskyddsombudet.

- vid behov fatta beslut i frågor som rör tolkning av gällande policys och riktlinjer avseende säkerhet.

- säkerställa att de säkerhetsanalyser, riskanalyser och säkerhetsrelaterade planer (utbildningsplan och kontrollplan m.m.) som krävs för Norrtälje kommun tas fram.

- säkerställa att rapportering av säkerhetsincidenter och identifierade brister i säkerheten tas omhand på ett systematiskt och effektivt sätt, leder till effektiva åtgärder samt bidrar till Norrtälje kommuns övergripande bild av säkerhetsläget.

- säkerställa att säkerhetsarbetet inom Norrtälje kommun följs upp regelbundet och utvärderas för att säkerställa att det bedrivs långsiktigt och kostnadseffektivt med bibehållen effekt och kvalitet.

5.3.2 Säkerhetsskyddschef

Organisationens säkerhetsskyddschef har till uppgift att leda och följa upp Norrtälje kommuns säkerhetsskyddsarbete. Säkerhetsskyddschefen ska även stödja kommundirektören, ledningsgruppen, förvaltnings- och avdelningschefer samt de lokala säkerhets- och beredskapssamordnarna med rådgivning i säkerhetsskyddsfrågor.

Säkerhetsskyddschefen är direkt underställd kommundirektören i säkerhetsskyddsfrågor.

Säkerhetsskyddschefen ska:

- ansvara för beredning vid framtagande och revidering av policys och riktlinjer avseende säkerhetsskydd.

- vid behov ta fram kommunövergripande anvisningar/rutiner i syfte att förtydliga hur policys och riktlinjer ska efterlevas.

- vid behov fatta beslut i frågor som rör tolkning av gällande policys och riktlinjer avseende säkerhetsskydd.

- säkerställa att säkerhetsskyddsanalys samt säkerhetsskyddsrelaterade planer (utbildningsplan och kontrollplan m.m.) som krävs för Norrtälje kommun tas fram.

- säkerställa att rapportering av säkerhetsskyddsincidenter och identifierade brister i säkerhetsskyddet tas omhand på ett systematiskt och effektivt sätt, leder till effektiva åtgärder.

- säkerställa att säkerhetsskyddsarbetet inom Norrtälje kommun följs upp regelbundet och utvärderas för att säkerställa att det bedrivs långsiktigt och kostnadseffektivt med bibehållen effekt och kvalitet.

5.3.3 Säkerhetsspecialister

Vid säkerhetsfunktionen inom Norrtälje kommun finns utpekade specialister inom följande områden:

- Systematiskt brandskyddsarbete
- Fysisk säkerhet

Specialisterna har till uppgift att stödja verksamheten inom respektive område samt att utverka kravställningar och följa upp efterlevnad.

5.3.4 Dataskyddsombud, DSO

Dataskyddsombudet har en oberoende rådgivande, informerande och övervakande roll avseende dataskydd i Norrtälje kommun och utgör tillsynsmyndighetens förlängda arm i Norrtälje kommun. Dataskyddsombudet stödjer tillsynsmyndigheten vid exempelvis inspektioner och i samråd.

Dataskyddsombudet är Norrtälje kommuns kontaktperson avseende dataskydd gentemot de registrerade (såväl inom Norrtälje kommun som externt), och har i sitt arbete stöd av säkerhets- och beredskapssamordnarna samt av förvaltningsledare, systemägare och objektsägare enligt kommunens systemförvaltningsmodell.

Dataskyddsombudet ska:

- kontrollera att Norrtälje kommun följer lagar, förordningar, föreskrifter och interna styrdokument avseende dataskydd.
- rapportera en lägesbild över dataskyddsarbetet direkt till Norrtälje kommuns ledningsgrupp, minst en gång i kvartalet.
- informera ledningsgrupp och säkerhets- och beredskapssamordnare om förändringar och nyheter avseende dataskydd.
- vid behov ge råd i samband med konsekvensbedömningar.
- initiera och tillhandahålla utbildningar inom dataskydd, på olika nivåer.
- stödja säkerhetschefen i arbetet med framtagande och revidering av policys, riktlinjer och anvisningar/rutiner som berör dataskyddsfrågor.
- säkerställa att rapportering av personuppgiftsincidenter och identifierade brister i dataskyddsarbetet tas omhand på ett systematiskt och effektivt sätt och leder till effektiva åtgärder samt bidrar till Norrtälje kommuns övergripande lägesbild över dataskyddsarbetet.

5.3.5 Säkerhets- och beredskapssamordnare

Samtliga förvaltningar/kontor och bolag inom kommunen ska ha en utpekad säkerhets- och beredskapssamordnare.

Samordnarna arbetar praktiskt med vissa säkerhets- och beredskapsfrågor inom den egna förvaltningen/kontoret/bolaget och fungerar som en länk mellan verksamheten och avdelningen för säkerhet och krisberedskap (vid Trygghets- och Säkerhetskontoret). På uppdrag av ansvarig chef ska dessa samordnare driva de förändringar som krävs i verksamheten för att efterleva policys, riktlinjer och anvisningar avseende säkerhet, beredskap och dataskydd.

Säkerhets- och beredskapssamordnarna ska:

- stödja dataskyddsombudet i arbetet med att följa upp hanteringen av personuppgifter inom verksamheten.
- sprida information som förmedlats av säkerhetschefen eller dataskyddsombudet inom den egna förvaltningen/kontoret eller bolaget.
- kontinuerligt stämma av verksamhetens behov avseende säkerhet och dataskydd och informera ansvarig chef om eventuella behov av ytterligare resurser.
- rapportera avvikelser från policys och riktlinjer till ansvarig chef och vid behov eskalera till säkerhetschefen respektive dataskyddsombudet.
- vid behov delta i samråd och inspektioner mellan verksamheten, dataskyddsombudet och tillsynsmyndigheten.
- stödja säkerhetschefen vid genomförande av kontroller av säkerhetsarbetet.

5.4 Medarbetare

Varje medarbetare ansvarar för att hålla sig informerad om gällande policys, riktlinjer och anvisningar/rutiner rörande säkerhet samt att vidta de åtgärder som krävs för att upprätthålla säkerheten i det dagliga arbetet.

Vid behov vända sig till närmaste säkerhets- och beredskapssamordnare för stöd i säkerhetsfrågor.

Ovanstående krav på medarbetare gäller även praktikanter och andra som deltar i Norrtälje kommuns verksamhet.

5.5 Leverantörer av varor och tjänster

Leverantörer av varor och tjänster till Norrtälje kommun ska säkerställa att den verksamhet bedrivs för Norrtälje kommuns räkning följer gällande policys, riktlinjer och anvisningar/rutiner som reglerar Norrtälje kommuns säkerhetsarbete.

Leverantören ska även säkerställa att samtliga krav på säkerhet som framgår av affärsavtal, säkerhetsskyddsavtal, tilläggsavtal, avrop eller bilagor till avtal efterlevs samt att efterlevnaden kontrolleras regelbundet.

Leverantören ska bereda Norrtälje kommun möjlighet att granska säkerheten rörande den verksamhet som bedrivs för Norrtälje kommuns verksamhet och tillhandahålla den dokumentation som krävs för att Norrtälje kommun ska kunna genomföra en sådan granskning.

Medarbetare anställda vid leverantör som levererar varor eller tjänster till Norrtälje kommun ansvarar för att hålla sig informerad om gällande policys, riktlinjer och anvisningar/rutiner rörande säkerhet samt att vidta de åtgärder som krävs för att upprätthålla säkerheten i det dagliga arbetet.

5.6 Besökare

Övriga personer som kommer i kontakt med Norrtälje kommuns verksamhet, såsom exempelvis besökare, praktikanter, eller kommuninvånare i övrigt, ska följa de anvisningar om säkerhet som finns i Norrtälje kommuns olika lokaler.

5.7 Kommunens systemförvaltningsmodell

Utöver ovanstående roller beskrivs roller och ansvar avseende kravställning och utförande av säkerhetsåtgärder kopplat till IT-system i Norrtälje kommuns systemförvaltningsmodell. I systemförvaltningsmodellen regleras bland annat informationsägarens kravställande roll, och systemförvaltarens utförande roll, vad gäller informationssäkerhet (såväl konfidentialitet, som riktighet och tillgänglighet samt spårbarhet) för de system i kommunens IT-miljö som ska hantera en viss informationsmängd. IT-funktionen i Norrtälje kommun ansvarar för att upprätthålla dokumentation kring systemförvaltningsmodellen.

6 Behörigheter

För att medarbetare, leverantörer och förtroendevalda ska kunna delta i Norrtälje kommuns verksamhet krävs att de har tilldelats rätt behörigheter. Behörighet krävs exempelvis för att få tillgång till Norrtälje kommuns information och IT-miljö samt för att få tillträde till Norrtälje kommuns lokaler. Behörigheter tilldelas restriktivt baserat på behov i tjänst/uppdrag.

