Regler
för
informationssäkerhet i Sollentuna kommun

Antagna av kommunstyrelsen 2014-02-19 § 26, dnr 2014/0041 KS.063

Innehåll

1. Inledning

Fullmäktige har i december 2011 antagit en policy för informationssäkerheten i Sollentuna kommun. Av policyn framgår att kommunstyrelsen ska fastställa regler för kommunens informationssäkerhetsarbete.

Sollentuna kommun arbetar kontinuerligt för att skydda information på ett optimalt sätt. Information är en viktig tillgång som måste behandlas och skyddas samtidigt som tillgången till informationen och öppenheten inom kommunens verksamheter ska vara så stor som möjligt.

Offentlighetsprincipen ska alltid tillämpas vid hantering av kommunens information.

All information som produceras, lagras och sprids ska ha rätt nivå av skydd med utgångspunkt i informationens värde.

Syftet med kommunens informationssäkerhetsarbete är att säkerställa informationens

- konfidentialitet/sekretess
- tillgänglighet
- riktighet
- spårbarhet

2 Omfattning

Dessa regler ska fungera som en basnivå för informationssäkerhetsarbetet i Sollentuna där regelverket sätter ramar och tillämpningsanvisningar fastställs för specifika områden.

3 Process för informationssäkerhet inom Sollentuna kommun

Processen för informationssäkerhet i Sollentuna kommun baseras på ISO/IEC 27001:2006 - Ledningssystem för informationssäkerhet (LIS) och anges i detalj i tillämpningsanvisningar. Skiss över processen för informationssäkerhet finns i avsnitt 22 i dessa regler.

4 Organisation för informationssäkerhetsarbetet

4.1 Kommunstyrelsens ansvar

Kommunstyrelsen leder, samordnar och granskar kommunens arbete med informationssäkerhet.

Kommunstyrelsen ansvarar för att ta fram tillämpningsanvisningar till dessa regler.

4.2 Nämndernas ansvar

Respektive nämnd ska upprätthålla informationssäkerheten inom sin verksamhet.

4.3 Ansvar inom förvaltningarna

4.3.1 Förvaltningschef

Inom varje förvaltning är förvaltningschefen ansvarig för informationssäkerheten.

Förvaltningschefen kan utse informationssäkerhetskoordinatorer för att stödja förvaltningschefen i arbetet med informationssäkerhet.

4.3.2 Medarbetare

Varje medarbetare ansvarar för informationssäkerheten inom det egna området.

Medarbetare ska följa tillämpningsanvisningar inom informationssäkerhet för medarbetare i Sollentuna kommun och bör delta i säkerhetsrelaterade utbildningar.

4.3.3 Säkerhetschef

Säkerhetschefen är informationssäkerhetschef och har det övergripande ansvaret att samordna informationssäkerhetsarbetet inom kommunen.

Säkerhetschefen utarbetar, förvaltar och följer upp policyn, reglerna och tillämpningsanvisningarna.

4.3.4 Informationsägare

Informationsägare är den som äger och ansvarar för information.

Informationsägaren ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids.

4.3.5 Informationsförvaltare

Informationsförvaltare är den som är utsedd att förvalta informationen.

Informationsförvaltaren är ansvarig för att informationen skyddas genom informationsklassning.

4.3.6 Objektsägare/systemägare

Objektsägare/systemägare är den som ansvarar för att det finns adekvata system eller liknande som hanterar verksamhetens information.

En utpekad objektsägare ska finnas för alla kommunens system. Objektsägaren ansvarar för att det finns adekvat skydd för den information som lagras eller bearbetas i systemet.

4.3.7 Förvaltningsledare

Förvaltningsledaren är den som förvaltar det system som informationen finns i.

Förvaltningsledaren ansvarar för systemets funktion ur ett verksamhetsperspektiv samt stöder användarna av systemet.

4.4 Samverkansforum för informationssäkerhet

Det ska finnas ett samverkansforum för informationssäkerhet i kommunen. Detta forum har till uppgift att samverka i frågor som rör informationssäkerhet.

