



Informationssäkerhetsplan för Eskilstuna kommun

Informationssäkerhetsplanen med tillhörande instruktioner styr Eskilstuna kommuns informationssäkerhetsarbete. Informationssäkerheten är den del i organisationens lednings- och kvalitetsprocess som anger hur kommunens information ska hanteras på ett säkert sätt.

Informationssäkerhetsplanen med tillhörande instruktioner ersätter delar av säkerhetsplan för Eskilstuna kommun 2005-2007, antagen av kommunfullmäktige den 24 november 2005, § 8.

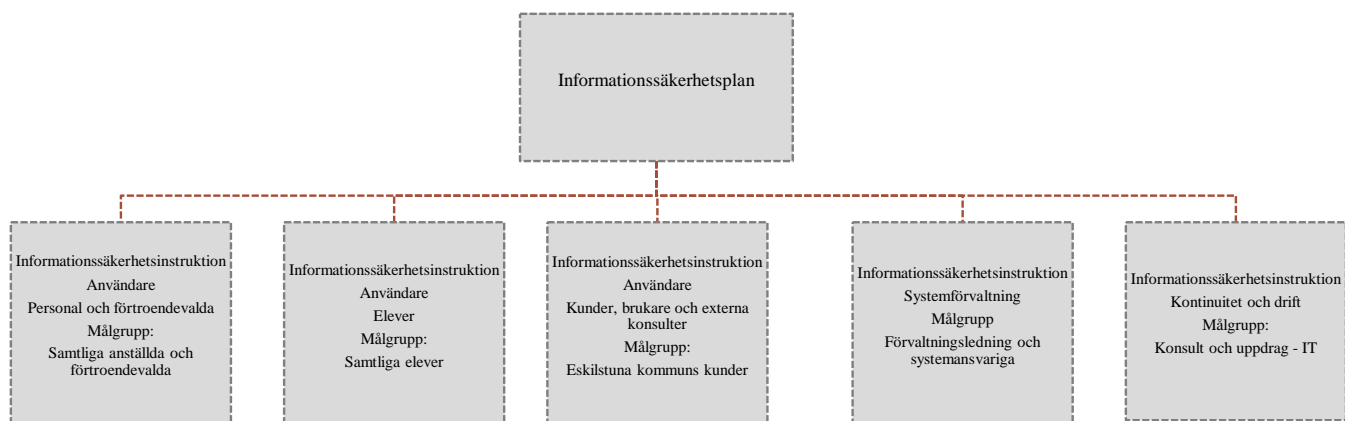
Om innehållet i informationssäkerhetsplanen strider mot något annat dokument som berör samma område gäller informationssäkerhetsplanen.

Planen är antagen av kommunfullmäktige 30 maj 2013, § 154, och gäller från och med 12 juni 2013. Reviderad av kommunfullmäktige den xxx 2014, § xxx.

Innehållsförteckning:

| Avsnitt | | Sid |
|---------|--|-----|
| 1. | Planens roll i informationssäkerhetsarbetet | 3 |
| 2. | Definitioner | 4 |
| 3. | Allmänt om informationssäkerhet | 6 |
| 4. | Avgränsning – samband och gränssnitt med andra processer | 7 |
| 5. | Mål och strategier | 8 |
| 6. | Organisationsstruktur informationssäkerhet | 9 |
| 7. | Roller och ansvar | 10 |
| 8. | Generella krav | 13 |
| 9. | Sanktioner | 16 |
| 10. | Uppföljning och översyn | 16 |
| 11. | Publicering | 16 |

1. Planens roll i informationssäkerhetsarbetet



Figur 1 Eskilstuna kommuns informationssäkerhetsplan med tillhörande informationssäkerhetsinstruktioner som vänder sig till olika målgrupper.

Syftet med informationssäkerhetsplanen är bland annat att fungera som styrdokument för de underliggande informationssäkerhetsinstruktionerna. Informationssäkerhetsplanen redovisar kommunfullmäktiges viljeinriktning och mål för informationssäkerhetsarbetet i Eskilstuna kommun.

