Kommunstyrelsens kontor

Södertälje kommun

Rapport | 2017-11-06

Riktlinjer för informationssäkerhet

Innehållsförteckning

1. Inledning

Hot mot Södertälje kommuns information förekommer i olika former. Bränder, vattenläckage, stölder, förfalskning och bedrägerier är bara några exempel. IT och Internet har blivit en arena för försäljning av varor, hot och utpressningar, stölder och bedrägerier. Kort sagt samma sorts kriminalitet som finns utanför den digitala världen. IT har förändrats från att ha varit ett stöd för, till att ha blivit en förutsättning för verksamheterna. Det är därför viktigt att den som har ett verksamhetsansvar också identifierar beroendet av IT för att kunna fullgöra sina åtagande även vid en kris, katastrof eller när informationssystemen inte fungerar.

Allmänhetens rättighet till insyn i den kommunala förvaltningen är ytterligare en orsak till att hålla god ordning på vår information. Informationssäkerhet handlar om hur Södertälje kommun ska minska sannolikheten för, eller konsekvenserna av, uppkomna eller identifierade hot mot den information kommunen har en skyldighet att skydda. Dessa riktlinjer anger vad och hur verksamheterna ska agera för att initiera, införa, behålla och förbättra informationssäkerheten i Södertälje kommun. Riktlinjerna anger de lägsta kraven vid utveckling eller inköp av nya system och målet för redan driftsatt system.

Denna riktlinje vänder sig till nämnder, verksamheter och medarbetare. I tillämpliga delar även för andra användargrupper som får tillgång till kommunens informationstillgångar genom användaridentitet eller liknande, t.ex. privata utförare, bolag, leverantörer eller inhyrd personal. Riktlinjen ska läsas tillsammans med övrigt regelverk och anvisningar inom området IT och säkerhet.

1.1 Disposition

Riktlinjen har samma rubriktexter som SS-ISO/IEC 27002:2013 vilket innebär en internationell anpassning av kommunens regler. Varje kapitel och underkapitel inleds med ett förklarande syfte med den efterföljande texten och beskriver vad som ska uppnås. Detaljanvisningar för hur syftet ska uppnås anges i underliggande anvisningar och instruktioner.

2. Definitioner

Användare: Individ som nyttjar informationstillgångar.

Autentisering: Kontroll av uppgiven identitet.

Behandling av personuppgifter: Varje åtgärd eller serie av åtgärder som någon vidtar med personuppgifter, vare sig det görs på automatiserad väg eller inte.

Dataskyddsombud: Utsedd person som ansvarar för kontrollen att Dataskyddsförordningen följs inom kommunen genom att till exempel utföra kontroller och informationsinsatser.

Hot: Möjlig oönskad händelse med negativa konsekvenser för verksamheten.

Identitet: Unik beteckning för en viss individ.

Incidenter: Händelser som negativt påverkar eller kan komma att påverka säkerheten för Södertälje kommuns information eller informationstillgångar.

Informationsbehandlingsresurser: Information som hanteras i system, service eller infrastruktur eller platser som innehåller dem såsom datorer, serverhallar mm.

Informationsklassificering: Ett formellt sätt att fastställa rätt skyddsnivå för information.

Informationssäkerhet: Skyddet av information för att tillförsäkra affärskontinuitet, minimera affärsrisker och maximera förtjänsten av investeringar och affärstillfällen. Information kan finnas i många former; till exempel skriftligt på papper, visat på filmer, delad över telefon eller annan media.

Informationstillgångar: En organisations informationsrelaterade tillgångar, vilka har ett värde för organisationen och därmed är skyddsvärda.
Exempel på informationstillgångar är: Information (databaser, filer, metodik, dokument, etc.)
Program (tillämpningar, operativsystem, etc.)
Tjänster (nätförbindelser, abonnemang, etc.)
Fysiska tillgångar (datorer, datamedia, lokala nätverk, etc.)

Kontinuitetsplan: Dokument som beskriver hur verksamhet skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod.

Konsekvens: Påföljden av ett inträffat hot.

Logg: Insamlad information om de operationer som utförs i ett system.

Medarbetare: Södertälje kommuns anställda och konsulter samt samarbetspartners som har arbetsuppgifter som kan påverka Södertälje kommuns informationssäkerhet.

Mobil enhet: Mobiltelefon, surf- eller läsplatta eller liknande teknisk enhet. Bärbar dator innefattas inte i begreppet.

Personuppgifter: All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Bild- och ljuduppgifter om en identifierbar fysisk person räknas som personuppgifter, även om inga namn nämns. Krypterade uppgifter och olika slag av elektroniska identiteter är också personuppgifter om de direkt eller indirekt kan kopplas till fysiska personer som är i livet.
Rollbaserad behörighet (RBB): Personer tilldelas en behörighet som består av åtkomst till ett antal system och program som ger dem åtkomst till den information de behöver för sin handläggning.

Riktighet: Egenskap att informationen inte obehörigen, av misstag eller på grund av funktionsstörning.

Risk: Produkten av sannolikhet och konsekvens för att ett hot realiseras.

Riskanalys: Process som identifierar säkerhetsrisker, bestämmer deras betydelse och identifierar skyddsåtgärder. Riskerna definieras som hot mot tillgänglighet, sekretess eller integritet eller kombination av dessa.

Samtycke: Varje slag av otvetydig viljeyttring genom vilken den registrerade godtar att personuppgifter som rör honom eller henne behandlas.

SaaS: Software as a Service, en typ av molntjänst som tillhandahåller programvara över internet. Applikationerna tillhandahålls i "molnet" och kan användas för en rad olika uppgifter för både privatpersoner och organisationer. Exempel på SaaS är Projektplatsen, Google-drive, Spotify m.fl.

Sekretess: Avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga.

SLA: Service Level Agreement – Överenskommelse mellan beställare samt leverantör av tjänsteleverans, definierar verksamhetens krav på IT-tjänsten. Både på IT tjänsteleveransens tid då den är tillgänglig, prestanda etc. samt mjuka värden som service desk.

Stark autentisering: Autentisering som innebär att identiteten kontrolleras på minst två sätt.

Sårbarhet: Brist i skyddet av en tillgång som innebär att den är exponerad för hot.

Säkerhet: Egenskap eller tillstånd som innebär skydd mot risk i samband med insyn, förlust eller påverkan även i samband med medvetna försök att utnyttja eventuella svagheter.

Tillgänglighet: Möjligheten att utnyttja informationstillgångar efter behov i förväntad utsträckning och inom önskad tid.

Åtkomst-/behörighetskontroll: Funktion att reglera och kontrollera en användares åtkomst till olika informationstillgångar samt att skydda information och program så att de endast är tillgängliga utifrån tilldelad behörighet.

3. Läsanvisning

3.1 Struktur för säkerhetsdokumentation

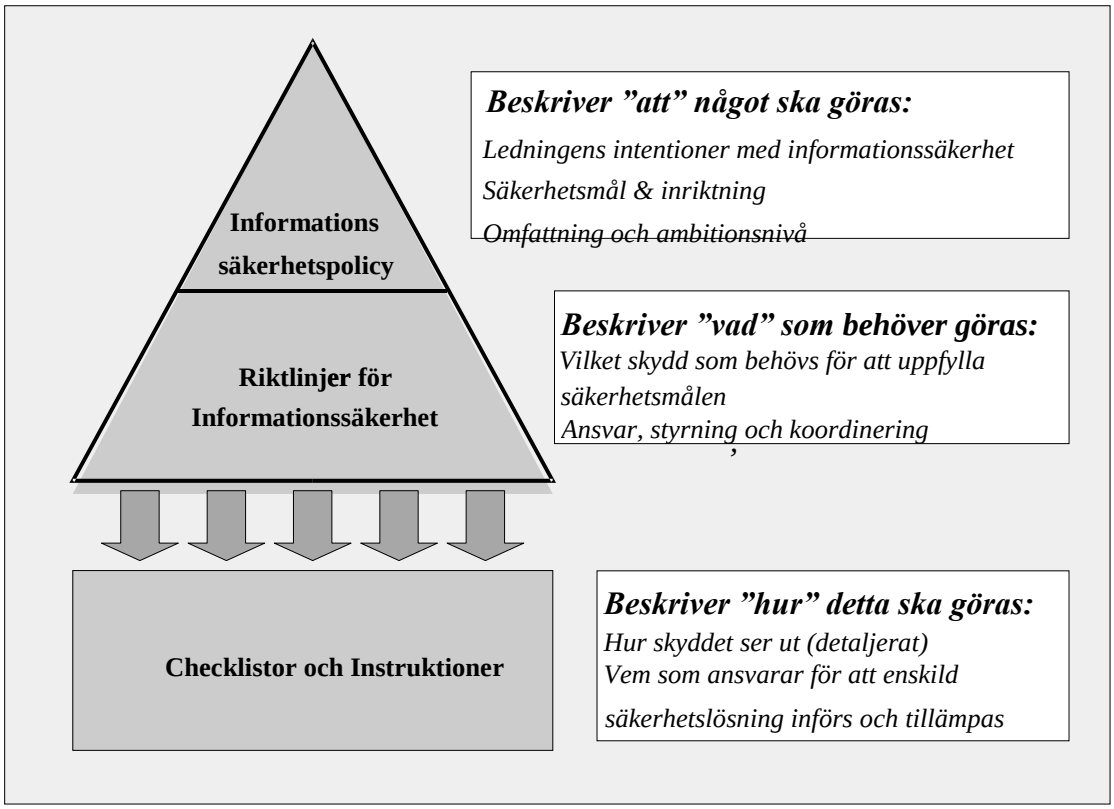
Nedanstående bild visar struktur för Södertäljes säkerhetsdokumentation.

I Informationssäkerhetspolicyn fastställer kommunstyrelsen sin syn på informationssäkerhet, övergripande mål och intention med informationssäkerhetsarbetet.

Riktlinjerna för informationssäkerhet beskriver vilka rutiner och säkerhetslösningar som måste etableras, för att uppfylla de mål som beskrivs i Informationssäkerhetspolicyn. Dessa riktlinjer framgår av detta dokument.
Riktlinjerna syftar inte till att detaljerat beskriva hur rutiner och säkerhetslösningar i praktiken ska utformas, utan ger en minsta förväntad nivå för dessa. Detta för att dels etablera en gemensam säkerhetsnivå som alltid måste uppnås, dels för att rutiner och säkerhetslösningar ska kunna anpassas till verksamhetens normala rutiner och sätt att arbeta.

Utifrån detta upprättas *Checklistor och instruktioner*, som detaljerat redogör för hur rutiner och säkerhetslösningar ska utformas och tillämpas, för att Informationssäkerhetspolicyns krav ska efterlevas.