Forumet ska ledas av säkerhetschefen och bör ha medlemmar från samtliga förvaltningar.

5. Hantering av informationssäkerhet mot externa parter

5.1 Definition

Med externa parter avses här konsulter, entreprenörer och andra utförare av kommunal verksamhet och övriga samarbetsparter med vilka kommunen har avtal.

5.2 Avtal

Innan en extern part medges åtkomst till information hos kommunen ska lämpliga och relevanta skyddsåtgärder vidtas. Ett avtal ska tecknas som definierar villkor och förutsättningar för åtkomst, eventuell bearbetning och övrig hantering av informationen. Avtalet ska, avseende den information som hanteras, reglera frågor om konfidentialitet/sekretess, tillgänglighet, riktighet och spårbarhet samt i övrigt följa kommunens regler för bland annat it- och informationssäkerhet.

Den som anlitar konsult eller annan samarbetspartner ansvarar för att det i avtal med dessa säkerställs att informationssäkerheten upprätthålls.

I avtal om extern drift av it-system ska säkerställas att

- kommunen har rätt att granska informationssäkerheten hos leverantören och dennes eventuella underleverantörer
- leverantörens åtagande avseende informationssäkerhet kan förändras av kommunen

5.2.1 Personuppgiftsbiträdesavtal

Ett personuppgiftsbiträdesavtal ska tecknas i de fall där den externa parten hanterar information enbart i enlighet med instruktion från kommunen.

För det fall en extern part anlitar underleverantörer ska den som anlitar den externa parten försäkra sig om att personuppgiftsbiträdesavtal även tecknas med underleverantören.

Om personuppgifter kommer att behandlas i ett land utanför EU/EES ska den personuppgiftsansvarige se till att något av undantagen från förbudet mot överföring till tredje land kan tillämpas.

5.3 Sekretessförbehåll

I förekommande fall ska kommunen fatta beslut om sekretessförbehåll enligt offentlighet- och sekretesslagen.

6 Anskaffning av it-system m.m.

6.1 Rutin

Det ska finnas en rutin för anskaffning av nya it-system, förvaringsplatser, utrustning eller annan metod för digital eller analog hantering av information som påverkar informationssäkerheten. Anskaffningen ska göras i samråd med de funktioner som ansvarar för it, informationssäkerhet, arkiv, juridik, ekonomi och administration. Innan anskaffning ska samråd ske med personuppgiftsombudet på respektive myndighet.

I överenskommelser med utomstående leverantör ska säkerställas att granskning kan ske utan att säkerheten för Sollentuna kommun äventyras.

Säkerhetskrav på nya informationssystem m.m. ska identifieras under analysfasen av systemutvecklings- eller anskaffningsprocessen.

6.2 Risk- och sårbarhetsanalys

Före anskaffning och införande av nya it-system ska en risk- och sårbarhetsanalys göras i syfte att få en tillräcklig säkerhetsnivå för den information som systemet ska innehålla.

6.3 Gallringsutredning

Före anskaffning och införande av nya system ska en gallringsutredning göras i syfte att kartlägga vilka allmänna handlingar som ska bevaras respektive gallras i systemet.

Mot bakgrund av gallringsutredningen ska gallringsbeslut fattas och föras in i respektive verksamhets dokumenthanteringsplan.

6.4 Förteckning enligt PUL

Vid anskaffning och införande av nya system ska den eventuella personuppgiftsbehandling som sker i systemet förtecknas enligt personuppgiftslagen (PUL).

7 Riskhantering och kartläggning

7.1 Definition

Riskhantering innebär identifiering, värdering och prioritering av risker i informationshanteringen i syfte att identifiera skyddsåtgärder för dessa.

Skyddsåtgärderna ska vara väl avvägda och kostnadseffektiva.