Indelning och tilldelning av behörigheter ska alltid utgå ifrån verksamhetens behov av tillgång och säkerhet.

Behörigheter till information såväl som till system och lokaler kan komma att spärras om det finns anledning att anta att de har missbrukats (exempelvis då en behörighet har använts av flera personer).

6.1 Tilldelning av behörigheter

Behörigheter inom kommunen tilldelas enligt följande:

6.1.1 Behörighet till Norrtälje kommuns information

Behörighet till information som klassificerats som intern tilldelas då anställning eller uppdrag påbörjas och gäller till dess att anställning eller uppdrag avslutas.

Behörighet till information som klassificerats som känslig tilldelas baserat på befattning och gäller längst under en period av 12 månader.

Behörighet till information som klassificerats som begränsat hemlig eller högre ges efter genomförd säkerhetsprövning, inplacering i säkerhetsklass samt genomförd säkerhetsskyddsutbildning. Krav på skriftligt beslut om behörighet fattad av säkerhetsskyddschefen. Behörigheten gäller så länge som behovet kvarstår, dock längst under en period av 12 månader.

6.1.2 Behörighet till Norrtälje kommuns IT-miljö

Behörighet till IT-system godkända för hantering av information som klassificerats som öppen eller intern tilldelas då anställning eller uppdrag påbörjas och gäller till dess att anställning eller uppdrag avslutas.

Behörighet till IT-system godkända för hantering av information som klassificerats som känslig tilldelas baserat på befattning och gäller längst under en period av 12 månader.

6.1.3 Behörighet till Norrtälje kommuns lokaler

Behörighet till lokaler i behörighetszon ”2 – Gul zon”, tilldelas då anställning eller uppdrag påbörjas och gäller till dess att anställning eller uppdrag avslutas.

Behörighet till lokaler i behörighetszon ”3 – Röd zon” tilldelas baserat på befattning och gäller tills behovet i tjänsten upphör, men som längst under en period av 12 månader.

Samtliga behörigheter ska omprövas regelbundet. Behörig utdelare av behörigheter ska vända sig till berörda chefer och säkerställa att behovet av behörighet kvarstår.

6.1.4 Revidering av tilldelade behörigheter

Tilldelade behörigheter ska regelbundet omprövas för att säkerställa att behovet kvarstår. Om behovet inte kvarstår ska behörigheten återkallas omgående.

Behörigheter ska omprövas minst en gång per år, samt då anställningar eller uppdrag förändras eller avslutas, av den chef som tilldelat behörigheten.

7 Handlingssekretess och tystnadsplikt

Den som är anställd i Norrtälje kommun eller på annat sätt deltar i Norrtälje kommuns verksamhet (exempelvis i egenskap av anställd hos leverantör till Norrtälje kommun) omfattas av förbudet mot att röja uppgifter som omfattas av sekretess (tystnadsplikt och handlingssekretess) som framgår av offentlighets- och sekretesslagen.

Sekretessen gäller mot enskilda (personer och företag) och andra myndigheter[3] (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 organisationer.

[3] Observera att Norrtälje kommun består av flera separata myndigheter.

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 av tryckfrihetsförordningen och yttrandefrihetsgrundlagen (den så kallade meddelarfriheten).

Handlingssekretess innebär att en person inte har rätt att lämna ut handlingar som innehåller uppgifter som omfattas av sekretess till obehöriga[4]. 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, får uppgiften inte heller i övrigt utnyttjas utanför den verksamhet för vilken den är sekretessreglerad.

7.1 Sekretessförbindelse

Samtliga personer som deltar i Norrtälje kommuns verksamhet ska informeras om tystnadsplikten och handlingssekretessen och teckna en sekretessförbindelse som tydligt visar att de har delgivits informationen.

Sekretessförbindelsen sparas hos Norrtälje kommun. För anställda gäller att sekretessförbindelsen förvaras i personalakten.

Tecknande av sekretessförbindelse ska ske innan en person ges behörighet att ta del av uppgifter som omfattas av sekretess (informationssäkerhetsklass intern eller högre).

8 Informationssäkerhet

8.1 Informationsklassificering

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

8.1.1 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 Norrtälje kommuns IT-miljö, är konfidentialitet en angelägenhet för alla som kommer i kontakt med Norrtälje kommuns 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.

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

- **Informationssäkerhetsklass ”INTERN”**
  Med intern information avses uppgifter som behöver ges ett grundläggande skydd mot obehörig åtkomst. All information som förekommer i Norrtälje kommuns IT-miljö och som inte är öppen eller känslig är att betrakta som intern. Hit räknas uppgifter som omfattas av svag sekretess (rakt skaderekvisit). Hit räknas även personuppgifter som i normalfallet[5] inte är att betrakta som känsliga.

- **Informationssäkerhetsklass ”KÄNSLIG”**
  Med känslig information avses uppgifter som behöver ges ett särskilt skydd då obehörig åtkomst till uppgifterna skulle kunna innebära allvarliga konsekvenser för Norrtälje kommun eller enskilda. Hit räknas uppgifter som omfattas av stark sekretess (omvänt skaderekvisit) eller absolut sekretess och uppgifter som bedöms vara av särskilt intresse för obehöriga. Hit räknas även personuppgifter som i normalfallet[6] är att betrakta som känsliga.

- **Informationssäkerhetsklass ”BEGRÄNSAT HEMLIG”**
  Med begränsat hemlig information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, där obehörigt röjande av uppgifterna kan medföra ringa skada för Sveriges säkerhet.

- **Informationssäkerhetsklass ”KONFIDENTIELL”**
  Med konfidentiell information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, där obehörigt röjande av uppgifterna kan medföra en inte obetydlig skada, för Sveriges säkerhet.

- **Informationssäkerhetsklass ”HEMLIG”**
  Med hemlig information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, där obehörigt röjande av uppgifterna kan medföra en allvarlig skada för Sveriges säkerhet.

- **Informationssäkerhetsklass ”KVALIFICERAT HEMLIG”**
  Med kvalificerat hemlig information avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, där obehörigt röjande av uppgifterna kan medföra en synnerligen allvarlig skada för Sveriges säkerhet.

8.1.2 Riktighet

Informationens riktighet är avgörande för såväl Norrtälje kommuns verksamhet som allmänheten och medias förtroende för kommunen. Riktigheten säkerställs främst genom en strikt tillämpning av behörighet att påverka informationsmängder i Norrtälje kommuns IT-miljö och åtgärder för att säkerställa spårbarhet (och därmed möjlighet att utkräva ansvar) då åtgärder vidtas i IT-miljön (se även rubriken *Spårbarhet* nedan).

[5] Bedömningen av huruvida en personuppgift är känslig måste alltid ske från fall till fall.
[6] Bedömningen av huruvida en personuppgift är känslig måste alltid ske från fall till fall.

8.1.3 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 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 Norrtälje kommuns 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 verksamhetskritiska informationen hålls tillgänglig även om IT-miljön är otillgänglig (exempelvis genom att tillhandahålla utskrifter av viss information).

Ett SLA (Service Level Agreement) som reglerar krav på tillgänglighet för system, molntjänster och applikationer ska tecknas i varje enskilt fall då Norrtälje kommun nyttjar system, molntjänster eller applikationer som tillhandahålls av en leverantör. Även då system och applikationer tillhandahålls av kommunens egen IT-avdelning ska ett SLA tecknas. Kommunens IT-avdelning ansvarar för att SLA tecknas i varje enskilt fall. Verksamheter som är beroende av det system, den molntjänst eller den applikation som SLA berör ska kravställa vilken nivå av tillgänglighet som är acceptabel. Kommunens säkerhetsfunktion följer upp att tecknade SLA lever upp till ställda krav på kommunens verksamhet.

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

- **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 Norrtälje kommuns IT-infrastruktur alternativt för intern/extern kommunikation m.m. Åtgärder för att avhjälpa avbrott ska vidtas inom fyra timmar.

8.1.4 Spårbarhet

Att säkerställa informationens konfidentialitet, riktighet och tillgänglighet i Norrtälje kommuns 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. 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**
  Organisationens basnivå för loggning av system och tjänster. Åtgärder som vidtas för att uppfylla krav på begränsad spårbarhet beskrivs i Norrtälje kommuns 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 Norrtälje kommuns dokumentation av IT-säkerhetsåtgärder.

8.2 Informationshantering (hantering av dokument och lagringsmedia)

Nedan redogörs för de krav som ställs vid hantering av dokument och lagringsmedia innehållande Norrtälje kommuns information. Vilka krav som ställs på hanteringen bestäms av informationens informationssäkerhetsklass som i sin tur utgår ifrån behovet av konfidentialitet för den mest skyddsvärda uppgiften som ingår ett dokument eller ett lagringsmedium.

För en förenklad och överskådlig beskrivning av nedanstående hanteringsregler, se dokumentet ”Anvisning för informationshantering”.