Säkerhetsenheten ansvarar för Informationssäkerhetspolicyn samt dessa riktlinjer. Anvisningar för specifika områden upprättas av det kontor, avdelning, funktion eller den ansvarige tjänstemannen inom det område där anvisningen ska tillämpas.



Kapitel		Primär mottagare	Kort beskrivning över kapitel
4	Riskbedömning och riskhantering	Säkerhetschef, Kontorschef, enhetschef	Hur Södertälje kommun hanterar risker och genomför riskanalyser
5	Informationssäkerhetspolicy	Samtliga medarbetare	Introduktion, orientering till styrande dokument
6	Organisation och ansvar	Samtliga medarbetare	Fördelning av ansvaret för informationssäkerhet inom Södertälje kommun
7	Personal och Informationssäkerhet	HR, Chef med personalansvar	Säkerhet vid rekrytering, byte av tjänst, avslutande av anställning
8	Hantering av tillgångar	Samtliga medarbetare	Hantering av utrustning och information samt informationsklassning
9	Styrning av åtkomst	IT-personal, Produktägare Samtliga medarbetare (kap 9.3)	Hur vi styr tillgången till våra resurser och system
10	Kryptering	IT-personal, Produktägare	Hur kryptering ska korrekt införas och regler för krypteringsnycklar
11	Fysisk säkerhet	Samtliga medarbetare	Hur vi fysiskt ska skydda våra tillgångar mot obehörig åtkomst

12	Driftsäkerhet	IT-personal, Systemansvariga	Hur säkerhet och drift hanteras i system och informationsbehandlingsresurser
13	Kommunikationssäkerhet	IT-personal	Hur säkerheten av informationen i nätverk upprätthålls
14	Inköp, Utveckling och Underhåll av system	Produktägare, Utvecklare, IT-personal	Förvaltning av befintlig säkerhetsnivå vid nya eller underhåll av gamla system
15	Leverantörsrelationer	Avtalsansvariga	Hur informationssäkerheten upprätthålls för de tillgångar som leverantörer har åtkomst till.
16	Hantering av incidenter	Samtliga medarbetare	Hur incidenter ska rapporteras och hanteras
17	Kontinuitetsarbete	Säkerhetsansvarig, Ledningsgrupp	Hur verksamhetens kontinuitet ska säkerställas och upprätthållas
18	Efterlevnad	Samtliga medarbetare	Hur verksamheten ska undvika överträdelser av lagar, avtal och författningar

Kapitel	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
Medarbetare	x				x	x		x			x					x		x
Förtroendevalda	x				x	x		x			x					x	x	x
Chefer	x			x	x	x	x	x			x				x	x	x	x
Personal- administratör						x	x	x								x		x
Upphandling									x					x	x			
Kommunikation								x										
Systemägare/Systemförvaltare	x			x		x		x	x	x	x	x	x	x	x	x		
IT-drift	x						x		x	x	x	x	x	x	x	x		
Säkerhet	x			x	x	x	x	x	x	x	x				x	x	x	x

4. Riskbedömning och riskhantering

Det här avsnittet beskriver Södertälje kommuns riskhantering och arbete med riskanalyser

4.1 Process och hantering

Inom Södertälje kommun definieras risk som kombinationen av sannolikheten för att något ska inträffa och konsekvensen av det inträffade. Dessa risker identifieras på genomförda riskanalyser samt de incidenter som inträffar i Södertälje kommuns verksamhet.

Södertälje kommun har utarbetat en metod för hur risk- och sårbarhetsanalys ska genomföras för IT-system (se 4.2). Risk- och sårbarhetsanalyser är ett sätt att identifiera och bedöma risker och föreslå åtgärder utifrån behovet.

Inom Södertälje kommun skall detta genomföras för IT-system som är verksamhetskritiska (enligt ”Checklista för verksamhetskritiska system”) eller som innehåller viktig information enligt informationsklassning (nivå 2 eller 3).

Alla informationstillgångar och verksamheter är utsatta för risker och hot. Vid förändringar av verksamheten, av IT-stödet, av rättsliga krav eller andra förändringar som kan påverka bedömningen ska risk- och sårbarhetsanalysen omvärderas och uppdateras. I annat fall sker genomgång en gång per år.

Observera att risk- och sårbarhetsanalys ska göras ur både perspektivet IT-system och generella analyser för verksamheten i stort i samråd med säkerhetsavdelningen.

4.2 Relaterad dokumentation

- Risk- och sårbarhetsanalys
- Mall_Riskanalys
- Riskvärdering risk- o sårbarhetsanalys.xls

Dokumenten finns på http://kanalen/styrning/policyer-och-riktlinjer/ under rubriken *IT* och *Informationssäkerhet och systemförvaltning*

5. Informationssäkerhetspolicy

Det här avsnittet beskriver Södertälje kommuns avsikt med informationssäkerhetsarbetet.

5.1 Södertälje kommuns inriktning för informationssäkerhet

5.1.1 Policy för informationssäkerhet

I Södertälje kommuns informationssäkerhetspolicy fastställs kommunens syn på informationssäkerhet samt övergripande mål och intentioner med arbetet.

5.1.2 Riktlinjer för informationssäkerhet

Det här dokumentet utgör Södertälje kommuns riktlinjer inom informationssäkerhet. Riktlinjerna beskriver en lägsta säkerhetsnivå som ska uppnås inom hela kommunen och dess verksamheter.

Riktlinjerna utgår från verksamhetens krav som i sin tur baseras på identifierade risker och Södertälje kommuns övriga krav.

5.1.3 Granskning av regelverk för informationssäkerhet

Informationssäkerhetspolicyn ägs och underhålls av informationssäkerhetsansvarige och är beslutad av kommunstyrelsen (KS 14/93).

Riktlinjerna utfärdas och revideras årligen av informationssäkerhetsansvarige.

5.2 Relaterad dokumentation

Informationssäkerhetspolicyn i sin helhet finns på http://kanalen/styrning/policyer-ochriktlinjer/ under rubriken *IT* och *Informationssäkerhet och systemförvaltning*

Övriga styrande dokument såsom övriga policys, anvisningar och instruktioner finns publicerade på Kanalen.

6. Organisation och ansvar

Det här avsnittet beskriver hur ansvaret för informationssäkerheten ska vara fördelat och hur säkerhetsarbetet ska organiseras.

6.1 Södertälje kommuns interna organisation

Inom Södertälje kommun finns det verksamhet inom den politiska nivån samt en tjänstemannanivå. På tjänstemannanivån finns dessutom en uppdelning mellan förvaltning (kontoren) och Kommunens bolag.

När det gäller tjänstemannanivån beskrivs kontorets ansvar i rollerna: kontorschef, informationsägare, systemägare och systemförvaltare. Kommungemensamt ansvar beskrivs i rollerna stadsdirektör, IT-strateg, informationssäkerhetsansvarig och IT-chef. Ansvaret ligger alltid på nedan utpekad roll, även om arbetsuppgiften skulle delegeras till någon annan. För alla användare finns också ett generellt ansvar genom användarförsäkran.

6.2 Informationssäkerhetsroller och ansvar

6.2.1 Kommunfullmäktige

Beslutar om Södertälje kommuns allmänna mål, även när det gäller användning av IT, digitalisering och verksamhetsutveckling till följd av nya möjligheter och verktyg. Fattar beslut om nyinvesteringar samt större IT-relaterade projekt samt beslutar om det övergripande styrdokumentet ”informationssäkerhetspolicy för Södertälje kommun”.

6.2.2 Kommunstyrelsen

Ansvarar för att följa upp och revidera uppsatta mål som gäller användning av IT och digitalisering, följer upp att säkerhetsrevidering av IT-miljön genomförs och föreslår Kommunfullmäktige att anta nya mål.

6.2.3 Nämnderna

Skall följa kommunfullmäktiges mål för IT och digitalisering och beakta detta i sin budgetprocess.

- Nämnden är personuppgiftsansvarig för sin verksamhet, samt att tillse att gällande lagstiftning inom området följs, t.ex. Dataskyddsförordningen
- Ansvarar för att personuppgiftsombud och att kommande Dataskyddsombud utses.

6.2.4 Stadsdirektören

Stadsdirektören har det övergripande ansvaret för att kommunen som helhet drar nytta av de möjligheter som IT och digitalisering ger till verksamhetsutveckling, ökad medborgarnytta och effektiviseringar. Detta innebär också samordning av kontorens behov och utveckling, liksom med de kommunala bolagen, där det är relevant.

6.2.5 Informationssäkerhetsansvarig

Informationssäkerhetsansvarige har det övergripande och det strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet samt ansvarar för uppföljning av kommunens systemförvaltningsmodell. I uppdraget ingår även att genomföra oberoende informationssäkerhetsrevisioner inom verksamheten samt att samordna kommunens personuppgiftsombud.

6.2.6 Kontorschefer

Kontorschefen är övergripande ansvarig för hela kontorets verksamhet och ska säkerställa att kontoret som helhet drar nytta av de möjligheter som IT och digitalisering ger till verksamhetsutveckling, liksom att kontorets verktyg och system används säkert. Kontorschefen ska säkerställa att nämnderna har utsett personuppgiftsombud och att det finns systemägare för varje system som köps in eller ansvaras för inom kontoret.

6.2.7 Personuppgiftsombud

Personuppgiftsombudet har en kontrollfunktion och ska säkerställa att personuppgifter inom respektive nämnds område behandlas på ett korrekt och lagligt sätt. Personuppgiftsombudet ansvarar för att:

- Verksamhetens personuppgiftsbehandling kontrolleras
- Att förteckning förs över behandling av personuppgifter upprättas och uppdateras
- Kontrollera att personuppgiftsbiträdesavtal finns för system som behandlar personuppgifter (för system som köps som tjänst)
- Samråda med datainspektionen vid behov
- Att sammanställa registerutdrag enligt PUL vid begäran
- Att hjälpa registrerade att få rättelse och tillse att den registrerades uppgifter hanteras i enlighet med gällande lagstiftning

6.2.8 Informationsägare

Informationsägare har det övergripande och yttersta ansvaret för den information som används inom en avgränsad verksamhet och att nödvändiga resurser avsätts för informationssäkerheten. Informationsägaren fattar de avgörande besluten om hur, av vem och vilken information som ska registreras samt om informationen behöver revideras och i vilken form informationen ska bevaras för att tillgänglighet, riktighet, sekretess och spårbarhet ska säkerställas över tid.

Kontorschefen ansvarar för att utse en operativ informationsägare, eller i annat fall själv fungera som informationsägare.

6.2.9 Systemägare

För information som lagras eller bearbetas i IT-system har *systemägarna* ett övergripande ansvar för respektive system och hur information hanteras i systemet, samt systemets användning. System ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov så som dess innehåll klassificerats enligt anvisningar för informationsklassificering.