7.2 Riskanalyser

En analys avseende hot, risker, sårbarhet och liknande som kan påverka informationshanteringen ska göras regelbundet inom respektive verksamhet. En riskanalys ska också göras om särskilt behov uppstår.

En riskanalys ska göras vid anskaffning, komplettering, uppdatering och avveckling av it-system m.m.

7.3 Förteckning av informationstillgångar

Kommunens informationstillgångar ska identifieras och dokumenteras i dokumenthanteringsplaner.

Om informationstillgången utgörs av personuppgifter ska denna informationstillgång även dessa förtecknas enligt personuppgiftslagen.

7.4 Klassning av information

All information i kommunen ska klassas utifrån informationens skyddsvärde. Klassning ska göras mot bakgrund av respektive dokumenthanteringsplan, förteckning enligt personuppgiftslagen och i enlighet med tillämpningsanvisning till dessa regler.

7.5 Hantering av informationstillgångar

Sollentuna kommuns informationstillgångar får endast hanteras i av kommunen godkänd utrustning eller tjänst.

Det är inte tillåtet att hämta in eller installera program eller liknande via elektronisk post, internet, annan filöverföring eller via flyttbart media utan godkännande.

7.6 Granskning av system m.m.

Granskning av informationssystem och den information som hanteras i system ska ske regelbundet.

Åtkomst för till exempel granskningshjälpmedel till system ska begränsas för att hindra eventuellt missbruk eller otillåten påverkan.

8. Personal och säkerhet

8.1 Chefers ansvar

Respektive chef ansvarar för att alla medarbetare informeras om gällande regler för informationssäkerhet.

8.2. Kontroll av vissa blivande medarbetare

Inför anställning av blivande medarbetare i ledande ställning eller annars på särskilt känsliga befattningar ska en säkerhetskontroll göras på lämpligt sätt. Kontrollen ska stå i proportion till den åtkomst av känslig information som personen kommer att ha i sitt arbete.

8.3. Upphörande av anställning

Då en anställning eller ett uppdrag upphör ansvarar närmaste chef för att behörigheter spärras och informationsrelaterad utrustning återlämnas.

Informationstillgångar som tillhör Sollentuna kommun ska återlämnas i samband med att anställning eller uppdrag upphör.

8.4. Förändring av anställning

Om förändring i anställning medför nya arbetsuppgifter och ansvar ska behörigheter ses över. Ansvarig chef ska se till att varje anställd har rätt behörigheter för aktuell tjänst.

8.5 Sekretess

För anställda inom kommunen är sekretess och tystnadsplikt reglerat i lag. Varje medarbetare ska informeras om detta.

9 Mobil användning av IT och distansarbete

9.1 Mobil användning

Vid mobil användning av it ska som huvudregel kommunens it-arbetsplats användas. Annan användning ska godkännas av närmaste chef.

9.2 Distansarbete

Vid distansarbete ska som huvudregel kommunens it-arbetsplats användas.

Vid distansarbete ska lämpliga säkerhetsanordningar och skyddsåtgärder finnas.

Den anställde ska iaktta aktsamhet om den information och utrustning som hanteras på distansarbetsplatsen.

10. Fysisk säkerhet

10.1 Inledning

Kommunens informationstillgångar ska skyddas från fysiska skador och förstörelse.

10.2 Arkivbeständighet

Sådana informationstillgångar som ska bevaras, ska bevaras på ett arkivbeständigt sätt.

10.3 Säkrade utrymmen

10.3.1. Skalskydd och skydd av kontor m,m.

Skalskydd ska i lämplig omfattning användas för att skydda utrymmen där information och informationsbehandlingsutrustning finns.

Byggnader och lokaler ska i lämplig omfattning skyddas mot avlyssning och liknande.

10.3.2. Tillträdeskontroll

Utrymmen där information förvaras ska skyddas genom lämpliga tillträdeskontroller för att säkerställa att endast behörig personal får tillträde.

10.3.3. Allmänna tillträden, leverans- och lastutrymmen

Platser för leverans- och lastutrymmen och andra platser där obehöriga personer kan komma in ska bevakas och förses med system för tillträdeskontroll.