8.2.1 Märkning

Dokument som innehåller ÖPPEN information behöver inte märkas med informationssäkerhetsklass. Märkning med ÖPPEN får dock ske om behov föreligger.

Dokument som innehåller INTERN information ska förses med texten INTERN INFORMATION i sidhuvud och/eller sidfot, samt vid behov förses med en sekretessmarkering som innehåller tillämplig paragraf i offentlighets- och sekretesslagen samt datum för handlingens upprättande och NORRTÄLJE KOMMUN i svart.

Dokument som innehåller KÄNSLIG information ska förses med texten KÄNSLIG INFORMATION i sidhuvud och/eller sidfot, samt vid behov förses med en sekretessmarkering som innehåller tillämplig paragraf i offentlighets- och sekretesslagen samt datum för handlingens upprättande och NORRTÄLJE KOMMUN i svart.

Dokument som innehåller BEGRÄNSAT HEMLIG information ska förses med texten BEGRÄNSAT HEMLIG INFORMATION i rött längst till vänster i sidhuvud och sidfot. Om handlingen är upprättad av Norrtälje kommun ska detta tydligt framgå samt datum för upprättande.

Dokument som innehåller KONFIDENTIELL information ska förses med texten KONFIDENTIELL INFORMATION i rött längst till vänster i sidhuvud och sidfot. Om handlingen är upprättad av Norrtälje kommun ska detta tydligt framgå samt datum för upprättande. I förekommande fall även antal sidor och uppgifter om bilagor.

Dokument som innehåller HEMLIG information ska förses med texten HEMLIG INFORMATION i rött längst till vänster i sidhuvud och sidfot. Om handlingen är upprättad av Norrtälje kommun ska detta tydligt framgå, likväl som datum för upprättande och exemplarnummer. I förekommande fall ska antal sidor och uppgifter om bilagor också finnas med.

Dokument som innehåller KVALIFICERAT HEMLIG information ska förses med texten KVALIFICERAT HEMLIG INFORMATION i rött längst till vänster i sidhuvud och sidfot. Om handlingen är upprättad av Norrtälje kommun ska detta tydligt framgå, likväl som datum för upprättande och exemplarnummer. I förekommande fall ska antal sidor och uppgifter om bilagor också finnas med.

Lagringsmedia som innehåller, eller har innehållit, ÖPPEN information ska vara märkt så att det framgår att den tillhör Norrtälje kommun.

Lagringsmedia som innehåller, eller har innehållit, INTERN information ska vara märkt så att det framgår att den tillhör Norrtälje kommun samt förses med texten INTERN INFORMATION väl synligt.

Lagringsmedia som innehåller, eller har innehållit, KÄNSLIG information ska vara märkt så att det framgår att den tillhör Norrtälje kommun samt förses med texten KÄNSLIG INFORMATION väl synligt.

Lagringsmedia som innehåller, eller har innehållit, BEGRÄNSAT HEMLIG ska förses med texten BEGRÄNSAT HEMLIG och tydligt framgå att det tillhör Norrtälje kommun.

Lagringsmedia som innehåller, eller har innehållit, KONFIDENTIELL information ska förses med texten KONFIDENTIELL och tydligt framgå att det tillhör Norrtälje kommun. Lagringsmediet ska även märkas med identitetsuppgift (exempelvis serienummer).

Lagringsmedia som innehåller, eller har innehållit, HEMLIG information ska förses med texten HEMLIG och tydligt framgå att det tillhör Norrtälje kommun. Lagringsmediet ska även märkas med identitetsuppgift (exempelvis serienummer).

Lagringsmedia som innehåller, eller har innehållit, KVALIFICERAT HEMLIG information ska förses med texten KVALIFICERAT HEMLIG och tydligt framgå att det tillhör Norrtälje kommun. Lagringsmediet ska även märkas med identitetsuppgift (exempelvis serienummer).

8.2.2 Registrering

Krav på registrering av dokument styrs dels av klassificeringen av den information som förekommer i dokumentet och dels av huruvida dokumentet utgör en allmän handling[7].

Allmänna handlingar som innehåller ÖPPEN information har inga särskilda krav på registrering, utöver gällande generella krav på registrering av allmänna handlingar.

Allmänna handlingar som innehåller INTERN eller KÄNSLIG information registreras vid registraturen hos det förvaltningskontor där handlingarna förvaras.

[7] För mer information om hantering av allmänna handlingar, se kommunens dokumenthanteringsplaner.

Allmänna handlingar som innehåller BEGRÄNSAT HEMLIG information eller högre ska vara registrerade vid registraturen.

Lagringsmedia som endast innehåller, eller har innehållit ÖPPEN information behöver inte vara registrerade[8].

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som INTERN eller KÄNSLIG ska vara registrerade i förteckning hos IT-funktionen.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som BEGRÄNSAT HEMLIG eller högre ska vara registrerade i förteckning vid registraturen.

8.2.3 Kvittens

Dokument innehållande information klassificerad som KONFIDENTIELL eller högre ska kvitteras via registraturen.

Lagringsmedia som innehåller, har innehållit eller är avsedda att innehålla information klassificerad som INTERN eller KÄNSLIG ska kvitteras via IT-funktionen. Kvittens sker i enlighet med rutiner upprättade av IT-funktionen inom ramen för dessa riktlinjer.

Lagringsmedia som innehåller, har innehållit eller är avsedda att innehålla information klassificerad som BEGRÄNSAT HEMLIG eller högre ska kvitteras via registraturen.

8.2.4 Inventering

Dokument innehållande information klassificerad som KONFIDENTIELL eller HEMLIG ska inventeras årligen[9] . Inventeringen ska dokumenteras.

Dokument innehållande KVALIFICERAT HEMLIG information ska inventeras av registrator tillsammans med säkerhetschefen, minst årligen. Inventeringen ska dokumenteras.

Lagringsmedia som innehåller eller har innehållit information klassificerad som INTERN eller KÄNSLIG ska inventeras då anställning eller uppdrag upphör.

Lagringsmedia som innehåller eller har innehållit information klassificerad som BEGRÄNSAT HEMLIG ska inventeras vid återlämning.

Lagringsmedia som innehåller eller har innehållit information klassificerad som KONFIDENTIELL eller HEMLIG information ska inventeras årligen. Inventeringen ska dokumenteras.

Lagringsmedia som innehåller eller har innehållit, information klassificerad som KVALIFICERAT HEMLIG information ska inventeras av registrator tillsammans med säkerhetschefen, minst årligen. Inventeringen ska dokumenteras.

[8] Lagringsmedia måste däremot, oavsett klass på informationen, alltid vara godkänt för användande i kommunens IT-miljö.
[9] Gäller inte arkivlagda handlingar.

8.2.5 Kopiering av dokument

Kopiering av dokument innehållande ÖPPEN information får ske utan begränsningar utöver upphovsrätten.

Kopiering av dokument innehållande INTERN eller KÄNSLIG information får endast ske på de kopiatorer/multifunktionsskrivare som Norrtälje kommun tillhandahåller.

Dokument innehållande information klassificerad som BEGRÄNSAT HEMLIG, KONFIDENTIELL eller HEMLIG får endast inlämnas till registraturen för kopiering.

Dokument innehållande information klassificerad som KVALIFICERAT HEMLIG får inte kopieras och utdrag får inte göras.

8.2.6 E-post till intern mottagare

Information klassificerad som ÖPPEN eller INTERN får skickas med e-post till interna mottagare (adress som slutar på @norrtalje.se). Avsändaren ansvarar för att säkerställa att informationen endast skickas till interna mottagare som är behöriga att ta del av den.

Information klassificerad som KÄNSLIG får endast skickas via e-post till interna mottagare (adress som slutar på @norrtalje.se) via den tjänst som kommunen godkänt för säker e-post (Säkra Meddelanden), dit mottagaren loggar in med bank-ID/mobilt bank-ID. Detta för att säkerställa att endast avsedd mottagare får del av informationen.

Information klassificerad som BEGRÄNSAT HEMLIG eller högre får inte skickas med e-post.

8.2.7 E-post till extern mottagare

Information klassificerad som ÖPPEN får skickas till externa mottagare (adress som inte slutar på @norrtalje.se) utan begränsningar.

Information klassificerad som INTERN får skickas till externa mottagare via e-post. Avsändaren ansvarar för att säkerställa att informationen endast skickas till mottagare som är behöriga att ta del av den.

Information klassificerad som KÄNSLIG får endast skickas via e-post till externa mottagare (adress som inte slutar på @norrtalje.se) via den tjänst som kommunen godkänt för säker e-post (Säkra Meddelanden), dit mottagaren loggar in med bank-ID/mobilt bank-ID. Detta för att säkerställa att endast den avsedda mottagaren får del av informationen.

Information klassificerad som BEGRÄNSAT HEMLIG eller högre får inte skickas med e-post.

8.2.8 Intern distribution (internpost)

Dokument innehållande ÖPPEN eller INTERN information får skickas med internpost utan begränsningar.