För alla system som finns eller skall köpas in skall en systemägare utses. De flesta verksamhetssystem är det respektive kontor som ansvarar för, och då utser kontorschef systemägare (eller tar själv på sig rollen). För kommungemensamma system ansvarar Ksk och/eller IT-enheten för att systemägare utses.

6.2.10 Systemförvaltare

För information som lagras eller bearbetas i IT-system har systemförvaltarna det funktionella (dagliga) helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls. För mindre system kan systemägare och systemförvaltare vara en och samma person.

Rollen som systemförvaltare erhålls av en systemägare och arbetet utförs i nära samverkan med systemägaren, systemleverantören, outsourcingpartners och kommunens IT-enhet.

6.2.11 Chefer på alla nivåer

Chefer på alla nivåer har ett ansvar för att deras medarbetare är medvetna om och lever upp till informationssäkerhets policy och riktlinjer samt skall aktivt verka för en positiv attityd till och förståelse för syftet med säkerhetsarbetet.

6.2.12 Alla användare

Alla användare ska i sitt vardagliga arbete använda IT och moderna verktyg på ett sätt som bidrar till att verksamhetens mål uppfylls. Detta ska göras på ett säkert sätt och i enlighet med användarförsäkran och riktlinjer för informationssäkerhet.

6.3 Uppdelning av arbetsuppgifter

För att upprätthålla Södertälje kommuns informationssäkerhetsmål ska en separation av roller ske så långt det är möjligt inom kommunens kritiska verksamheter, t.ex. ekonomifunktioner och IT.

Inom t.ex. ekonomi ska det vara uppdelat ansvar på flera olika individer för attestering av fakturor, bokföring och utbetalning. Inom IT, tillsammans med drifts- eller systemleverantör, ska det vara uppdelat ansvar på flera individer för drifthantering, utveckling, test och driftsättning. Detta är viktigt för att möjliggöra bevakning av kvalitetsprocessen så att samtliga aktiviteter blir genomförda.

För viss typ av säkerhetskritisk/känslig information och för vissa arbetsuppgifter ska åtgärder vidtas för att minska tillfällen till obehörig eller oavsiktlig förändring samt missbruk av kommunens tillgångar. Det ska undvikas att samma individ ges behörigheter till system/tillgångar och att dessa kan användas utan att behörigheten prövas eller åtkomsten upptäcks.

6.4 Kontakt med myndigheter

För att säkerställa att Södertälje kommuns informationssäkerhetsarbete är på en god nivå, är aktuell och för att möjliggöra snabba åtgärder vid t.ex. säkerhetsincidenter, är det viktigt för kommunen att etablera nätverk med andra kommuner, organisationer och myndigheter.

Nätverken ger bland annat möjlighet att hålla sig informerad om nya hot och hur de kan bemötas. Det är också möjligt att få råd i säkerhetsfrågor och bygga upp kompetens inom kommunen.

6.5 Kontakt med särskilda intressegrupper

För att ha möjlighet till snabb hjälp samt kompetensutveckling hos personalen inom Södertälje kommun är individernas personliga nätverk ovärderliga. Även medlemskap i säkerhetsorganisationer eller särskilda intressegrupper uppmuntras.

6.6 Mobila enheter och distansarbete

6.6.1 Regler för mobila enheter

De mobila enheter (smartphone, bärbar dator, surfplatta, IoT) som Södertälje kommun tillhandahåller för de anställda måsta vara försedda med de säkerhetslösningar som anvisas. Distansarbete och Mobil datoranvändning omfattar användning av bärbara PC, handdatorer, läsplattor, avancerade mobiltelefoner och andra liknande enheter från annan plats än arbetsplatsen.

Följande punkter gäller för mobila enheter som används för synkronisering eller åtkomst till Södertälje kommuns e-post, kalender eller andra system som innehåller information som ägs av kommunen.

- I de fall Södertälje kommun påbjuder användaren av den mobila enheten ett Enterprise Mobility Management-verktyg (EMM-program) ska detta installeras.
- Enheten skyddas med tvingande PIN-kod eller grafiskt lösenord.
- För att få åtkomst till program och data krävs säkerhetsmässigt godkända lösningar.
- Applikationer och programvaror (Appar) som installeras på mobila enheter ska bekostas av användaren, om inte annan överenskommelse har gjorts med arbetsgivaren.
- De av kommunen godkända metoder för autentisering ska användas för åtkomst till kommunens tjänster.
- Den mobila enheten ska låsas efter 10 minuters inaktivitet om den befintliga utrustningen och tekniska plattformen medger detta. Nyanskaffad utrustning ska alltid kunna uppfylla detta krav.
- Kommunikation ska skyddas till en nivå som har framkommit vid informationsklassningen. De av kommunen rekommenderade lösningarna ska användas.
- De risker som finns med att använda trådlösa publika nätverk ska beaktas.
- Beaktande måste alltid göras till risken av att obehöriga kan ta del av medförd information, t.ex. människor som befinner sig i samma lokal.
- Registrering och säkerhetsinställningar på enheten ska göras av behörig tekniker innan utlämning av utrustning för mobil datoranvändning får ske.

6.7 Relaterad dokumentation

Detaljerad beskrivning över roller och dess ansvar finns på http://kanalen/styrning/policyerochriktlinjer/ under rubriken *IT* och *Informationssäkerhet och systemförvaltning*

7. Personal och informationssäkerhet

Det här avsnittet beskriver hur informationssäkerhet beaktas inför, under och efter en medarbetares anställning eller kontraktering av leverantörer samt konsulter.

7.1 Rekrytering

Vid rekrytering ska den platssökande kontrolleras på lämpligt sätt särskilt om anställningen medför åtkomst till sekretessbelagda uppgifter eller på annat sätt omfattar säkerhetskritiska aktiviteter. Kontroll och uppföljning av den arbetssökandes referenser och formella meriter såsom CV, meritförteckning, yrkeslegitimationsinnehav och bisysslor ska göras. Kontrollerna ska stå i proportion till Södertälje kommuns krav på tjänsten, den typ av information som den anställde ska hantera samt de förmodade riskerna. Inför byte av tjänst internt ska en förnyad bedömning ske.

7.1.1 Sekretessavtal

Som en del av sina avtalsskyldigheter ska anställda, uppdragstagare och tredjepartsanvändare godta och underteckna de villkor och förhållanden som anges i anställningsavtalet eller dess bilagor.

Samtliga anställda ska göras medvetna om sina skyldigheter enligt anställningsavtalet samt informeras om gällande regler för informationssäkerhet och sekretess. Innan åtkomst till Södertälje kommuns informationssystem medges, ska det också meddelas att bristande efterlevnad av riktlinjer, föreskrifter och instruktioner kan vara misskötsel vilket är ett brott mot anställningsavtalet. Ansvar för att informera om detta ligger på anställande chef.
Motsvarande ska i förekommande fall regleras i avtal med uppdragstagare och andra användare, som inte är anställda

7.2 Under anställning och kontrakterat uppdrag

Information om hur informationssäkerheten hanteras inom Södertälje kommun ska lämnas till nyanställd personal. Alla anställda, elever och kontrakterad personal ska göras medvetna om hot och problem som rör informationssäkerheten, sitt ansvar och sina skyldigheter. Detta görs genom utbildning och genom korrekt användning av informationsbehandlingsresurser.

7.2.1 Chefens ansvar

Alla med arbetsledande funktion ska kräva att anställda, uppdragstagare och tredjepartsanvändare tillämpar säkerhet i enlighet med kommunens beslutade riktlinjer och rutiner.

Varje kontorsledning ansvarar för att skapa förutsättningar så att alla anställda, elever samt kontrakterad personal kan hantera information och informationsbehandlingsresurser på ett säkert sätt. Detta görs genom att genomföra utbildningar och fastställa kontors specifika anvisningar/instruktioner.

7.2.2 Utbildning i informationssäkerhet

Verksamhetsansvarig chef ansvarar för att all personal och elever i verksamheten utbildas i informationssäkerhet inklusive betydelsen av incidentrapporteringar. Vid förändringar och tillägg av styrande dokumentation kring informationssäkerhet (riktlinjer, anvisningar, instruktioner), har alla chefer ett ansvar att dessa förändringar och tillägg blir kända av personalen.

7.2.3 Disciplinära åtgärder

Om en anställd bryter mot regelverket, ska denne i första hand utbildas. Om den anställde trots utbildning, fortsätter att bryta mot reglerna så kan det få (eller leda till) arbetsrättsliga konsekvenser.

7.3 När medarbetare slutar eller byter tjänst

Det ska finnas en fastställd rutin för hantering av personal som avslutar eller förändrar sin anställning. Denna rutin ska säkerställa att åtkomsträttigheter förändras eller upphör och att tillgångar återlämnas vid anställningens förändring eller avslut.

Denna rutin ska även i förekommande fall omfatta uppdragstagare, elever och andra användare, som inte är anställda.

Vid anställningens eller kontraktets upphörande ansvarar varje användare för att de allmänna handlingarna gallras och bevaras enligt gällande regler och lagrum.

Vid anställningens eller kontraktets slut, ansvarar varje användare för att datorer, telefoner, nycklar, passerkort och annan utrustning som har erhållits för tjänsten, återlämnas.

8. Hantering av tillgångar

Alla informationstillgångar, dyr och svårersättlig utrustning ska ha en ansvarig. Olika tillgångar har olika värde och bör därför ges olika skydd.

8.1 Ansvar för tillgångar

8.1.1 Förteckning över tillgångar, system och databaser

Tillgångar ska märkas, förtecknas och ha en utsedd ägare. Tillgångar kan vara databaser, datorutrustning, manualer mm. Chef inom respektive verksamhet och kontor ska tillse att detta hanteras. Utförandet kan ske hos outsourcingpartner. Förteckning görs lämpligt i ett kommun-centralt systemstöd

Förteckningen ska innehålla namn på system/applikation/databas, driftmiljö, produktägare, krav på riktighet, sekretess, tillgänglighetskrav. Även krav på arkiveringstid, logg och driftsmiljö ska finnas med.

Vid informationsutbyte mellan interna system ska informationsklassningen beaktas så att högre klassad information inte sänds till ett system som inte är avsedd för detta.

8.1.2 Ägarskap av tillgångar

All information och alla tillgångar ska ägas av en utsedd organisationsenhet.

8.1.3 Tillåten användning av tillgångar

Regler för hur information och tillgångar tillhörandes informationsbehandlingsresurser får användas ska utformas, dokumenteras och införas.