Lokaler för leverans- och lastutrymmen ska skyddas genom förstärkt skalskydd.

10.4 Skydd av utrustning

10.4.1. Placering och skydd av utrustning

Utrustning som hanterar konfidentiell eller sekretesskänslig information ska placeras så att onödigt tillträde minimeras.

10.4.2. Tekniska försörjningssystem

Utrustningen ska skyddas mot elavbrott och andra störningar orsakade av avbrott i tekniska försörjningssystem.

10.4.3. Kablageskydd

Kablar och utrustning ska vara tydligt märkta för att minska handhavandefel som t.ex. sammankoppling av fel nätverkskablar av misstag.

10.4.4. Underhåll av utrustning

Utrustning ska underhållas i enlighet med verksamhetens behov.

Tidpunkt och omfattning på underhåll ska anges i ett servicenivåavtal (SLA).

10.4.5. Säkerhet för utrustning utanför kommunens lokaler

Utrustning som används utanför kommunens lokaler ska skyddas mot risker för att utrustningen eller dess information avlyssnas, manipuleras, förstörs eller försvinner.

10.4.6. Säker avveckling eller återanvändning av utrustning

Vid avveckling av media som innehåller eller har innehållit skyddsvärd, känslig information eller licensierade program ska informationen förstöras, utplånas eller överskrivas genom användning av teknik som försvårar rekonstruktion. Alternativt ska mediet förstöras fysiskt.

Rutiner och verktyg för detta ska finnas.

10.4.7. Avlägsnande av utrustning

Utförsel av it-utrustning utanför kommunens lokaler innehållande kommunens information ska godkännas av närmaste chef.

10.5 Skydd av information som ej är digital

För skydd av ej digital information gäller motsvarande regler som för utrustning enligt 10.4.

11 Åtkomst till information

11.1 Tilldelning av åtkomst till information

11.1.1 Användaridentiteter

Varje användare i kommunens it-system ska ha en unik användaridentitet.

Tilldelning av dessa identiteter ska registreras.

11.1.2 Behörigheter

Användare ska ha åtkomst endast till den information och de tjänster som de fått behörighet att använda.

Användarnas behörighet i kommunens it-system ska registreras och vidmakthållas.

Varje användares behörighet ska vara riktig och aktuell i förhållande till den tjänst eller uppdrag som användaren har vid varje tidpunkt.

En dokumenterad rutin för registrering och avregistrering av användare i kommuns it-system ska finnas.

Det ska finnas rutiner och tekniskt stöd för kontroll och administration av tilldelade behörigheter.

11.1.3 Särskilda behörigheter

Särskilda behörigheter, som går utöver normal åtkomst i IT-system ska tillämpas restriktivt.

Granskning av de särskilda behörigheterna ska göras kontinuerligt.

11.1.4 Lösenordshantering

Tilldelning av lösenord ska ske genom en dokumenterad och sekretesskyddad rutin.

11.2 Användares ansvar

11.2.1 Användning av lösenord

Självvalda lösenord ska hållas hemliga och inte kunna associeras till användaren på ett enkelt sätt.

Lösenord får inte lagras oskyddat i det IT-system där det används.

Användare ska genast ändra lösenord när det finns indikation om att säkerheten för lösenord har äventyrats samt omgående rapportera incidenten.

11.2.2 Obevakad utrustning

Obevakad databehandlingsutrustning ska lämnas avloggade eller skyddade med låsmekanism för bildskärm och tangentbord. Dessa enheter ska vara skyddade med lösenord, aktivt kort eller liknande autentiseringsfunktion när de inte används.

11.2.3 Dokument med konfidentiell eller hemlig information

Information får inte förvaras så obehöriga kan ta del av den.

Dokument innehållande konfidentiell eller hemlig information ska, i de fall gemensamma skrivare används, omedelbart efter utskrift avlägsnas ur skrivaren.