Dokument innehållande KÄNSLIG information får endast skickas med internpost i förseglade kuvert. Avsändaren ansvarar för att säkerställa att endast den avsedda mottagaren får del av informationen.

Dokument innehållande information som klassificerats som BEGRÄNSAT HEMLIG eller högre får inte skickas med internpost. All distribution ska ske via registraturen.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som INTERN eller KÄNSLIG får inte distribueras via internpost. All distribution ska ske via IT.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som BEGRÄNSAT HEMLIG eller högre får inte distribueras via internpost. All distribution ska ske via registraturen.

8.2.9 Extern distribution (postförsändelser)

Dokument innehållande ÖPPEN information får skickas med postförsändelse utan begränsningar.

Dokument innehållande INTERN information får endast skickas med postförsändelse i förseglade kuvert. Avsändaren ansvarar för att säkerställa att endast den avsedda mottagaren får del av informationen.

Dokument innehållande KÄNSLIG information får endast skickas med rekommenderat brev (REK) i förseglade säkerhetskuvert (säkerhetspåse). Avsändaren ansvarar för att säkerställa att endast den avsedda mottagaren får del av informationen.

Dokument innehållande information som klassificerats som BEGRÄNSAT HEMLIG eller högre får inte skickas med postförsändelse. All distribution ska ske via registraturen.

Lagringsmedia som innehåller ÖPPEN information får skickas med postförsändelse utan begränsningar.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som INTERN eller KÄNSLIG får inte distribueras via postförsändelse. All distribution ska ske via IT-funktionen.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som BEGRÄNSAT HEMLIG eller högre får inte distribueras via postförsändelse. All distribution ska ske via registraturen.

8.2.10 Medförande utanför Norrtälje kommuns lokaler

ÖPPEN information får medföras utanför Norrtälje kommuns lokaler utan begränsningar.

INTERN information får medföras utanför Norrtälje kommuns lokaler då behov i tjänsten föreligger.

KÄNSLIG information får medföras utanför Norrtälje kommuns lokaler av den som är behörig att hantera informationen då det är absolut nödvändigt för tjänsteutövningen efter beslut av ansvarig chef. Ett sådant beslut kan avse enskilda individer eller en viss verksamhet och får längst vara giltigt i ett år.

BEGRÄNSAT HEMLIG information får endast i undantagsfall föras utanför kommunens lokaler av den som är behörig att ta del av informationen om det är absolut nödvändigt för tjänsteutövningen.

Information klassificerad som KONFIDENTIELL eller HEMLIG får endast medföras utanför Norrtälje kommuns lokaler efter beslut av säkerhetschefen. Ett sådant beslut ska avse en specifik individ och ett specifikt ändamål.

Information klassificerad som KVALIFICERAT HEMLIG får inte medföras utanför Norrtälje kommuns lokaler.

8.2.11 Distansarbete

Distansarbete som innebär hantering av information klassificerad som ÖPPEN får ske utan begränsningar.

Distansarbete som innebär hantering av information klassificerad som INTERN får ske under förutsättning att den som hanterar informationen säkerställer att ingen obehörig kan ta del av informationen (exempelvis genom att säkerställa att arbetsplatsen är insynsskyddad och att samtal inte kan överhöras).

Distansarbete som innebär hantering av information klassificerad som KÄNSLIG får ske på en plats som har motsvarande säkerhet som den ordinarie arbetsplatsen (exempelvis i en anställds bostad).

Distansarbete som innebär hantering av information klassificerad som BEGRÄNSAT HEMLIG eller högre är inte tillåtet.

8.2.12 Återlämning

Allmänna handlingar innehållande information som klassificerats som ÖPPEN, INTERN eller KÄNSLIG ska återlämnas till registrerande verksamhet senast då anställning eller uppdrag avslutas.

Dokument innehållande information som klassificerats som BEGRÄNSAT HEMLIG eller högre ska återlämnas till registraturen så snart den som kvitterat handlingarna inte längre har behov av dem i tjänsten.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som INTERN eller KÄNSLIG ska återlämnas till IT då de inte längre behövs i verksamheten, men senast i samband med att anställning/uppdrag upphör. Återlämning sker i enlighet med av IT specificerade rutiner.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som BEGRÄNSAT HEMLIG eller högre ska återlämnas till registraturen så snart den som kvitterat lagringsmediet inte längre har behov av dem i tjänsten.

8.2.13 Gallring

För information om regler för gallring av allmänna handlingar se Norrtälje kommuns arkivreglemente och aktuella dokumenthanteringsplaner.

8.2.14 Återanvändning av lagringsmedia

Lagringsmedia som innehåller, eller har innehållit, öppen information får återanvändas inom Norrtälje kommuns verksamhet utan begränsningar.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som INTERN eller KÄNSLIG får återanvändas inom Norrtälje kommuns verksamhet efter att de återlämnats till IT-funktionen och skrivits över med en av Norrtälje kommun godkänd programvara.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som BEGRÄNSAT HEMLIG eller högre får inte återanvändas, utan ska destrueras efter återlämning till registraturen.

8.2.15 Destruktion

Nedanstående regler gäller endast dokument som INTE utgör allmänna handlingar. Eventuell destruktion av allmänna handlingar hanteras av registratur och arkiv i samband med gallring.

Dokument innehållande ÖPPEN information behöver inte destrueras innan de lämnas till återvinning.

Dokument innehållande INTERN eller KÄNSLIG information destrueras genom att lämnas i de förslutna kärl (sekretesstunnor) som Norrtälje kommun tillhandahåller.

Dokument innehållande BEGRÄNSAT HEMLIG information destrueras i en destruktör som uppfyller kraven enligt lägst DIN 66399 Level 5.

Dokument innehållande information som klassificerats som KONFIDENTIELL eller högre destrueras av medarbetare vid registratur efter återlämnande.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som ÖPPEN behöver inte destrueras.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som INTERN eller KÄNSLIG ska destrueras så att data inte går att återskapa. Sådan destruktion kan ske genom mekanisk förstöring (fragmentering) i mobil destruktionsanläggning[10], alternativt genom att avmagnetiseras med hjälp av en s.k. ”degausser” (utrustning för avmagnetisering) som Norrtälje kommun godkänt för ändamålet. Destruktion av lagringsmedia som innehåller/innehållit INTERN eller KÄNSLIG information hanteras av IT-funktionen.

Lagringsmedia som innehåller, eller har innehållit, information klassificerad som BEGRENSAT HEMLIG eller högre destrueras av medarbetare vid registratur efter återlämnande.

8.3 Säkerhet i Norrtälje kommuns IT-miljö

Att upprätthålla ändamålsenlig informationssäkerhet för Norrtälje kommuns information är särskilt viktigt då informationen hanteras i IT-system.

Den grundläggande principen är att Norrtälje kommuns utrustning (datorer, mobiltelefoner och surfplattor m.m.) och de IT-system och applikationer som Norrtälje kommun tillhandahåller (såväl fysiska som virtuella system och molnbaserade tjänster) ska

[10] Behörig person måste övervaka destruktionen och säkerställa resultatet.

användas för att hantera Norrtälje kommuns information. Undantag från denna regel ska beslutas av säkerhetschefen efter samråd med verksamheten och IT.

Utöver nedanstående generella krav på IT- och kommunikationssäkerhet regleras Norrtälje kommuns IT-säkerhet i de anvisningar och rutiner som tas fram av IT[11] inom ramen för gällande riktlinjer.

8.3.1 Anskaffning, utveckling och underhåll av system

Samtliga användarenheter och lagringsmedia som används för att hantera Norrtälje kommuns information ska vara godkända för ändamålet av kommunens organisation.

Samtliga IT-system, applikationer och molntjänster som används för att hantera Norrtälje kommuns information ska vara godkända för ändamålet av kommunens organisation. Det ska även finnas ett avtal som reglerar användandet av systemet, applikationen eller molntjänsten samt ägande och regler för nyttjande av informationen som Norrtälje kommun hanterar. Avtalskravet gäller *även* för gratistjänster.

IT-funktionen ansvarar för att föra register över befintliga användarenheter och lagringsmedia som används inom Norrtälje kommun. Undantaget detta är enheter och lagringsmedia som är avsedda för att hantera information klassificerad som BEGRÄNSAT HEMLIG eller högre, dessa ska istället vara registrerade vid registraturen.

IT-funktionen ansvarar för att upprätthålla register över IT-system, applikationer och molntjänster (såväl inom som utanför Norrtälje kommuns IT-miljö) som är godkända för att hantera Norrtälje kommuns information samt uppgifter om vilken informationsklass som respektive system, applikation eller tjänst är godkänd för att behandla. Innan ett IT-system, en applikation eller en molntjänst nyttjas för att hantera Norrtälje kommuns information ska ett beslut om driftgodkännande fattas av IT-funktionen. Driftgodkännandet ska baseras på den kravställning som ligger till grund för att bedöma behov av konfidentialitet, riktighet och tillgänglighet som krävs för informationen som systemet eller tjänsten ska hantera utifrån föreliggande krav och verksamheten behov.