8.1.4 Återlämnande av tillgångar

Alla anställda och kontrakterad personal skall då anställning eller uppdrag upphör på eget initiativ återlämna all utrustning, passerkort, nycklar osv. som har erhållits av Södertälje kommun.

8.2 Klassificering av information

Klassificering av information betyder att inordna informationen i säkerhetsnivå avseende sekretess, riktighet och tillgänglighet. Klassning görs för att säkerställa att informationen har ett lämpligt skydd baserat på värdet.

8.2.1 Klassning av information

Informationsklassificering är ett sätt att värdera och prioritera information utgående från verksamhetens krav på konfidentialitet (sekretess), tillgänglighet, riktighet och spårbarhet. Utifrån kraven kan informationen hanteras på ett effektivt sätt med rätt avvägda skyddsnivåer.

Informationsägaren är den som ansvarar för att informationsklassningen genomförs, Informationssäkerhetsansvarige fungerar som stöd för planering och genomförande. När det gäller information som lagras i IT-system blir även systemägare, systemförvaltare och kanske även leverantörer viktiga parter.

8.2.2 Märkning och hantering av information

Information som är belagd med sekretess ska märkas så att detta framgår. Information som omfattas av säkerhetsskyddslagstiftningen hanteras inte i detta dokument.

Kommunens informationshantering styrs främst av bestämmelser i Tryckfrihetsförordningen och Offentlighet- och sekretesslagen (OSL) 2009:400. Huvudregeln i Tryckfrihetsförordningen är att informationen ska vara tillgänglig för allmänheten, den s.k. offentlighetsprincipen. Undantag från huvudregeln utgör information som med stöd av reglerna i OSL kan omfattas av sekretesskydd. Det är väsentligt att varje anställd känner till vilken information, inom i första hand sitt eget ansvarsområde, som är sekretessbelagd och hur den ska hanteras. Prövning av sekretess föreligger för viss information varje gång en begäran om utlämning sker. Detta oavsett om handlingen är sekretessbelagd eller inte

8.3 Hantering av lagringsmedia

8.3.1 Hantering, transport och avveckling av flyttbara lagringsmedia.

Vid hantering av lagringsmedia (t.ex. hårddisk, CD/DVD, USB-minnen) skall det säkerställas att all känslig information skyddas på ett adekvat sätt, t.ex. att lagringsmediet hålls under uppsikt eller att informationen är krypterad och skyddad med lösenord.

Om lagringsmediet ska överlämnas till någon individ eller organisation utanför Södertälje kommun ska det i säkerställas att den informationen som finns på mediet endast är av sådan art att den kan delges mottagaren. Sekretessbedömning ska göras enligt OSL.

Trasig, förbrukad eller inaktuell lagringsmedia ska destrueras.

8.4 Relaterad dokumentation

Informationsklassning ska genomföras med hjälp av SKL's verktyg KLASSA: https://klassainfo.skl.se/

9. Styrning av Åtkomst

Det här avsnittet beskriver vilka regler som gäller för behörighet och åtkomst till Södertälje kommuns system och information. Åtkomst till information, IT-system och nätverk ska styras utifrån verksamhetsbehov, lagkrav och säkerhetskrav.

9.1 Verksamhetskrav för styrning av åtkomst

Den som har behov av åtkomst till informationstillgångar för att kunna utföra sina arbetsuppgifter ska tilldelas åtkomsträttigheter (behörigheter). Även om det är tekniskt möjligt för en anställd eller konsult att få åtkomst till information som inte krävs för de egna arbetsuppgifterna, t.ex. uppdragsgivares information, är det inte tillåtet att aktivt söka efter sådan och liknande uppgifter.

Systemadministratörer/-tekniker ska ha individuella användaridentiteter. Om det inte är möjligt ska manuell logg föras.

Åtkomst/behörighet ska tilldelas formellt och endast efter behov samt följas upp regelbundet. Den som använder Södertälje kommuns informationstillgångar på ett sätt som strider mot kommunens regler, kan bli föremål för en disciplinär åtgärd.
Interna och externa nätverk betraktas som informationstillgångar varför åtkomst styrs enligt samma principer som åtkomststyrning i övrigt. Kommunens nätverk ska vara tydligt avgränsat mot omvärlden genom lämplig teknik.

9.2 Hantering av användaråtkomst

9.2.1 Registrering och avregistrering av användare

Det är eftersträvansvärt att så långt som det är möjligt knyta all autentisering till verksamhetssystem till användaridentiteten (AD-kontot). Ansvarig för att användarna får rätt behörigheter är respektive systemägare/informationsägare… Anledningarna till att det är fördelaktigt att koppla användarnas användaridentitet och autentisering till verksamhetssystem är flera:

- För att på ett effektivt sätt kunna stänga en användares åtkomst och behörigheter till många system när denne slutar.
- För att minska förekomsten av återanvända lösenord i olika system och minska risken att lösenord som används inom kommunen sprids vid intrång hos en extern leverantör.
- För att tillse att lösenordet skyddas, har tillräcklig komplexitet samt byts med regelbundna mellanrum i samtliga system.

Användaridentiteter skapas, avslutas och styrs automatiserat utifrån informationen i lönesystemet för anställda samt från skolans verksamhetssystem för elever.

Externa konton och konton för timanställda i den gemensamma katalogen skapas efter beställning.

Det ska finnas en tydlig process för tilldelning respektive borttagning av användaridentiteter. Alla användaridentiteter ska vara unika och knutna till en individ.

Rutin för regelbunden uppdatering av utdelade användaridentiteter ska finnas och rutinen ska även innehålla kontroll av att inte upphörda användaridentitet återanvänds.

Beställning av uppläggning av ny användare, ändring av befintlig användare, samt borttagning av användare görs skriftligen av avdelningschefen med hjälp av en blankett.

I de fall när en outsourcing partner används som t ex molntjänst ska vid avtalets slut all information, tillhörande Södertälje kommun och som har lagrats om denna, raderas och elimineras ur tjänsteleveratörens system, om inget annat har angetts. Södertälje kommun

ansvarar för att, i de fall data ska arkiveras, säkerställa innehållet till arkivfunktion innan upphörandet av tjänsteleverans enligt gällande lagar och regler om bevarande av information. Data som hanteras av molntjänst och som ska, efter avveckling av tjänst, bevaras eller överföras till annat system ha kompatibelt standardiserat format för att säkerställa överföringen.

9.2.2 Tilldelning av användaråtkomst

Behörighet tilldelas normalt via rollbaserad behörighet (RBB) d.v.s. genom att användaren tilldelas (blir medlem i) en roll som ger tillgång till systemresurser.

Behörighet till en systemresurs får tilldelas direkt till användaren om systemresursen inte kan tilldelas genom RBB. När nedan talas om tilldelning av roller avses även sådan direkt tilldelning av behörighet.

9.2.3 Hantering av privilegierade åtkomsträttigheter

Med privilegierade behörigheter avses sådana roller som ger användaren administrativ åtkomst till operativsystem, databassystem, kommunikations- och systemprogram eller motsvarande.

Tilldelning och användning av privilegierad åtkomsträtt ska begränsas, styras och ska följa arbetsuppgifterna, inte personen.

Särskilda rättigheter/priviligierad åtkomst ska användas mycket restriktivt. När särskilda rättigheter används för t.ex. åtkomst till operativsystem, databassystem, nätverksadministration etc. ska användaridentiteten så långt det är möjligt vara en annan än den som nyttjas i den normala verksamheten.

9.2.4 Hantering av användares konfidentiella autentiseringsinformation

Användaren skall initialt tilldelas ett tillfälligt lösenord som omedelbart skall ändras vid första inloggning. Ett initialt lösenord som inte är bytt inom en viss tid ska automatiskt spärras för användning.

9.2.5 Granskning av användares åtkomsträttigheter

Det skall göras en uppföljning av användarnas behörigheter till de informationssystem och resurser som är verksamhetskritiska eller innehåller personuppgifter. Uppföljningen ska göras minst två gånger per år av respektive systemägare/informationsägare och ska minst omfatta om det finns skäl för användaren att ha kvar sin behörighet. Om något inte stämmer ska detta omgående korrigeras.

Lösenord och koder ska generellt vara individuella och får inte överlåtas eller lånas ut. Möjlighet till spårbarhet ska alltid finnas.

SQL-, ODBC-, ADO (ActiveX Data Objects)-tjänster får inte installeras så att IT-systemets databas kan anropas från klient utan att åtkomsten prövas.

9.2.6 Borttagning eller justering av åtkomsträttigheter

En förteckning ska föras över alla utdelade användaridentiteter och rutin ska finnas för regelbunden uppdatering av denna förteckning. Rutinen ska även innehålla kontroll av att inte upphörda användaridentitet återanvänds. Historikfunktion ska finnas.

9.3 Användaransvar

Så långt det är möjligt ska användarna nå de resurser som de behöver för sin tjänst genom att de loggar in i Södertälje kommuns Windows-miljö (Active Directory). Så långt det är tekniskt möjligt skall Single Sign On lösning användas till de olika systemen, programmen och tillämpningarna.

Detaljer i användarnas ansvar framgår av dokumentet Användarförsäkran Dnr 16/179

9.4 Styrning av åtkomst till system och tillämpningar

9.4.1 Begräsning av åtkomst till information

Säkerhetsmekanismer ska användas för att begränsa åtkomst till och inom IT-systemen. Logisk åtkomst till program och data ska begränsas till behöriga användare. En bestämd lagringsstruktur som utgår från verksamhetens organisation och ansvarsförhållanden ska användas för att skydda mot obehörig åtkomst. Informationen lagras i anvisade system eller i särskilda kataloger på centrala lagringsplatser.
System som innehåller information som omfattas av lag om säkerhetsskydd får endast vara åtkomliga från kommunens datorer och verksamhetsställen.

9.4.2 Säkra inloggningsrutiner

Inom Södertälje kommun tillämpas stark autentisering, vid inloggning via VPN.
Engångslösenord skall antingen skickas krypterat eller i en separat kanal så att de inte kan fångas upp av t ex spionprogram.

Vid inloggning till nätverk eller system ska inte lösenordet visas i klartext.

IT-enhetens framtagna lösningar ska användas för åtkomst, autentisering, identifiering till nätverk samt system.

9.4.3 System för lösenordshantering

För att undvika svaga lösenord, ska system och nätverk säkerställa att lösenorden är av god kvalitet. Även systemens hantering av lösenord ska vara på ett säkert sätt – lösenord ska t.ex. inte lagras i klartext i systemet, de ska inte skickas i epost till användaren utan ska då vara ett engångslösenord som måste bytas vid första inloggningen. Om detta inte sker kan användarens behörighet spärras/låsas.