Finns funktion för fördröjd/styrd utskrift (PullPrint) ska denna användas.

12 Styrning av åtkomst till information

12.1 Begränsning av åtkomst

Begränsning av åtkomst ska baseras på riskanalyser, behov av åtkomst samt vilken roll användaren har.

Möjlighet att spåra åtkomst till information ska finnas genom tekniska och administrativa lösningar.

12.2 Isolering av känsliga system

Verksamhetssystem som är särskilt känsliga för förluster kräver särbehandling.

Isolering av verksamhetssystemet kan uppnås med fysiska eller logiska metoder.

13. Drift av it-system och analog hantering av information

Med it-system jämställs här även analog hantering av information om den är sytematiserad.

13.1 Rutiner

Det ska finnas rutiner för drift av kommunens it-system för att säkerställa informationen i systemen.

Rutinerna ska dokumenteras.

13.2 Förändring i it-system

Alla förändringar i kommunens it-system ska hanteras i en ändringshanteringsprocess.

Av processen ska framgå hur förändringarna ska planeras, koordineras, schemaläggas, dokumenteras och kvalitetssäkras.

13.3 Fördelning av driftansvar

Då det är möjligt ska driftansvar för kommunens it-system fördelas på flera personer för att minska risken för obehörig eller oavsiktlig förändring eller missbruk av information.

13.4 Uppdelning av it-miljöer

Om möjligt ska utvecklings-, test- och produktionsmiljöer åtskiljas för att minska risken för obehörig åtkomst till eller ändringar av informationen i systemen.

14 Hantering av informationsbärande media

14.1 Hantering av flyttbara och stationära media

Rutiner och skyddsåtgärder ska finnas för att skydda stationär och flyttbara media, t ex datorer, läsplattor och s.k. smarta telefoner.

Nivån på skyddsåtgärderna ska stå i proportion till informationens skyddsvärde.

15 Övervakning

15.1 Loggning

Loggning ska göras utifrån informationsklassning och riskanalys för it-system och annan informationshantering.

Loggning kan i särskilda fall även göras om det finns befogad anledning att misstänka otillåten användning av kommunens information eller andra oegentligheter.

Loggning ska omfatta användaraktiviteter, avvikelser, oregelbundenheter och andra informationsskyddsrelaterade händelser.

Användare ska informeras om att loggning sker.

Åtgärder som utförs av system- och nätverksadministratörer ska loggas. Manuell loggning ska tillämpas om funktioner saknas för automatisk loggning.

Det är viktigt att beakta de krav som finns för att skydda individers personliga integritet.

15.2 Övervakning av systemanvändning

Det ska finnas rutiner och system för övervakning och analys av kommunens verksamhetssystem.

Syftet är att upptäcka brister i informationssäkerheten inom områdena konfidentialitet, riktighet och tillgänglighet.

15.3 Skydd av logginformation

För att säkerställa att data inte ändras eller raderas ska loggningsresurser och logginformation skyddas mot manipulering och obehörig åtkomst.

Loggar ska förvaras under en bestämd tidsperiod och omfattas av gallringsbeslut.

16 Kryptering

Kryptering ska användas om möjligt för att skydda information om en riskanalys visar att behovet finns.

Ett nyckelhanteringssystem ska finnas för att stödja Sollentuna kommuns användning av krypteringsteknik.

17 Hantering av incidenter

17.1 Rapportering av informationssäkerhetshändelser

Det ska finnas en rutin för händelserapportering av informationssäkerhets-relaterade incidenter. Rapportering av incidenter ska ske omedelbart i enlighet med fastställd rutin.

Kommunens användare ska känna till rutinen.

17.2 Rapportering av säkerhetsbrister

Det ska finnas en rutin för händelserapportering av brister i it-miljön som kan påverka informationssäkerheten.

Kommunens användare ska känna till rutinen.

17.3 Hantering av incidenter och förbättringar

Det ska finnas en process för hantering av informations- och it-säkerhetsincidenter med fastställda roller och ansvar.