Inom Norrtälje kommun ska det finnas på förhand definierade typlösningar (säkerhetsnivåer) för systemsäkerhet som tagits fram utifrån verksamhetens varierande behov samt med stöd av systemet ”KLASSA” i syfte att underlätta kravställningen för verksamheten i samband med IT-projekt.

Säkerheten ska särskilt uppmärksammas i samband med utvecklingsprojekt. All användning av testdata ska föregås av en dokumenterad riskbedömning. I första hand ska information som klassificerats som ÖPPEN användas som testdata, alternativt kan anonymiserad information användas. Som sista alternativ kan information klassificerad som INTERN användas, under förutsättning att den är att betrakta som pseudonymiserad (inte är direkt identifierbar utan tillgång till ytterligare information). Information klassificerad som KÄNSLIG eller högre får inte användas som testdata.

Det är alltid de verksamheter inom Norrtälje kommun som ska nyttja ett IT-system som kravställer såväl funktionskrav som krav på säkerhet (såväl konfidentialitet som riktighet och tillgänglighet). Ansvarig chef för respektive verksamhet som ska nyttja systemet, eller

[11] Det gäller exempelvis detaljerade krav på kryptering, konfiguration, loggning och säkerhetskopiering som förändras över tid beroende på förändrad risk och hotbild och teknikutvecklingen.

den som chefen utser, ska delta i arbetet med att fastställa säkerhetskrav för systemet. IT-funktionen samordnar kravfångstarbetet och föreslår en lämplig säkerhetslösning utifrån ställda krav.

Kommunen har inte implementerat hårddiskkryptering för samtliga användarenheter. Därmed får lagring av information klassificerad som KÄNSLIG inte ske lokalt. Denna lösning kan komma att ändras på sikt, om heltäckande kryptering av användarenheter införs.

Filer och lagringsytor som innehåller information klassificerad som INTERN eller KÄNSLIG ska vara krypterade med av Norrtälje kommun godkänt krypto. För enskilda filer finns möjligheten att kryptera med BitLocker.

Lagringsmedia, filer och lagringsytor som innehåller, eller har innehållit, information klassificerad som BEGRÄNSAT HEMLIG eller högre får endast krypteras med krypto som godkänts av Försvarsmakten för den aktuella informationsklassen.

Samtliga backuper som förvaras hos extern part ska vara krypterade med metod som godkänts av Norrtälje kommuns säkerhetschef.

8.3.2 Driftsäkerhet

IT-funktionen ansvarar för att upprätthålla rutiner för driftsäkerhet avseende Norrtälje kommuns IT-miljö, samt tillse att dessa finns dokumenterade.

IT-funktionen ansvarar för att säkerställa att det finns fastställda processer för att skydda Norrtälje kommuns IT-miljö och användarutrustning mot skadlig kod samt att det finns rutiner för att hålla skyddet uppdaterat skydd mot skadlig kod.

IT ansvarar för att dokumentera behov av säkerhetskopiering för samtliga system och utrustningar som hanterar Norrtälje kommuns information.

Kommunens organisation kan komma att logga samtliga aktiviteter i Norrtälje kommuns IT-miljö och i de molntjänster som hanterar Norrtälje kommuns information samt i användarenheter (såväl bärbara datorer som mobiltelefoner och surfplattor). Syftet med loggningen är att säkerställa efterlevnad av säkerhetsregler, identifiera sårbarheter och att kunna utreda eventuella incidenter.

IT ansvarar för att löpande utvärdera förekomst av tekniska sårbarheter i Norrtälje kommuns IT-miljö och användarutrustning samt att säkerställa att identifierade tekniska sårbarheter hanteras skyndsamt. Vid upptäckt av tekniska sårbarheter av allvarlig karaktär ska Norrtälje kommuns säkerhetschef informeras.

IT ansvarar för att upprätthålla en plan för genomförande av revisioner av IT-säkerheten i Norrtälje kommuns system.

8.3.3 Säkerhet för användarutrustning (datorer, mobiltelefoner, surfplattor)

Endast utrustning som godkänts av Norrtälje kommun får användas för att hantera Norrtälje kommuns information. All godkänd utrustning ska finnas registrerad i ett register som IT ansvarar för att upprätthålla.

All Norrtälje kommuns IT-utrustning ska så långt som möjligt vara stöldskyddsmärkt för att minska stöldrisken och underlätta återtagande.

Användarutrustning ska, vid leverans till användare, vara konfigurerad så att inloggning med lösenord krävs vid uppstart, samt då viloläge avaktiveras och skärmlås ska aktiveras automatiskt efter en fastställd tidsintervall. Användare ska normalt inte ges administratörsrättigheter på utrustningen.

Mobil användarutrustning (exempelvis mobiltelefoner och surfplattor) ska, om möjligt, vara försedd med en aktiverad funktion för fjärradering i syfte att begränsa risken för informationsförluster då utrustning blir stulen eller förkommer.

Säkerhetskopiering av mobiltelefoner i molntjänster ska begränsas till den information som inte finns säkerhetskopierad i andra system. Organisationens mejlkonton säkerhetskopieras redan centralt i MS Office 365 och behöver därför inte kopieras till andra molntjänster och riskera att spridas mer än nödvändigt.

Samtliga användarkonton till Norrtälje kommuns IT-miljö samt system och molntjänster ska vara personliga och ägs av Norrtälje kommun. Privata konton får inte användas inom Norrtälje kommuns verksamhet. Organisationen äger rätt att spärra eller radera kommunägda konton vid behov samt att radera eller begränsa säkerhetskopior för konton.

8.3.4 Avveckling av system, utrustning och lagringsmedia

När system, utrustning eller lagringsmedia som har innehållit information tillhörande Norrtälje kommun avvecklas ska den ansvarige för avvecklingen säkerställa att de hanteras på ett sätt som innebär att information inte sprids till obehöriga personer.

Vilka krav som ställs vid avvecklingen beror på den högst klassificerade informationen som har hanterats.

8.4 Kommunikationssäkerhet

Organisationen förlitar sig främst på mobiltelefoni, e-post och fax samt radiosystemet Rakel för att kommunicera internt och externt.

Mobiltelefoni, fax samt Rakel är godkänt för hantering av information klassificerad upp t.o.m. KÄNSLIG. Detta under förutsättning att skydd mot insyn och överhörning säkerställts.

E-post till/från såväl interna adresser (adresser som slutar på @norrtalje.se) som externa adresser är godkänt för hantering av information klassificerad upp t.o.m. INTERN. Kommunen nyttjar en separat tjänst (Säkra Meddelanden) som möjliggör e-post med KÄNSLIG information, detta för att säkerställa att endast den avsedda mottagaren får del av informationen. Användandet av tjänsten ”Säkra Meddelanden” gäller för både intern och extern e-post när KÄNSLIG information ska skickas.

8.5 Skydd mot informationspåverkan

Med informationspåverkan avses i detta fall olika typer av påverkanskampanjer som utförs av en aktör riktat mot Norrtälje kommun. Med påverkanskampanjer avses koordinerad verksamhet som en aktör bedriver och som innefattar spridande av

vilseledande eller oriktig information. Påverkanskampanjer kan även innefatta annat för ändamålet särskilt anpassat agerande som syftar till att påverka politiska beslut, opinioner eller annan typ av beslutsfattande av offentliga verksamheter.

Åtgärder som syftar till att skydda kommunen mot informationspåverkan regleras huvudsakligen i Norrtälje kommuns riktlinje för beredskap.

9 Säkerhet i Norrtälje kommuns lokaler

Att Norrtälje kommuns lokaler har ändamålsenlig säkerhet är 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.

9.1 Tillträdesbegränsning

Tillträdesbegränsningen för Norrtälje kommuns lokaler regleras efter varje verksamhets behov av nivå på säkerhet och tillträde. Tre olika grundnivåer på behörighetszoner finns dock definierade att utgå ifrån.

Samma lokal kan bestå av en eller flera behörighetszoner.

9.1.1 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.

9.1.2 Zon 2 – gul zon

Gul zon avser lokal, eller del av lokal, dit Norrtälje kommuns medarbetare 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.

9.1.3 Zon 3 – röd zon

Röd zon avser lokal, eller del av lokal, dit endast vissa medarbetare 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. Röd zon kan exempelvis utgöras av datahallar, korskopplingsutrymmen (utrymmen avsedda för teknisk infrastruktur) eller kontorslokaler där särskilt skyddsvärd verksamhet bedrivs.

9.2 ID-kort och behörigheter till lokaler

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

9.2.1 Beställning av ID-kort

Kommunens ID-kort med tillhörande behörigheter för tillträde till lokaler beställs av närmaste chef, alternativt av projektledare eller motsvarande ansvarig person då det gäller leverantörer.