9.4.4 Användning av systemverktyg

Systemverktyg som används för att övervaka tjänsteleveranser ska överenskommas och beslutas i samråd med Södertälje kommun. Med detta avses samtliga verktygsprogram som har förmåga att kringgå säkerhetsåtgärder i system och program. Verktygen får endast användas under begränsad tid och för ett definierat och dokumenterat syfte.

9.4.5 Åtkomstkontroll till källkod för program

Mjukvara ska alltid köpas från välkända och etablerade leverantörer. I händelse av att ett program ska inköpas från en mindre leverantör, ska en riskanalys genomföras och bedömning av konsekvenserna göras ifall leverantörens verksamhet upphör. Deponering av källkod hos handelskammaren kan övervägas.

Åtkomst till systemfiler och källkod ska styras.

10. Kryptering

Detta avsnitt beskriver hur korrekt och verkningsfull kryptering ska införas och upprätthållas.

10.1 Kryptografiska säkerhetsåtgärder

10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder

- Kommunens godkända programvara för kryptering ska användas
- Nycklar och algoritm ska skyddas mot obehörig åtkomst och manipulation minst lika väl som den information kryptot avser att skydda
- Möjligheten för obehöriga att ta del av information genom avlyssning ska beaktas

10.1.2 Nyckelhantering

Det ska finnas ett system för bevakning av certifikats giltighet, alternativt att utfärdaren/säljaren bevakar giltighet och informerar Södertälje kommun eller dess driftsansvarig minst 50 dagar innan certifikatets sista giltighetsdag om att certifikat närmar sig sin bortre tidsgräns och upphör att gälla. Det ska finnas säkerhetskopia på certifikat.

11. Fysisk säkerhet

Detta avsnitt beskriver hur otillåten fysisk åtkomst till lokaler, information, IT- och kommunikationsutrustning och informationsbehandlingsresurser ska förhindras.

11.1 Säkra områden

11.1.1 Fysiska säkerhetsavgränsningar

Med säkra utrymmen avses utrymmen som är speciellt uppbyggda för att uppfylla högre krav på skal- och brandskydd samt säker tillgång till el och kyla.

11.1.2 Fysiska tillträdesbegränsningar

För att säkerställa att endast behörig personal ges tillträde till säkrade utrymmen, ska dessa utrymmen skyddas med hjälp av lämpliga tillträdeskontroller. Åtgärder ska vidtas för att förhindra att obehöriga får tillträde till utrymmen med informationstillgångar. Åtgärder ska även vidtas för att förhindra skador och störningar där tillgångarna är placerade.

Tillträdeskontroll ska tillämpas för att säkerställa att endast behörig personal får tillträde till säkrade utrymmen.

Tillträdeskontroll kan vara bemannade receptioner eller datoriserade passagekontrollsystem med individuella passagekort. Speciella krav på begränsning av tillträdet som kan finnas per individ, tid på dygnet etc. måste kunna tillgodoses.

11.1.3 Säkerställande av kontor, rum och anläggningar

Alla lokaler där kommunen bedriver verksamhet ska utformas och skyddas med tanke på risker för stöld och obehörigt tillträde.

Det fysiska skyddet ska vara i nivå med verksamhetens krav och risker. Utrustning som är viktig för verksamheten ska inte placeras så att den är allmänt tillgänglig.

11.1.4 Skydd mot yttre och miljörelaterade hot

Alla lokaler byggnader och rum där kommunen bedriver verksamhet ska ha ett övervägt skydd mot skada orsakad av brand, översvämning, explosion och andra former av naturliga eller av människa orsakad skada.

Hänsyn ska även tas till sådant som kan uppstå i angränsande utrymmen, t.ex. brand eller explosion i angränsande byggnad.

11.1.5 Arbeta i säkra utrymmen

Allt tillträde för att arbeta i säkra utrymmen ska loggas. Personer som behöver tillfällig behörighet kan ges sådan och då ska personen i varje stund ledsagas.

11.1.6 Leverans och lastningsområden

Platser dit obehöriga kan få tillträde och som ligger i anslutning till skyddade lokaler eller säkra utrymmen ska övervakas och skyddas med skalskydd. Leverans- och lastområden ska om möjligt utformas så att gods kan lossas, utan att leveranspersonalen får tillträde till andra delar av byggnaden.

11.2 Utrustning

Med informationsklassificering och riskanalys som grund ska åtgärder vidtas för att förhindra förlust eller skada på informationstillgångar och avbrott i verksamheten. Utrustning som tillhandahållits av arbetsgivaren/uppdragsgivaren ska behandlas på ett korrekt sätt.

11.2.1 Placering av utrustning och skydd

Beroende på placering av utrustningen krävs olika typer av fysiskt skydd. Hänsyn ska tas till eventuella miljörisker och obehörig åtkomst.

Brandskydd ska alltid finnas i eller i anslutning till server- och kommunikationsutrymmen.

Verksamhetskritisk information/material ska förvaras i säkerhetsskåp i låst utrymme.

Stöldbegärlig, dyr och svårersatt reservutrustning ska förvaras i låst utrymme med begränsat tillträde.

11.2.2 Tekniska försörjningssystem

Utrustning som är kritisk för verksamheten ska skyddas mot elavbrott och andra störningar. Elektricitet, avlopp, värme och ventilation samt luftkonditionering ska i tillräcklig omfattning för den verksamhet och system som de stödjer.

11.2.3 Kablagesäkerhet

Alla kablar – både starkström samt sådana som används för data- och teletrafik eller andra stödjande tjänster, ska skyddas mot avlyssning samt åverkan.

11.2.4 Underhåll av utrustning

Leverantörens rekommenderade underhållsplan för utrustningen ska i första hand följas.

Reparation och service får endast utföras av auktoriserad underhållspersonal.

Alla krav som ställs i försäkrings- Samt garantivillkoren ska vara uppfyllda.

I de fall där molntjänster används ska det finnas ett krav på Service Level Agreement (SLA). I ett SLA beskrivs den garanterade tiden som system ska vara tillgängligt samt åtgärdstider vid fel och maximal tid då system är otillgängliga. Oavsett driftsätt (egen regi, outsourcad eller moln), ska SLA-nivåer finnas och som ska beskriva det eventuella tillgänglighetsbehovet som finns eller varierar över tid. Kraven på tillgängligheten är betydelsefull vid drift av applikationer, funktioner och övriga tjänster. Dessa krav framgår i t ex klassificering av den information dessa bearbetar.

11.2.5 Utförsel av tillgångar

Utrustning som innehåller känslig information ska inte avlägsnas från Södertälje kommuns lokaler utan att tillstånd har erhållits från verksamhetens chef. Om det är möjligt ska tidsgräns anges för avlägsnande av utrustning.

11.2.6 Säkerhet för utrustning och tillgångar utanför Södertälje kommuns lokaler

Utrustning, persondatorer, handdatorer, mobiltelefoner, smartphones mm. som används utanför de egna lokalerna ska ha lika högt säkerhetsskydd som om den används i de egna, kommunala lokalerna. Särskild hänsyn ska tas till risken för stöld och obehörig informationsåtkomst.

Utrustning som används utanför kommunens lokaler ska ha tillräckligt försäkringsskydd.

11.2.7 Säker kassering eller återanvändning av utrustning

Lagringsmedia, som innehåller känslig information eller licensierade program, ska förstöras, avmagnetiseras eller överskrivas på ett säkert sätt, i samband med avveckling eller återanvändning.

11.2.8 Obevakad utrustning som hanteras av användare

Utrustning (PC, dator, surfplatta, smartphone) som används av medarbetare eller kontrakterad personal för Södertälje kommuns information ska låsas när enheten inte används eller när arbetsplatsen lämnas. Dator, surfplatta samt smartphone som inte används ska automatiskt låsas enligt IT-enhetens bestämmelser.

11.2.9 Regel om rent skrivbord och tom skärm

Känslig och kritisk information på papper eller på elektroniska lagringsmedia ska låsas in i t.ex. kassaskåp när de inte används och i synnerhet när lokalerna är obemannade

Datorer, smartphones, läsplattor ska ha skydd mot obehörig åtkomst, förlust eller skada. Detta skydd kan vara skärmsläckare, lås, PIN-kod, kryptering, etc.

Dokument som innehåller känslig eller sekretessbelagd information ska omedelbart efter utskrift avlägsnas ur skrivaren.

12. Driftsäkerhet

Det här avsnittet beskriver hur säker och korrekt drift skall upprätthållas samt hur driften sköts av tjänsteleverantör.

12.1 Driftsrutiner och ansvar

IT-chef eller utsedd systemägare/informationsägare är ansvarig för ledning av kommunens gemensamma informationstillgångar. Ansvar för kommunens system kan ligga på annan roll än IT-chefen, t ex. specifikt utsedd ansvarig eller extern leverantör när kommunen är beställare av en IT-tjänst. Inom kommunen ska det finnas skriftlig dokumentation med övrig ansvarsfördelning, t.ex. driftsansvarig leverantör, driftsform, systemägare etc.

12.1.1 Dokumenterade driftsrutiner

Driftrutiner ska finnas dokumenterade och hållas aktuella. Ändringsrutin för driftdokumentation ska tillämpas. I drift- och/eller förvaltningsåtagande för IT system (utlagd drift, SaaS) ska anvisningar finnas för att regelbundet kunna ta del av leverantörers systemrevisioner.

Driftrutinerna ska minst innehålla instruktioner för att utföra säkerhetskopiering, hantering av fel, lista över kontaktpersoner vid oväntade drifts- eller tekniska problem, hanteringsregler för sekretessbelagda utdata, återstarts- och återställningsrutiner samt hantering av logginformation.

12.1.2 Ändringshantering

- Fastställda processer för hantering av förändringar i IT-system ska alltid följas
- Process för ändringshantering ska följas även för åtgärder som är av rent infrastrukturell karaktär
- Motsvarande process ska följas när det gäller IT-system som anskaffas från eller driftas av extern leverantör
- Samtliga ändringar ska kunna härledas till en ansvarig beställare

12.1.3 Kapacitetshantering

Kapacitetshantering syftar till att förutse och beakta kapacitets- eller prestandaförändringar. Regelbunden hantering av kapaciteten ska genomföras av drifts- eller SaaS-leverantören. Detta är särskilt viktigt för de system som bedöms som verksamhetskritiska.

12.1.4 Separation av utvecklings-, test- och driftsmiljöer

Kommunen eller IT-tjänstleverantören ska ha tillgång till en systemmiljö med åtskilda produktions-, utvecklings- och testmiljöer. Säkerhetsreglerna för produktionsmiljöerna ska i relevanta delar även gälla för utvecklings- och testmiljöerna.

Det är viktigt att testmiljön efterliknar driftmiljön så långt som det är möjligt. Det är också viktigt att känsliga data inte kopieras in i testmiljön samt att den information som finns i testmiljön skyddas. Så långt som det är möjligt ska anonymiserad eller påhittad information användas i testmiljön.