Det ska finnas en funktion inom Sollentuna kommun som har till uppgift att hantera it-säkerhetsincidenter.

18 Kontinuitetsplanering

18.1 Process för kontinuitetsplanering

För varje verksamhetsprocess ska det finnas en kontinuitetsplanering för att motverka avbrott och upprätthålla informationsskyddet.

Syftet med processen är att minimera följderna för organisationen efter förlust av information samt säkerställa återhämtning av informationen.

Händelser som kan orsaka avbrott i verksamheten ska kontinuerligt identifieras i syfte att bedöma sannolikheten för incidenter och konsekvenser för informationsskyddet.

Kontinuitetsplaneringen ska göras genom en risk- och sårbarhetsanalys.

19 Efterlevnad

19.1 Kommunstyrelsens uppsikt

Enligt kommunallagen ska kommunstyrelsen ha uppsikt över de övriga nämndernas förvaltning. Kontroll av efterlevnaden av dessa regler sker enligt detta uppsiktsansvar.

19.2 Dataintrång och missbruk av information

Kommunens information är avsedd för den verksamhet som bedrivs på respektive myndighet.

Anställda och därmed jämförbara personer får bara söka efter och ta del av sådan information som man behöver för att utföra sina arbetsuppgifter.

Arbetsgivaren har rätt att, genom åtgärder för övervakning, kontrollera och förhindra att missbruk sker.

19.3 Skydd av personuppgifter

Varje myndighet i kommunen ska säkerställa att berörda medarbetare känner till reglerna om behandling av personuppgifter och integritetsskydd.

19.3.1 Personuppgiftsbiträdesavtal

Varje myndighet ska säkerställa att det finns personuppgiftsbiträdesavtal kopplat till varje avtal som innebär behandlingar av personuppgifter.

20 Tillämpningsanvisningar

Kommunledningskontoret ska utfärda tillämpningsanvisningar till dessa regler.

21 Definitioner

Begrepp	**Förklaring**
Analog hantering/förvaring av information	Hantering/förvaring av t.ex. pappersdokument, akter, kartotek eller hängmappar. Förvaringsplatsen kan vara t.ex. arkivlokal eller aktskåp.
Användare	Individ som utnyttjar informationstillgångar
Autentisering	Kontroll av uppgiven identitet.
Dokumenthanteringsplan	Systematisk presentation av de allmänna handlingar/information som hanteras av en myndighet.
Förvaltningsledare	Förvaltningsledaren är den som förvaltar det system som informationen finns i.
Gallringsbeslut	Beslut som medger att allmänna handlingar får förstöras så att de inte kan återskapas.

Begrepp	Förklaring
Hemlig information	Information som omfattas av sekretess enligt offentlighets- och sekretesslagen
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten.
Identitet	Unik beteckning för en viss individ.
Information	Med information avses all information som hanteras inom hela den kommunala verksamheten oavsett om den behandlas manuellt eller med IT-baserade system och oberoende av i vilken form eller miljö den förekommer.
Informationsbehandlingsresurs	System, tjänst eller infrastruktur för informationsbehandling, eller de lokaler där dessa finns.
Informationsförvaltare	Av informationsägare bemyndigad person som ansvarar för klassning och hantering av ett informationsobjekt eller dokument.
Informationsklassning	Ett formellt sätt att fastställa rätt skyddsnivå för information.
Informationssäkerhet	Säkerhet beträffande informationstillgångar avseende förmågan att upprätthålla önskad sekretess, riktighet, tillgänglighet och spårbarhet.
Informationssäkerhetsincident	Säkerhetshändelse som kan/kunnat få/har fått allvarliga konsekvenser för verksamheten Enskilda eller en serie av oönskade eller oväntade informationssäkerhetshändelser vilka med stor sannolikhet kan äventyra verksamheten och hota informationssäkerheten
Informationssäkerhets-koordinator	Funktion som samordnar informationssäkerhetsarbetet
Informationstillgångar	En organisations informationsrelaterade tillgångar. 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.)
Informationsägare	Informationsägare är den som skapar och/eller fastställer information.
It-system	En sammansställning av datorer, minnesenheter, program, kommunikationsutrustningar, metoder och procedurer organiserade med uppgift att genomföra elektronisk behandling av information i syfte att tillgodose ett uttalat behov.