Beställningen läggs till fastighetsavdelningen alternativt den lokala administratören.

Beställande chef eller projektledare ansvarar för att tilldelningen av behörigheter sker baserat på ett faktiskt behov i tjänsten eller uppdraget. För icke-anställda (leverantörer, förtroendevalda) ska tilldelningen av behörigheter tidsbegränsas till den tid som uppdraget genomförs. Även föreningsmedlemmar som nyttjar kommunens lokaler ska ha tidsbegränsade behörigheter.

9.2.2 Utfärdande av ID-kort

Organisationens ID-kort med tillhörande behörigheter för tillträde till lokaler utfärdas av fastighetsavdelningen eller den lokala administratören för kontoret.

Fastighetsavdelningen eller den utfärdande administratören ansvarar också för dokumentation av utfärdade ID-kort och behörigheter.

9.2.3 Återlämnande av ID-kort

Vid avslutad tjänst eller uppdrag ska ansvarig chef eller projektledare anmäla till fastighetsavdelningen eller den utfärdande administratören att återtagande av behörigheter ska ske.

Fastighetsavdelningen eller den utfärdande administratören ansvarar för att vid anmälan återta givna behörigheter.

Ovanstående gäller även då en redan anställd byter tjänst eller arbetsplats inom kommunen, som kräver ändrade (minskade eller utökade) behörigheter.

9.3 Säker arbetsplats

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

9.3.1 Möjlighet att hantera skyddsvärda tillgångar

En arbetsplats där information som klassificerats som INTERN hanteras ska vara insynsskyddad mot ytor som definierats i nivå med Zon 1 – Grön zon och mot externa ytor.

En arbetsplats där information som klassificerats 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 klassificerats som INTERN diskuteras ska vara skyddad mot överhörning från ytor som definierats i nivå med Zon 1 – Grön zon och från externa ytor.

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

9.3.2 Möjlighet att förvara skyddsvärda tillgångar

Vid en arbetsplats där information som klassificerats som KÄNSLIG hanteras ska det finnas tillgång till en låst förvaringsenhet dit endast behöriga personer har tillträde (exempelvis ett låst skåp). Gäller för definierade i nivå med Zon 2 eller högre[12].

Vid en arbetsplats där information som klassificerats som BEGRÄNSAT HEMLIG eller högre hanteras ska det finnas tillgång till en förvaringsenhet godkänd enligt normen SSF 3492 dit endast behöriga personer har tillträde. Gäller också för ytor definierade i nivå med Zon 3[13].

9.3.3 Distansarbete

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

9.4 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 Norrtälje kommuns lokaler är att skapa en trygg miljö för allmänheten, anställda, leverantörer och förtroendevalda. Tydliga och förutsägbara regler ger möjlighet att sprida information om Norrtälje kommuns 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 verksamhetens specifika förutsättningar, men tre grundnivåer har definierats enligt nedan.

- **Fotografering, filmning och ljudupptagning i Zon 1 – Grön zon**
  Fotografering, filmning och ljudupptagning i 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 Norrtälje kommun 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. Enskild individ har dock laga rätt att spela in samtal, men får ej sprida inspelad sekretessreglerad information.

[12] För mer information se ”Tillträdesbegränsning”
[13] För mer information se ”Tillträdesbegränsning”

- **Fotografering, filmning och ljudupptagning Zon 3 – Röd zon**
  Utöver eventuell kamerabevakning som utförs på uppdrag av Norrtälje kommun 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.

9.5 Skyltning av säkerhetskrav och säkerhetsåtgärder i lokalerna

För att främja tydlighet och transparens 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 ska följa Norrtälje kommuns grafiska profil.

Det gäller exempelvis krav som reglerar under vilka förutsättningar som allmänheten får vistas i lokalerna samt i vilken omfattning tillträdesbegränsning, 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, eller sekretesstunnor).

9.6 Mekaniskt inbrottsskydd

För varje lokal som Norrtälje kommun 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 Norrtälje kommun beslutat om.

Fastighetsavdelningen ansvarar för att upprätthålla dokumentation avseende mekaniskt inbrottsskydd i Norrtälje kommuns lokaler.

9.7 Tekniska säkerhetssystem

Kommunen strävar efter ett säkert och effektivt nyttjande av tekniska säkerhetssystem för att komplettera det mekaniska inbrottsskyddet och upprätthålla ändamålsenlig säkerhet för Norrtälje kommuns 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 för respektive byggnad/lokal och anpassas efter verksamhetens behov av säkerhet.

Vid kravställning av tekniska säkerhetssystem ska Svenska Stöldskyddsföreningens normer användas som referens så långt det är möjligt för att säkerställa en långsiktigt hållbar kravställning och leverantörsoberoende.

Fastighetsavdelningen ansvarar för att upprätthålla dokumentation avseende tekniska säkerhetssystem i Norrtälje kommuns lokaler.

9.8 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 ska det finnas en bevakningsinstruktion som reglerar bevakningens omfattning.

Fastighetsavdelningen ansvarar för att upprätthålla dokumentation avseende ronderande bevakning i Norrtälje kommuns lokaler.

9.9 Insats

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

Fastighetsavdelningen tillsammans med Räddningstjänsten ansvarar för att upprätthålla dokumentation avseende insats vid larm i Norrtälje kommuns lokaler.

9.10 Principer för inpassering

Inpassering till Norrtälje kommuns lokaler sker med behörigheter som lagts på Norrtälje kommuns ID-kort.

Som generell regel gäller att under kontorstid krävs endast ID-kortet för inpassering till Zon 1 – Grön zon och Zon 2 – Gul zon. Övrig tid (kvällar, nätter och helger) och vid tillkopplat larm krävs såväl ID-kort som en personlig PIN-kod.

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

10 Säkerhet för medarbetare

Med säkerhet för medarbetare avses de åtgärder som vidtas för att medarbetare inte ska utgöra ett hot mot kommunens verksamhet och att kommunens verksamhet inte ska utgöra ett hot mot medarbetare.

10.1 Säkerhetsprövning av medarbetare

Säkerhetsprövning, bakgrundskontroller och liknande åtgärder syftar till att säkerställa att personer som deltar i Norrtälje kommuns verksamhet är pålitliga ur säkerhetssynpunkt och inte har okända sårbarheter som kan påverka verksamhetens säkerhet negativt.

10.1.1 Befattningsanalys

I vilken omfattning olika säkerhetsåtgärder ska vidtas för att säkerställa att en person är pålitlig ur säkerhetssynpunkt och lämplig för en viss tjänst styrs av vilken befattning personen har. Inom Norrtälje kommun ska det finnas en övergripande befattningsanalys som reglerar vilka befattningar som kräver en viss typ av säkerhetsåtgärder. Säkerhetschefen ansvarar för upprättande och revidering av befattningsanalysen i samråd med berörda förvaltnings- och avdelningschefer.

10.1.2 Säkerhetsprövningsåtgärder inom Norrtälje kommun

De säkerhetsprövningsåtgärder som vidtas inom Norrtälje kommun kan indelas i fem kategorier enligt följande:

- **Initial personkontroll**
  Den initiala personkontrollen genomförs av samtliga medarbetare som inte omfattas av någon av nedanstående kategorier och omfattar identitetskontroll. Personkontrollen ska genomföras innan dess att arbetet påbörjas.

- **Lämplighetsbedömning vid arbete med barn**
  Lämplighetsbedömning vid arbete med barn genomförs av samtliga medarbetare som arbetar i skola, vård och omsorg och som kommer i kontakt med barn inom Norrtälje kommuns verksamhet. Lämplighetsbedömningen omfattar inlämnande och bedömning av ett utdrag ur belastningsregistret och ska genomföras innan dess att arbetet påbörjas.

- **Lämplighetsbedömning för särskilda befattningar**
  Lämplighetsbedömning med bakgrundskontroll baserad på öppna källor och referenser kan komma att genomföras för särskilda befattningar som kan komma att hantera betydande ekonomiska medel eller som omfattar ett stort medarbetaransvar/verksamhetsansvar. Kommundirektör fattar beslut om lämplighetsbedömning för särskilda befattningar.

- **Grundläggande säkerhetsprövning**
  Grundläggande säkerhetsprövning genomförs för befattningar där detta bedömts tillämpligt i kommunens befattningsanalys. Säkerhetsprövningen omfattar en säkerhetsprövningsintervju med berörd person, samt efterföljande utvärdering och vid behov även kontroll av betyg, intyg och referenser. Ska genomföras innan dess att arbetet påbörjas.

- **Säkerhetsprövning vid inplacering i säkerhetsklass 3**
  Säkerhetsprövning vid inplacering i säkerhetsklass 3 genomförs för befattningar där detta bedömts tillämpligt i kommunens befattningsanalys. Säkerhetsprövningen omfattar förutom grundläggande säkerhetsprövning (se ovan) genomförande av registerkontroll för den prövade. Säkerhetsprövningen ska genomföras innan dess att arbetet påbörjas.