I de fall där kommunen använder sig av tjänsteleverantör sker dessa separationer, utveckling och tester, hos tjänsteleverantören. Kommunen involveras därmed inte alltid i dessa processer.

12.2 Skydd mot skadlig kod

Åtgärder för att upptäcka, förebygga och skydda mot skadlig programkod ska genomföras. Rutiner ska också finnas för hur användarna ska uppmärksammas på risker och regler.

Dessa åtgärder ska innehålla föreskrifter och instruktioner för hantering av skadlig kod (virus) och till detta relaterade incidenter. Föreskrifterna och instruktionerna ska innefatta anvisningar för hur användare ska identifiera, åtgärda och rapportera möjliga virusangrepp. Om IT-systemet driftas av annan part än Södertälje kommun ska leverantören uppvisa att åtgärder finns för skydd mot skadlig kod.

12.2.1 Säkerhetsåtgärder mot skadlig kod

Skydd mot skadlig kod baseras på programvara, användarnas säkerhetsmedvetande samt skyddsåtgärder för åtkomst.

Samtlig utrustning som används inom Södertälje kommuns verksamheter ska om det är tekniskt möjligt innehålla program för detektering av skadlig kod (antivirusprogram). Dessa program ska automatiskt uppdateras regelbundet. Dessa program ska genomföra automatiska kontroller av hårddisken så att skadlig kod upptäcks.

Skyddsåtgärder ska vidtas för riskerna som är förknippade med att ladda ner filer och program, antingen från eller via ett externt nätverk eller från annat medium.
Det ska finnas tekniska lösningar förhindra åtkomst till webbsidor/-adresser (URL) med skadlig påverkan och/eller olämpligt innehåll genom filter mot internetanvändning till olämpliga webbsidor.

12.3 Säkerhetskopiering

Utrymme eller skåp som innehåller säkerhetskopior ska brandskyddas i enlighet med normer från försäkringsinstitut. Kritiska säkerhetsfunktioner som återställning av säkerhetskopior ska övas och kontrolleras minst en ggr/år. Om IT-systemet driftas av annan part än Södertälje kommun, ska leverantören uppvisa att säkerhetskopiering hanteras enligt dessa regler. Detta gäller även om systemet köps som tjänst av en s.k. molnleverantör (SaaS).

12.3.1 Säkerhetskopiering av information

Nivån och frekvensen på säkerhetskopiering av information ska definieras av systemägarrepresentant eller motsvarande, eventuellt med stöd av kontorens dokumenthanteringsplan. Säkerhetskopieringen ska schemaläggas, dokumenteras och utföras av behörig personal. Säkerhetskopior ska inte förvaras i samma lokaler som driftmiljön.

12.4 Loggning och övervakning

12.4.1 Loggning av händelser

Kritiska och säkerhetsrelevanta händelser i drift och datakommunikation ska övervakas samt vara spårbara. Varje transaktion ska kunna knytas till den som utfört den. Detta ska i första hand åstadkommas med automatiska loggningsfunktioner. Alternativt redovisas händelser skriftligt. Övervakningen ska inriktas på drift-, transaktions- och säkerhetshändelser. Loggning görs av driftsorganisationen samt av kontoren i deras specifika verksamhetssystem.

12.4.2 Skydd av logginformation

Loggar ska skyddas mot obehörig åtkomst och ändringar.

12.4.3 Administratörs- och operatörsloggar

Nödvändiga loggar ska insamlas för att ha relevant spårbarhet och kunna genomföra relevant felsökning. Vid behov ska loggarna kunna redovisas för kommunen.

12.4.4 Synkronisering av tid

Korrekt inställning och exakt funktion av datorklockor är väsentligt för att säkerställa giltigheten hos de loggar som förs. Samtliga datorklockor i kommunens nätverk eller system som skapar loggar enligt ovan tidssynkroniseras automatiskt och tiden ska vara spårbar till den svenska officiella tidsskalan UTC (SP).

12.5 Styrning av driftsystem

12.5.1 Installation av program på driftsystem

För att minimera risken för obehörig åtkomst till känslig information ska lämpliga sårbarhetsanalyser, scanningar samt penetrationstester genomföras i samband med driftsättning av nya system och applikationer samt vid större förändringar. Efter driftsättning ska minst en årlig uppföljning utföras.

Det ska finnas instruktioner angående hur ändringar får ske. Alla ändringar som sker i drift ska vara loggade och kunna följas upp.
System och systemändringar får inte driftsättas om de inte har testats, granskats, dokumenterats och godkänts. I de fall säkerhetsbrister identifieras skall en riskanalys utföras och allvarliga brister åtgärdas innan produktionssättning.

Vid leverans ska det finnas systemdokumentation.

Konfigurering och systemförändringar ska kunna följas upp i efterhand och spåras.

12.6 Hantering av tekniska sårbarheter

12.6.1 Hantering av tekniska sårbarheter

Det är viktigt att i rätt tid hämta in information om den tekniska sårbarheten hos informationssystem i drift. Det gäller också att bedöma Södertälje kommuns utsatthet för sådan sårbarhet och att sätta in lämpliga åtgärder för att hantera risken. Vid dessa åtgärder ska följande hanteras:

- Förteckning ska finnas över Södertälje kommuns tillgångar, programleverantör, versionsnummer och produktägare. Se vidare avsnitt 8.1
- Uppdateringar hanteras och bedöms av Södertälje kommuns IT-drift samt outsourcing leverantör. Södertälje kommuns IT-enhet ska informeras löpande
- Uppdateringar (patch) ska alltid bedömas innan den installeras
- Konsekvensen av att avstå respektive genomföra en säkerhetsuppdatering ska alltid analyseras
- Relevanta utgivna säkerhetspatchar ska testas och installeras så fort som möjligt efter testning. Detta gäller både operativsystem och applikationer. Extremt kritiska säkerhetspatchar installeras senast inom 5 arbetsdagar
- Logg över tagna beslut genomförda åtgärder och uppdateringar ska finnas
- Hanteringen av uppdateringar ingår i den fastställda förändringsprocessen men kan vid speciellt kritiska lägen följa rutinen för incidenthantering

12.6.2 Restriktioner för installation av program

Södertälje kommun är mycket restriktiv med behörigheter som lokal administratör på datorer. Användarna har begränsningar i programinstallationer på datorerna, vid behov av nya program hanteras dessa installationer av IT-driften.

I händelse att det finns användare som är lokala administratörer på sina datorer och därför kan installera mjukvara själv, måste detta ske kontrollerat. Det får endast finnas godkända program, tillämpningar, script eller dylikt på dessa enheter. Användaren har inte rätt att göra installationer, även om det är tekniskt möjligt. Detsamma gäller de användare (IT-personal) som har en användaridentitet med administrativa behörigheter.

12.7 Överväganden gällande revision av informationssystem

12.7.1 Revisionskontroller för informationssystem

IT-systeminriktad revision ska noggrant planeras, överenskommas och regelbundet genomföras för att minska risken för störningar i verksamhetsprocesserna.

Åtkomst till granskningsverktyg för informationssystem ska begränsas för att hindra eventuellt missbruk eller otillåten påverkan.

13. Kommunikationssäkerhet

Detta avsnitt beskriver hur säkerheten av information i nätverk och dess stödjande resurser uppnås.

13.1 Hantering av nätverkssäkerhet

13.1.1 Säkerhetsåtgärder för nätverk

Södertälje kommuns nätverk ska styras och skyddas från obehörig förändring, åtkomst och andra obehöriga aktiviteter. IT-enheten ansvarar för förvaltningen av nätverket och nätverksutrustningen. Datordriften hanteras av IT-enheten med hjälp av en outsourcingpartner.

Nätverk och genomförda ändringar ska vara dokumenterade med god spårbarhet av gjorda förändringar. Dokumentationen ska vara aktuell och förvaras oåtkomlig för obehöriga enligt informationsklassningsmodellen.

Brandväggar ska förhindra att obehörig nätverkstrafik släpps in till Södertälje kommuns interna nätverk. God spårbarhet ska finnas i hur brandväggarna är konfigurerade samt vilka aktiviteter som skett via brandväggarna.

Övervakning av nätverk, serverresurser och hård- samt mjukvara skall ske. I de fall annan part sköter övervakningen ska detta regleras med avtal. I avtalet ska åtkomstregler och rättigheter regleras. I övervakningsansvaret ingår att påtala brister/stopp i kommunikationen för drabbade enheter. Beredskap ska finnas för att åtgärda störningar i nätverksfunktonalitet.

13.1.2 Säkerhet hos nätverkstjänster

För varje IT-system, molntjänst eller applikation som är ansluten till Södertälje kommuns gemensamma IT-infrastruktur ska det finnas en förteckning över de nätverkstjänster som används. Med nätverkstjänster avses trafik mellan systemet och en server eller klient.

Användarnas tillgång till samtliga nätverkstjänster ska begränsas med hjälp av åtkomstkontroll och baseras på tjänstens behov (need-to-know).

Södertälje kommuns IT-drift ska säkerställa att samtliga nätverkstjänster som används är korrekt uppsatta och underhålls. Om säkerheten i nätverkstjänsterna inte kan säkerställas ska användningen anpassas med hänsyn till detta.

13.1.3 Separation av nätverk

Interna och externa nätverk betraktas som informationstillgångar varför åtkomst styrs enligt samma principer som åtkomststyrning i övrigt. Kommunens nätverk ska vara tydligt avgränsat mot omvärlden genom lämplig teknik. Säkerheten i kommunens nätverk ska kunna styras genom att dela upp nätet i separata logiska nätverksdomäner, t.ex. en extern, en för elever samt en intern domän som skyddas med rekommenderad teknik och skyddsåtgärder. Vidare ska nätverket kunna segmenteras så att kritiska tillgångar är extra skyddade

De trådlösa näten består av fyra nät. Nedanstående sammanfattning visar det huvudsakliga användningsområdet för respektive nät:

Nät	Användningsområde
Administrativt nät	Datorer som ägs av kommunen, och används av anställd eller förtroendevald

Pedagogiskt nät	Datorer som ägs av kommunen och används av studerande, elever och lärare.
Gästnät	Tillfälliga besökare till kommunens verksamheter.
IoT-nät	Nät för sensorer, AV-skärmar med mera

Samtliga nät ger åtkomst till Internet, och övervakas av den centrala tjänst som blockerar åtkomst till internetsidor som innehåller skadlig kod, eller som tillhör en kategori som bedömts vara olämplig utifrån användarförsäkran eller motsvarande riktlinjer.