Begrepp	Förklaring
It-säkerhetsincidenter	Enskilda eller en serie av oönskade eller oväntade it-säkerhetshändelser vilka med stor sannolikhet kan äventyra It-system
Klient	Klient är programvaran (hårdvaran) som används för att komma åt en informationsresurs.
Konfidentialitet	Skydd mot obehörig åtkomst till information.
Kontinuitetsnivå	Verksamhetens acceptabla nivå av förhållandet mellan risk och kostnad.
Kontinuitetsplan för verksamheten	Dokument som beskriver hur verksamheten skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod
Kontinuitetsplanering	En metod för att säkerställa organisationens leveransförmåga genom att planera för fortsatt verksamhet vid förlust av operativ förmåga. .
Logg	Insamlad information om de operationer som utförs i ett IT-system. Logg ger spårbarhet för händelser.
Medarbetare	Den som är anställd i Sollentuna kommun
Media	Fysiskt objekt som innehåller data.
Objektsägare	Den som ansvarar för att det finns adekvata system eller liknande som hanterar verksamhetens information.
Operativsystem	Program som skapar miljö att exekvera andra program/system på en specifik hårdvara
Outsourcing	Drift av IT-system utförs av annan organisation.
Personuppgiftsbiträdesavtal	Ett skriftigt avtal mellan en personuppgiftsansvarig och ett personuppgiftsbiträde.
Policy	Anger ledningens viljeinriktning och stöd för informationssäkerhet. Policyn beskriver ”att något ska finnas”.
Regler	Anger vad som skall göras för att uppfylla de övergripande målen i policyn
Riktighet	Egenskap att information inte obehörigen, av misstag eller på grund av funktionsstörning har förändrats
Risk	Produkten av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad.
Riskanalys	Process som identifierar säkerhetsrisker, bestämmer deras betydelse och identifierar skyddsåtgärder.

Begrepp	Förklaring
Riskhantering	Samordnade aktiviteter för att leda och styra en organisation med avseende på risk
Sekretess	Skydd för information i enlighet med offentlighets- och sekretesslag (2009:400)
Sekretessförbehåll	En inskränkning i någons rätt att utnyttja eller lämna vidare information
Skalskydd	Skydd av fysiskt utrymme
Skyddsvärde	det värde en informationsmängd har efter att informationen klassats
SLA [Service Level Agreement]	Dokument som reglerar vad som överenskommits mellan systemägare och tjänsteleverantör gällande främst tillgänglighet i drift och förvaltning av visst IT-system.
Spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i IT-systemet till en identifierad användare.
Sårbarhet	Brist i skyddet av en tillgång exponerad för hot.
Säkerhet	Egenskap eller tillstånd som innebär skydd mot risk i samband med insyn, förlust eller påverkan; oftast i samband med medvetna försök att utnyttja eventuella svagheter.
Tillgänglighet	Säkerhetsprincip med innebörden att informationstillgångar är tillgängliga för behöriga användare, i förväntad utsträckning och inom önskad tid
Tillämpningsanvisningar	Styrdokument fastställt av tjänsteman. Beskriver tillämpning av antagna regler.
Ändringshantering	Processen för att på ett strukturerat sätt samla in behov och önskemål om förändring, beskriva förändringens påverkan, värdera och prioritera dessa och utifrån detta besluta och genomföra ändringar.
Ändringshanteringsprocess	En process för att göra medvetna beslut vid förändring av it-system. Innehåller exempelvis beskrivning av förändring, riskhantering och återställningsrutin

22. Process för informationssäkerhet inom Sollentuna kommun