- **Säkerhetsprövning vid inplacering i säkerhetsklass 2**
  Säkerhetsprövning vid inplacering i säkerhetsklass 2 genomförs för befattningar där detta bedömts tillämpligt i kommunens befattningsanalys. Säkerhetsprövningen omfattar förutom grundläggande säkerhetsprövning (se

ovan) genomförande av registerkontroll och särskild personutredning för den prövade. Säkerhetsprövning vid inplacering i säkerhetsklass 2 omfattar även registerkontroll av eventuell make/maka/sambo till den prövade. Säkerhetsprövningen ska genomföras innan dess att arbetet påbörjas.

10.1.3 Före anställning

Före anställning ska de kontroller som är relevanta för befattningen (baserat på befattningsanalysen) genomföras. Den som rekryteras ska även ges information om gällande säkerhetskrav samt underteckna en sekretessförbindelse.

10.1.4 Under anställning

För medarbetare som genomgått säkerhetsprövning (med eller utan inplacering i säkerhetsklass) ska en löpande uppföljning av säkerhetsprövningen genomföras av närmaste chef. Den löpande uppföljningen innebär att ett antal frågor diskuteras och ska åtminstone genomföras årligen.

10.1.5 Vid ändring av anställning

Om anställningen förändras eller om en person byter befattning eller arbetsuppgifter ska en bedömning göras om huruvida den aktuella kategorin (se ovan) fortfarande är relevant och om ytterligare säkerhetsåtgärder behöver vidtas, alternativt om de åtgärder som vidtagits inte längre är relevanta. Närmaste chef ansvarar för att bedömningen görs och dokumenteras.

Om anställningen för en person inplacerad i säkerhetsklass förändras så att personen inte längre bedöms ha behov av att vara inplacerad i säkerhetsklass ska detta meddelas Säkerhetspolisen så att registerkontrollen kan upphöra.

10.1.6 Vid avslut av anställning

Vid avslut av anställning, uppdrag eller liknande är det särskilt viktigt att säkerhetsfrågor hanteras på ett systematiskt sätt för att säkerställa att all utrustning och all information återlämnas samt att alla behörigheter återkallas.

Om anställningen för en person inplacerad i säkerhetsklass avslutas (så att personen inte längre bedöms ha behov av att vara inplacerad i säkerhetsklass) ska detta meddelas Säkerhetspolisen så att registerkontrollen kan upphöra.

Då en medarbetare avslutar sin anställning ansvarar närmaste chef för att Norrtälje kommuns checklista vid avslutande av anställning gås igenom och signeras då samtliga punkter gåtts igenom.

Då en anställd vid en leverantör avslutar sitt uppdrag för Norrtälje kommun ansvarar chef för upphandlande förvaltning/avdelning eller enhet inom Norrtälje kommun för att Norrtälje kommuns checklista vid avslutande av anställning gås igenom och signeras då samtliga punkter gåtts igenom. Checklistan ska förvaras av ansvarig chef till dess att projektet avslutas och därefter arkiveras eller gallras i enlighet med dokumenthanteringsplan.

10.2 Säkerhetsutbildning och informationsinsatser för medarbetare

10.2.1 Säkerhetsinformation till nyanställda

Alla medarbetare i Norrtälje kommun 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.

10.2.2 Introduktionsutbildning

Medarbetare som har en tillsvidareanställning, eller visstidsanställning, ska genomföra Norrtälje kommuns introduktionsutbildning i säkerhet. Utbildningen fokuserar på medarbetarens eget ansvar för att följa regler och upprätthålla säkerheten i verksamheten. Kommunens målsättning är att säkerhetsutbildningen så långt som möjligt ska genomföras i form av en interaktiv utbildning.

10.2.3 Återkommande utbildning

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

10.2.4 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 säkerhetsutbildningar samordnas av säkerhetschefen utifrån verksamhetens behov.

10.2.5 Informationsinsatser

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

Det huvudsakliga ansvaret för att medarbetare hålls informerade om säkerhetsfrågor ligger på närmaste chef med stöd av säkerhets- och beredskapssamordnare, Norrtälje kommuns säkerhetschef och dataskyddsombudet.

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

10.3 Förebyggande arbete mot hot och våld

Kommunen bedriver ett långsiktigt förebyggande arbete för att förhindra förekomsten av hot och våld riktat mot medarbetare 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 mer information om hantering av uppkomna incidenter som innefattar hot eller våld, se Norrtälje kommuns policy samt tillhörande riktlinjer för arbetet mot hot och våld riktat mot medarbetare respektive förtroendevalda.

11 Leverantörssäkerhet

I syfte att säkerställa att ändamålsenlig säkerhet upprätthålls för Norrtälje kommuns verksamhet oavsett om den bedrivs i egen regi, eller av leverantörer, så ska säkerhetsåtgärder vidtas i samband med upphandling av tjänster. Chef för upphandlade enhet eller projektledare (om sådan utsetts) ansvarar för att säkerheten upprätthålls under och efter avtalstiden.

11.1 Säkerhetsprövning av leverantörer

11.1.1 Inför uppdraget

Innan uppdraget eller engagemanget påbörjas ska de kontroller som skulle ha varit relevanta om motsvarande arbete utförts av en anställd (baserat på befattningsanalysen) genomföras. Den som ska påbörja uppdrag eller engagemang ska även ges information om gällande säkerhetskrav samt underteckna en sekretessförbindelse.

11.1.2 Under uppdraget

Under uppdragets genomförande ska medarbetare hos leverantör som genomgått säkerhetsprövning (med eller utan inplacering i säkerhetsklass) genomgå uppföljning av säkerhetsprövningen tillsammans med närmaste chef. Den löpande uppföljningen innebär att ett antal frågor diskuteras och ska åtminstone genomföras årligen (förslagsvis i samband med medarbetar-samtal). Resultatet av uppföljningen ska dokumenteras och eventuella identifierade riskfaktorer ska kommuniceras med Norrtälje kommuns säkerhetschef.

11.1.3 Vid förändrat uppdrag eller engagemang

Om uppdraget eller engagemanget förändras eller om en person byter befattning eller arbetsuppgifter ska en bedömning göras om huruvida den aktuella kategorin (se ovan) fortfarande är relevant och om ytterligare säkerhetsåtgärder behöver vidtas eller om de åtgärder som vidtagits inte längre är relevanta. Chef för upphandlade enhet eller projektledare (om sådan utsetts) ansvarar för att bedömningen görs och dokumenteras.

11.1.4 Vid uppdrags avslut

Vid avslut av uppdrag eller engagemang är det särskilt viktigt att säkerhetsfrågor hanteras på ett systematiskt sätt för att säkerställa att all utrustning och all information återlämnas samt att alla behörigheter återkallas.

Då en anställd vid en leverantör avslutar sitt uppdrag för Norrtälje kommun ansvarar chef för upphandlande förvaltning/avdelning eller enhet inom Norrtälje kommun för att Norrtälje kommuns checklista vid avslutande av anställning gås igenom och signeras då samtliga punkter gåtts igenom. Checklistan ska förvaras av ansvarig chef till dess att projektet avslutas och därefter arkiveras eller gallras i enlighet med dokumenthanteringsplan.

11.2 Säkerhetsutbildning och informationsinsatser för leverantörer

11.2.1 Projektsäkerhetsutbildning

Projektledare ansvarar för att inblandade i projekt som Norrtälje kommun driver ges en projektsäkerhetsutbildning som motsvarar behovet av säkerhet i det aktuella projektet.

Projektsäkerhetsutbildningen ska vara anpassad efter vilka skyddsvärda tillgångar som kommer att hanteras inom ramen för projektet och genomföras i samband med att arbetet i projektet påbörjas. Särskild vikt ska läggas vid att utbilda leverantörer i de krav som ställs vid hantering av Norrtälje kommuns skyddsvärda information utifrån respektive informationsmängds klassificering.

11.2.2 Informationsinsatser

Kommunens leverantörer ska ges regelbunden och löpande information om säkerhetsrelaterade frågor rörande det arbete leverantören utför för Norrtälje kommun. Det huvudsakliga ansvaret för att leverantörer hålls informerade om säkerhetsfrågor ligger på ansvarig chef för upphandlande förvaltning/kontor, avdelning eller enhet med stöd av Norrtälje kommuns säkerhetschef och dataskyddsombud.

12 Kontinuitet

Organisationens 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.

Organisationens 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.

13 Incidenthantering

Med en säkerhetsincident avses alla säkerhetsrelaterade händelser som skadar, eller riskerar att skada, Norrtälje kommuns verksamhet. Även identifierade brister i Norrtälje kommuns 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 tre kategorier beroende på omfattning, potentiell skada och hur tidskritisk hanteringen av incidenten är enligt nedan.