13.2 Informationsöverföring

13.2.1 Regler och rutiner för informationsöverföring

Speciell hänsyn krävs vid kommunikation över organisationsgränser samt vid överföring av information som omfattas av sekretess.

13.2.2 Överenskommelser om informationsöverföring

Vid informationsöverföring mellan Södertälje kommun och externa parter ska det gemensamt bedömas behovet av skydd mot åtkomst, riktighet, tillgänglighet och spårbarhet. Det ska vara tydligt vem som ansvarar för vad.

För informationsöverföringen ska väl etablerade och säkra kommunikationslösningar användas, t.ex. kryptering.

Informationsöverföring mellan systemen inom Södertälje kommun ska hållas på en restriktiv nivå. Systemen ska i stor utsträckning vara sammankopplade med automatisk överföring. Informationsöverföring ska så långt det är möjligt ske utan mänsklig interaktion. I de fall där överföring sker automatiskt ska möjligheter finnas för spårbarhet och manuell kontroll av informationens riktighet.

13.2.3 Elektronisk meddelandehantering

Information inbegripen i elektronisk meddelandehantering som skickas över allmänt tillgängliga nätverk ska skyddas mot bedrägliga förfaranden samt obehörigt avslöjande, och modifiering.

13.2.4 Konfidentialitet och förbindelser om konfidentialitet

Sekretessavtal ska tecknas med medarbetare, konsulter, outsourcingpartners, leverantörer och övriga samarbetspartners som i sin yrkesroll eller uppdrag får ta del av Södertälje kommuns information om den kan vara sekretessbelagd enligt OSL.

Förbindelsen är en bekräftelse på att individen har informerats om tystnadsplikten och fungerar också som en försäkran att han/hon följer Södertälje kommuns bestämmelser.

Ett sekretessavtal bör minst innehålla:

- Åtgärder som krävs när avtalet upphör, anställning eller uppdrag avslutas
- Ägande av information
- Tillåten användning av Södertälje kommuns information
- Rätten att granska och övervaka aktiviteter som involverar konfidentiell information
- Åtgärder vid avtalsbrott

13.3 Relaterad dokumentation

Södertälje kommuns riktlinjer för e-post – finns på http://kanalen/styrning/policyer-ochriktlinjer/ under rubriken *Arkivering, diarieföring och E-post* samt *E-post.*

14. Inköp, utveckling och underhåll av system

Detta avsnitt innehåller de regler som gäller vid inköp, utveckling och förvaltning av informationssystem.

14.1 Säkerhetskrav på informationssystem

14.1.1 Analys och specifikation av informationssäkerhetskrav

Säkerhetskraven ska vara uppfyllda innan driftgodkännande till informationssystem kan ges.

Det är inte tillåtet att skapa, skaffa eller installera dubblerande funktioner inom de områden där kommunen har gemensamma lösningar om inte kommunstyrelsen beslutar om undantag.

14.1.2 Säkerställande av programtjänster på publika nätverk

Information som hanteras via tjänster på publika nätverk (Internet) ska skyddas mot bedrägliga förfaranden, samt obehörigt avslöjande och förändring.

Skyddet av information som hanteras via tjänster på publika nätverk ska innehålla:

- Autentisering av användaren minst på den nivå som informationsklassningen kräver
- Säkerställande att korrekt person genomför viktiga transaktioner, t ex genom stark autentisering eller digital signatur
- Identifierade och dokumenterade legala krav samt upphandlingskrav och avtal
- Krypterad överföring där det krävs (framkommer vid informationsklassningen)
- VPN-förbindelse ska användas i de fall behov av detta föreligger (framkommer vid informationsklassningen)
- Skydd för personuppgifter

14.1.3 Skydd av transaktioner i tillämpningstjänster

Information och transaktioner som hanteras i Södertälje kommuns program ska skyddas mot felaktiga eller ofullständiga överföringar, duplicering, bedrägligt förfarande samt obehörigt avslöjande eller förändring.

14.2 Säkerhet i utvecklings- och support processer

14.2.1 Regler för säker utveckling

I händelse av att Södertälje kommun beställer utveckling av ett system, ska systemutvecklingen alltid ske i enlighet med fastställda modeller och metoder. För samtliga informationstillgångar ska säkerhetskraven sammanställas utifrån genomförd riskanalys och informationsklassificering.

14.2.2 Rutiner för hantering av systemändringar

Ändringshantering av program och driftsättning ska ske enligt dokumenterade process- och rutinbeskrivningar. Produktionssättning ska genomföras i samråd med verksamheten och genomföras vid en tidpunkt då verksamhetens processer störs så lite som det är möjligt vilket oftast är utanför kontorstid eller helger. Det ska vara två personer utsedda som ansvarar för produktionssättningen.

14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö

I samband med underhåll och uppdatering av komponenter i systemplattform är det inte ovanligt att andra komponenter/applikationer som har beroende till den uppgraderade komponenten slutar fungera. På grund av detta skall alla ändringar i samband med uppgradering och säkerhetspatchning verifieras i testmiljö, innan de appliceras i driftsmiljö.

14.2.4 Restriktioner för ändringar av programpaket

Programpaket som kommer från extern programleverantör ska användas utan att modifieras eller förändras i dess funktion eller säkerhet. I övrigt ska Södertälje kommuns process för ändringshantering följas.

14.2.5 Principer för utveckling av säkra system

Innan ett system övergår från utveckling till förvaltning ska en dokumenterad överlämning genomföras där förvaltnings-/driftsorganisationen kommer överens om bl.a. SLA, backuper mm.

Det ska finnas en aktuell systemdokumentation över alla system som produktionssätts, dokumentationen ska endast vara tillgängliga för behöriga. Denna dokumentation ska inte kunna förändras av obehöriga.

14.2.6 Säker utvecklingsmiljö

Utvecklingsmiljön ska vara separerad från produktionsmiljön så att inte nätverk, program eller användare kan påverka produktionsmiljöerna. Testmiljön ska vara separerad från produktionsmiljön.

Tester ska ske enligt en separat testrutin och vara dokumenterade.

14.2.7 Outsourcad utveckling

Vid outsourcing av informationsbehandlingsresurs skall en riskanalys genomföras. Med underlag av resultatet från riskanalysen, eventuella åtaganden mot kunder och rättsliga krav skall krav specificeras i avtal.

I de fall som systemutveckling är outsourcat ska följande beaktas:

- Process för acceptanstester för att verifiera kvalitet och korrekthet i leverabler
- Bevis för att tillräcklig testning har genomförts för skydd mot att skadlig kod förs in vid leverans
- Bevis för att tillräcklig testning har genomförts för att skydda mot förekomsten av kända sårbarheter
- Licenser, äganderätt till kod och andra immateriella rättigheter

14.2.8 Säkerhetstestning

Ifall ett system utvecklas på uppdrag av kommunen ska denna utveckling på ett sådant sätt att det möjliggör säkerhetstester under utveckling och regelbundet i produktion.
Säkerhetstestning ska säkerställas att det genomförs av produktägare eller systemansvarig i samband med produktionssättning.

Omfattningen av testerna ska stå i proportion till systemets betydelse för verksamheten.

14.2.9 Acceptanstestning av system

System som har förändrats ska innan produktionssättning genomgå en testprocess som består av enhets-, system, integrations- och acceptanstester.

Acceptanstester genomförs alltid av den person, roll eller enhet som har beställt förändringen.

Vid säkerhetstestning kan automatiserade verktyg användas för t.ex. sårbarhetsscanning, kodgranskning etc.

14.3 Testdata

14.3.1 Skydd av testdata

Data i testmiljö bör inte innehålla verkliga persondata. I de fall där data i testmiljö innehåller verkliga persondata, ska de skyddas och hanteras på samma sätt som de hanteras i den skarpa miljön. Om möjligt bör fingerad data eller avpersonifierad data användas.

- Kopiering av produktionsdata ska loggas för att vara spårbar.
- Kopiering får endast ske efter skriftlig beställning från projektledare/ systemägarrepresentant/ systemförvaltare och ska registreras i ärendehanteringssystem eller motsvarande.

15. Leverantörsrelationer

Det här avsnittet beskriver hur säkerheten upprätthålls av de tillgångar som leverantörer har åtkomst till.

15.1 Informationssäkerhet i leverantörsrelationer

15.1.1 Informationssäkerhetsregler för leverantörsrelationer

Den som, för Södertälje kommun, bolag eller verksamheter, tecknar avtal med externa parter ansvarar för att avtalet även omfattar relevanta säkerhetskrav och att avtalet ger verksamheten möjlighet att följa upp säkerheten hos underleverantörer/externa parten. Systemägaren ansvarar även för att säkerställa att säkerhetsgranskning av såväl tjänst som leverantör sker i samband med avtalstecknande och därefter regelbundet.

Verksamheten ska ha en förteckning över aktuella leverantörer och avtalstider.

Följande punkter ska beaktas för informationssäkerheten i leverantörsrelationer:

- Förutom ett SLA ska ett Särskilt kravdokument undertecknas av leverantör som hanterar verksamhetens information utanför lokalerna eller på utrustning som ej ägs av Södertälje kommun, dess bolag eller verksamheter.
- Tillvägagångssätt för att hantera incidenter och kontinuitetsplanering rörande oförutsedda avbrott som är förknippade med leverantörens leverans till verksamheten.
- De resurser från extern leverantör som arbetar för Södertälje kommun, dess bolag eller verksamheter i verksamhetens lokaler ska genomgå utbildning i informationssäkerhet, se avsnitt *7.2.2 Utbildning i informationssäkerhet.*

15.1.2 Hantering av säkerhet inom leverantörsavtal

Det kravdokument som ska tecknas med leverantör eller ingå som en del av leverantörsavtalet ska innehålla punkter som:

- Informationsklassning och sekretessförbindelse

- Rättsliga krav inklusive hantering, definition och skydd av personuppgifter
- Regler för tillåten användning av Södertälje kommuns information
- Krav och rutiner för incidenthantering, särskilt rapportering
- Leverantörens skyldighet att uppfylla Södertälje kommuns säkerhetskrav
- Det kan även vara relevant att teckna sådant kravdokument med underleverantörer.

15.1.3 Försörjningskedja för informations- och kommunikationsteknologi

Södertälje kommun ska för varje leverantör säkerställa att:

- Leverantören ställer krav på rätt nivå av säkerheten på samtliga ingående komponenter, tekniska lösningar samt underleverantörer.
- Möjlighet finns för övervakning och validering att leveransen sker enligt avtal, både i omfattning och i fastställda säkerhetskrav.
- Det finns övervakning av de för Södertälje kommuns kritiska processerna. Denna övervakning är särskilt viktigt om leverantören outsourcar hela eller delar av beställd produkt eller tjänst.
- Det finns möjlighet till fullständig spårbarhet i tjänstens leverans och administration
- Leverantören försäkrar att produkten eller tjänsten fungerar som förväntat utan oväntade, oönskade eller dolda funktioner

Det ska finnas kontinuitetsplaner och/eller riskanalys gjord, ifall beställd produkt/tjänst blir otillgänglig.