- **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 Norrtälje kommuns verksamhet eller bortfall av kritiska förmågor under en längre tid. Hit räknas incidenter som kan komma att påverka Norrtälje kommuns 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 Norrtälje kommuns 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 Norrtälje kommuns säkerhets-

eller beredskapsarbete (som inte är av betydelse för säkerhetsskyddet eller civilförsvarsförmågan) 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 Norrtälje kommuns 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.

13.1 Rapportering av säkerhetsincidenter

Säkerhetsincidenter ska huvudsakligen rapporteras genom en anmälan via Norrtälje kommuns incidentrapporteringssystem som återfinns på intranätet. Undantaget är incidenter som bedöms kunna påverka Norrtälje kommuns säkerhetsskydd. Dessa ska istället endast rapporteras muntligen till Norrtälje kommuns säkerhetschef.

Anledningen till detta är att systemet som hanterar incidentrapporter inte är godkänt för att hantera uppgifter som är säkerhetsskyddsklassificerade.

Vid tveksamhet avseende huruvida en viss information kan rapporteras via incidentrapporteringssystemet, kontakta Norrtälje kommuns säkerhetschef för råd.

- **Mycket allvarlig incident**
  Mycket allvarliga incidenter ska omgående rapporteras via telefonkontakt med Norrtälje kommuns tjänsteman i beredskap (TiB). Därefter ska kontakt tas med Norrtälje kommuns säkerhetschef och/eller dataskyddsombudet (beroende på typ av incident) samt berörda chefer. Då kontakter har tagits enligt ovan ska incidenten registreras i Norrtälje kommuns incidenthanteringssystem. ***Observera att rapporter som innehåller information rörande Norrtälje kommuns säkerhetsskydd, civilförsvarsplanering eller i övrigt kan ge kunskap om förekommande brister eller sårbarheter i kommunens säkerhetsarbete inte får registreras i incidenthanteringssystemet.***

- **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 Norrtälje kommuns incidenthanteringssystem. ***Observera att rapporter som innehåller information rörande Norrtälje kommuns säkerhetsskydd, civilförsvarsplanering eller i övrigt kan ge kunskap om förekommande brister eller sårbarheter i kommunens säkerhetsarbete inte får registreras i incidenthanteringssystemet.***

- **Begränsad incident**
  Begränsade incidenter ska rapporteras genom registrering i Norrtälje kommuns incidenthanteringssystem. Från systemet kommer information att komma närmaste chef, säkerhetschefen och dataskyddsombudet tillhanda. ***Observera att rapporter som innehåller information rörande Norrtälje kommuns***

säkerhetsskydd, civilförsvarsplanering eller i övrigt kan ge kunskap om förekommande brister eller sårbarheter i kommunens säkerhetsarbete inte får registreras i incidenthanteringssystemet.

13.2 Hantering av säkerhetsincidenter

Säkerhetsincidenter och identifierade brister i Norrtälje kommuns 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 Norrtälje kommun, alternativt rör gemensamma IT-system eller säkerhetsfunktioner. I sådana fall ansvarar Norrtälje kommuns 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 medarbetare som uppmärksammar en personuppgiftsincident.

13.3 Dokumentation och uppföljning av säkerhetsincidenter

Utöver den dokumentation om inträffade säkerhetsincidenter och identifierade säkerhetsbrister som framgår av Norrtälje kommuns incidenthanteringssystem och andra inrapporterade incidenter, 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 Norrtälje kommuns säkerhetschef.

Syftet med dokumentationen är att Norrtälje kommun 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.

14 Bristande efterlevnad

Alla som genom anställning, uppdrag eller av annan anledning utför arbete för Norrtälje kommun är skyldiga att följa Norrtälje kommuns Riktlinje för systematiskt säkerhetsarbete.

Vid bristande efterlevnad av riktlinjerna genomför närmaste chef en intern utredning där HR kan vara ett stöd. Innan ytterligare åtgärder vidtas kontaktas HR för en arbetsrättslig bedömning. Vid misstanke om brott kan en polisanmälan göras.

15 Uppföljning och utvärdering av Norrtälje kommuns säkerhetsarbete

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

Vid Norrtälje kommun ska det finnas en övergripande plan för säkerhetskontroller. Organisationens 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 Norrtälje kommun.

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 Norrtälje kommuns säkerhets- och beredskapsarbete.

NORRTÄLJE KOMMUN

2020-10-22
Diarienummer: KS 2020-1900

Policy för systematiskt säkerhetsarbete– Norrtälje kommun

Den interna säkerheten är viktig för att skydda såväl Norrtälje kommun som de personer och organisationer som är beroende av att kommunen kan fortsätta bedriva sin verksamhet. Att vi har ett ändamålsenligt och väl fungerande internt säkerhetsarbete är avgörande för att vi ska kunna upprätthålla förtroendet för kommunen och den kommunala verksamheten.

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

Kommunens systematiska säkerhetsarbete omfattar åtgärder som regleras av krav inom ett stort antal områden. Dessa områden är informationssäkerhet, säkerhetsskydd, fysisk säkerhet, säkerhet vid upphandling, säkerhet vid rekrytering samt incidentrapportering. Även säkerhetsrelaterade krav som följer av den europeiska dataskyddsförordningen (GDPR/DSF) har inarbetats i kommunens säkerhetsarbete och de inriktande, styrande och stödjande dokument som reglerar kommunens säkerhetsarbete.

Vårt övergripande mål för det interna säkerhetsarbetet är att bedriva ett ändamålsenligt och kostnadseffektivt arbete med den interna säkerheten som uppfyller samtliga föreliggande krav, samt tillgodoser Norrtälje kommuns behov av säkerhet, och är utformat utifrån Norrtälje kommuns förutsättningar för att bedriva ett långsiktigt effektivt internt säkerhetsarbete.

Det interna säkerhetsarbetet ska baseras på genomförda analyser och vara väl avvägt utifrån förekomsten av skyddsvärda tillgångar och den dimensionerande hotbilden för Norrtälje kommuns verksamhet.

Det interna säkerhetsarbetet är utformat för att åstadkomma ett ändamålsenligt skydd för Norrtälje kommuns skyddsvärda tillgångar, vilka indelas i följande kategorier:

- Kommunens medarbetare och övriga personer som deltar i vår verksamhet
- Förtroendet för Norrtälje kommun och vårt varumärke
- Kommunens information och den information som vi hanterar för våra kunders räkning
- Kommunens egendom (i form av lokaler och utrustning m.m.) och egendom som vi nyttjar
- Kommunens ekonomiska tillgångar
- Kommunens kulturhistoriska värden

Ansvaret för den interna säkerheten är uppdelat på ett antal roller, enligt följande:

POSTADRESS
Box 803, 761 28 Norrtälje
Trygghets och Säkerhetskontoret

BESÖKSADRESS
Estunavägen 14

KONTAKT
0176-710 00
kontaktcenter@norrtalje.se
www.norrtalje.se

- Kommundirektören är ytterst ansvarig för säkerheten inom Norrtälje kommun och ansvarar för att resurser avdelas för säkerhetsarbetet utifrån fastställda målsättningar. Kommundirektören beslutar i säkerhetsfrågor som inte delegerats.
- Kommunens säkerhetschef leder och följer upp säkerhetsarbetet och ger stöd till ledning och medarbetare i säkerhetsfrågor. Säkerhetschefen beslutar i säkerhetsfrågor efter delegering från kommundirektören.
- Säkerhetsskyddschef beslutar i frågor som rör kommunens säkerhetsskydd efter delegering från kommundirektören.
- Chefen för IT-avdelningen ansvarar för implementation av säkerhetsåtgärder för kommunens IT-miljö och kommunikationslösningar utifrån fastställda krav i styrande dokument. IT-chefen ska säkerställa att arbetet med IT- och kommunikationssäkerhet inom kommunen följs upp och får avsedd effekt.
- Dataskyddsombudet leder arbetet med att säkerställa Norrtälje kommuns efterlevnad av dataskyddsförordningen och utgör kontaktperson mot datainspektionen och ger stöd till ledning och medarbetare i frågor rörande behandling av personuppgifter.
- Medarbetare och andra som deltar i Norrtälje kommuns verksamhet ansvarar för att efterleva styrande dokument och se till att det dagliga arbetet utförs i enlighet med gällande regler samt rapportera säkerhetsincidenter enligt fastställd rutin.

Säkerhetsarbetet inom Norrtälje kommun styrs av följande inriktande, styrande och stödjande dokument:

- Kommunens säkerhetspolicy utgör inriktande dokument för det interna säkerhetsarbetet.
- Kommunens riktlinje för säkerhet utgör styrande dokument för säkerhetsarbetet.
- Anvisningar och rutiner utgör stödjande dokument för säkerhetsarbetet.

I slutändan utgör personalens kunskap om-, och förståelse för, det interna säkerhetsarbetet det bästa skyddet för verksamheten. Norrtälje kommun strävar efter ständig kompetensutveckling inom säkerhetsområdet för samtliga medarbetare och tillhandahåller återkommande internutbildningar i säkerhetsfrågor.