15.2 Hantering av leverantörers tjänsteleverans

15.2.1 Övervakning och granskning av leverantörstjänster

Inom Södertälje Kommun ska det finnas rutiner för att granska och övervaka leveranserna från externa leverantörer.

Denna typ av övervakning och granskning kan ske genom ofta förekommande, återkommande och regelbundna möten med leverantörens representant där leveransen granskas, inträffade incidenter och leveransproblem analyseras och behov av kommande förändringar diskuteras.

15.2.2 Ändringshantering av leverantörers tjänster

Leveranser från en enskild leverantör kan under avtalstiden behöva förändras. Detta ska vara möjligt att genomföra enligt fastställda rutiner. I dessa rutiner ska minst följande ingå:

- Fastställt vem som är behörig att beställa förändring av leverans.
- Person som är behörig att förända avtalet.
- Uppdatering av avtal, informationssäkerhetspolicy och tillhörande regelverk.
- Behov av förnyad riskanalys och informationsklassificering.

16. Hantering av informationssäkerhetsincidenter

Det här avsnittet beskriver hur informationssäkerhetsincidenter ska rapporteras och hanteras.

16.1 Hantering av informationssäkerhetsincidenter och förbättringar

16.1.1 Ansvar och rutiner

Ledningsansvar och rutiner ska fastställas för att säkerställa en snabb, effektiv och ordnad respons vid informationssäkerhetsincidenter

16.1.2 Rapportering av informationssäkerhetshändelser

Incidenter och säkerhetsmässiga svagheter ska rapporteras snarast till systemägare och inforationssäkerhetsansvarig så att åtgärder för att minimera skada, åtgärda brister och utreda eventuell brottslighet kan påbörjas.

Det är viktigt att rapportera incidenter för att kunna bedöma vilka säkerhetsåtgärder som ska prioriteras. Incidentrapporteringen möjliggör att hotbildens relevans kan säkerställas och att satsningar görs på de viktigaste områdena. Exempel på incidenter som ska rapporteras är omfattande virusangrepp, intrång/intrångsförsök och manipulation/radering av information

16.1.3 Rapportering av svagheter gällande informationssäkerhet

Anställda, uppdragstagare och tredjepartsanvändare av informationssystem och -tjänster ska notera och rapportera alla observerade eller misstänkta säkerhetsbrister i system eller tjänster.

16.1.4 Hantering av informationssäkerhetsincidenter

När en incident har inträffat, som påverkar tillgängligheten i system eller IT-miljö, ska återställning till normalläge ske så snabbt som möjligt.

Vid misstanke om brott måste bevis insamlas innan eventuell återställning kan ske. Insamlandet måste ske med god kunskap om säkring av bevis och vid IT relaterade problem måste detta ske med hjälp av fackman.

16.1.5 Att lära av informationssäkerhetsincidenter

Det ska finnas metoder för att möjliggöra kvantifiering och övervakning av typer, volymer och kostnader för informationssäkerhetsincidenter

16.1.6 Insamling av bevis

Då en uppföljande åtgärd mot en person eller organisation efter en informationssäkerhetsincident innefattar en juridisk åtgärd (civil- eller brottmål) ska bevis kunna insamlas, bevaras och presenteras.

17. Kontinuitetsarbete

Att motverka avbrott i kommunens verksamhet och att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel i informationssystem samt att säkra återstart inom rimlig tid.

17.1 Kontinuitet för informationssäkerhet

Kontinuitetsplanering för verksamheten ska innefatta åtgärder för att identifiera och minska risker, förutom den allmänna riskbedömningsprocessen, begränsa konsekvenserna av skadliga incidenter och säkerställa att den information som krävs för verksamheten är tillgänglig.

17.1.1 Planering av kontinuitet för informationssäkerhet

Begreppet ”avbrottsplanering” ingår i ”kontinuitetsplanering” som den del av planeringen som syftar till att återupprätta IT-stödet i händelse av att det drabbats av avbrott.

Synonymt med begreppet kontinuitetsplan används kan också begrepp som katastrofplan och beredskapsplan förekomma. Konsekvenserna av störningar, allvarlig händelse och extraordinära händelser ska analyseras med hänsyn till inverkan på verksamheten. Kontinuitetsplaner ska upprättas och införas för att säkerställa att viktiga funktioner kan återställas inom rimlig tid och att verksamheten kan fortgå utan IT-stöd.

Arbetet med kontinuitetsplanering ska fokusera på den aktuella verksamhetens prioriterade åtaganden och verksamhetssystem. Det innebär planering och förberedelser av åtgärder så att verksamheten kan upprätthållas trots att allvarliga störningar/avbrott har inträffat.

Händelser som kan orsaka avbrott i verksamhetsprocesser ska identifieras tillsammans med sannolikheten och effekten av sådana avbrott och deras konsekvenser för informationssäkerheten.

17.1.2 Införa kontinuitet för informationssäkerhet

Inom respektive verksamhet ska planer utarbetas och införas för att upprätthålla eller återställa drift och säkerställa tillgänglighet till information på den nivå som krävs och inom erforderlig tid efter avbrott eller fel i kritiska verksamhetsprocesser.

Ett samlat ramverk för kontinuitetsplanering bör finnas för att säkerställa att alla planer är konsekventa, att informationssäkerhetskraven behandlas konsekvent och för att fastställa prioriteringar gällande test och underhåll av planerna.

För att minska konsekvenserna vid allvarliga störningar/avbrott i verksamheter med starkt IT beroende krävs en i förväg upprättad och dokumenterad kontinuitetsplan.

Systemägaren är ansvarig för att hålla systemets kontinuitetsplan aktuell samt att ställa krav på systemleverantörer att de har tillräcklig kontinuitetsplanering för kommunens verksamhet.

Kontorschefen är ansvarig för verksamhetens fortsatta kontinuitet vid händelse av avbrott i IT-stödet. Detta kan innebära att alternativt arbetssätt eller manuella rutiner måste på förhand definieras och etableras.

Verksamhetens ramverk för kontinuitetsplanering ska minst omfatta:

- Ansvar och befogenheter för kritiska rollinnehavare
- Informationskanaler och vilka man informerar
- Reservdriftalternativ
- Rutin för återstart
- Behov av utrustning/reservdelar
- Rutin för att uppdatera av avbrottsplanen

17.1.3 Styra, granska och utvärdera kontinuitet för informationssäkerhet

Kontinuitetsplaner för verksamheten ska testas och uppdateras regelbundet för att säkerställa att de är aktuella och verkningsfulla. Leverantörer av verksamhetskritiska system ska uppvisa genomförda tester eller andra bevis att deras kontinuitetsplan är aktuell och verkningsfull.

17.2 Redundans

17.2.1 Tillgänglighet för informationsbehandlingsresurser

Systemägarna ska ställa krav på respektive driftsleverantör för de viktigaste systemen att det finns systemredundans. Detta kan t.ex. ske genom att information kopieras över till alternativt driftplats, och att det till dessa båda finns flera olika anslutningsmöjligheter. I beredskapsplanen finns identifierat vilka system som är de viktigaste för kommunen.

Det ska även i beredskapsplanen finnas beskrivet alternativa sätt att kommunicera i händelse av att mail, e-post eller telefoni är utslaget.

18. Efterlevnad

Det här avsnittet beskriver hur överträdelser av juridiska, författningsenliga eller avtalsmässiga skyldigheter relaterade till informationssäkerhet ska undvikas.

18.1 Efterlevnad av juridiska och avtalsmässiga krav

18.1.1 Identifiering av gällnade lagstiftning och avtalsmässiga krav

Tillämpliga krav i författningar och i avtal liksom organisationens sätt att uppfylla dessa krav ska explicit definieras, dokumenteras och hållas uppdaterade för varje informationssystem och för organisationen som helhet.

Minimikraven för informationssäkerhet fastställs i lagar och förordningar. Tryckfrihetsförordningen ställer krav på att allmänna handlingar ska vara tillgängliga medan Offentlighets- och sekretesslagen (OSL) inskränker på handlingars offentlighet

18.1.2 Immateriella rättigheter

Kommunens hantering av programvarulicenser ska för kommungemensamma system hanteras av kommunens IT-enhet eller utsedd systemägare. Verksamhetsnära system och licenser hanteras av respektive verksamhet. I detta ansvar ingår att säkerställa att licenser köps på rätt avtal, att licenser återanvänds där det är möjligt och att kommunens verksamheter har tillgång till statistik över licensutnyttjande i kommunens IT-miljö. Programvaror ska användas i enlighet med avtal och licensregler.

18.1.3 Skydd av dokumenterad information

Chefer ska säkerställa att alla säkerhetsrutiner inom deras respektive ansvarsområden utförs korrekt för att uppnå efterlevnad av kommunens beslutade dokument

18.1.4 Skydd av personlig integritet och personuppgifter

Data- och integritetsskyddet ska säkerställas enligt lagstiftningen och avtalsklausuler om sådana finns (t ex. samtycke). Detta ska även regleras med utomstående parter och externa leverantörer.

Hanteringen av personuppgifter i IT- system ska dokumenteras och anmälas till personuppgiftsombud eller kommande dataskyddsombud. Detta sker bland annat i samband med informationsklassificeringen.

18.1.5 Reglering av kryptografiska säkerhetsåtgärder

Innan användning av kryptering samt tillhörande nyckelhantering ska IT-enheten kontaktas och rådfrågas.

18.2 Granskningar av informationssäkerhet

18.2.1 Oberoende granskning av informationssäkerhet

Revisionsaktiviteter ska samordnas med systemdrift för att tjänsteleveranser inte ska påverkas. Genomgång ska göras av Södertälje kommuns ramverk, processer och tillhörande resurser inom Informationssäkerhet (Ledningssystemet för informationssäkerhet). Detta ska granskas och bedöms vara fortsatt lämpligt, effektivt och i tillräcklig omfattning. Denna genomgång ska dokumenteras.

18.2.2 Efterlevnad av säkerhetspolicy, regler och standarder

Chefer ska se till att alla anställda och kontrakterad personal följer samtliga säkerhetsrutiner inom respektive ansvarsområde.

Södertälje kommun förbehåller sig rätten att granska innehållet i all IT-utrustning som tillhör kommunen för att kontrollera efterlevnaden av säkerhetsreglerna.

18.2.3 Granskning av teknisk efterlevnad

Informationssystem ska regelbundet kontrolleras vad avser efterlevnad av riktlinjer.