Planen konkretiseras i nedanstående informationssäkerhetsinstruktioner:

- Informationssäkerhetsinstruktion användare.
 - Personal och förtroendevalda
 - Elever
 - Kunder, externa konsulter och brukare
- Informationssäkerhetsinstruktion förvaltning (beskriver hur systemägare och systemansvariga ska förvalta informationssystem).
- Informationssäkerhetsinstruktion kontinuitet och drift (beskriver hur Konsult och Uppdrag – IT ska hantera informationssystem).

Samtliga dokument som gäller för Eskilstuna kommun avseende informationssäkerhet finns dokumenterade på internportalen.

2. Definitioner

| | |
|--------------------------------|---|
| Arbetsgivaren: | Med uttrycket avses arbetsgivaren Eskilstuna kommun. Med uttrycket avses också funktionen som uppdragsgivare för de förtroendevalda som är utsedda av kommunen. |
| BITS: | Basnivå för informationssäkerhet. |
| Brukare: | Fysisk person som genom särskilt beslut är föremål för en kommunal insats. |
| Elev: | Elever inskrivna vid skola i Eskilstuna kommun och som har tillgång till IT-utrustning, nätverk med mera från Eskilstuna kommun. |
| Förtroendevald: | De personer som innehar politiskt uppdrag för Eskilstuna kommun och har tillgång till IT-utrustning, nätverk med mera från Eskilstuna kommun. |
| Incidenthantering: | Vidtagande av åtgärder efter någon form av incident till exempel angrepp av skadlig kod. |
| IP-adress: | Internet Protocol address. Det är ett unikt nummer som används som adress för den grundläggande standarden för trafik på internet och som identifierar din dator. |
| ISO/IEC 27000 | ISO 27000-serien ger ett strukturerat och effektivt arbetssätt för verksamheter som strävar efter förbättrad intern kontroll över informationssäkerheten. Utgör grunden för LIS – Ledningssystem för informationssäkerhet – som är den nivå som MSB numera rekommenderar. |
| ITIL: | Information Technology Infrastructure Library. Är principer för att hantera IT-infrastruktur, processer för bl.a. incident- och förändringshantering, kontinuitetsplan etc. |
| IT-utrustning: | All den utrustning som används av Eskilstuna kommun för elektronisk/-digital hantering. |
| Kommunlednings- | Den förvaltning inom Eskilstuna kommun som har i uppdrag att leda kontoret och samordna kommunens angelägenheter. |
| Konsult (extern): | Representant från leverantör som på uppdrag av Eskilstuna kommun har tillgång till IT-utrustning, nätverk, verksamhetssystem med mera från kommunen. |
| Konsult o uppdrag-IT (KoU-IT): | Konsult och uppdrag är en förvaltning inom Eskilstuna kommun och IT är en av förvaltningens avdelningar. |

| | |
|-------------------|--|
| Kontinuitetsplan: | Dokument och process som beskriver hur verksamheten kan bedrivas vidare när störningar påverkar kritisk verksamhet under en tidsperiod. Tillgängligheten till informationssystem vid exempelvis ett datorhaveri kan innebära såväl omedelbar brist till information som svår återställning av systemmiljö. |
| Kund: | Allmänheten/kommuninvånare som nyttjar IT-utrustning, nätverk med mera från Eskilstuna kommun till exempel vid nyttjande av publik dator i stadshuset, på bibliotek med mera. |
| MSB: | Myndigheten för samhällsskydd och beredskap. |
| Medarbetare: | Anställda inom Eskilstuna kommun. |
| SLA: | Service Level Agreement. Det är en överenskommelse, det vill säga vad som ska levereras och till vilken servicegrad, mellan en IT-leverantör och en kund. |
| Säkerhetsprofil: | Kommunens alla IT-system har ett skyddsbehov av informationen som avgör till vilken grad som skyddsåtgärder ska sättas in. Klassificering av informationssystemet är styrande för säkerhetslösningen. |

3. Allmänt om informationssäkerhet

Information är en av våra viktigaste tillgångar och hanteringen av den är en viktig del i arbetet med riskhanteringsarbete. Informationssäkerheten är en integrerad del av Eskilstuna kommuns verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till informationssäkerhet samt att informationssäkerhetsplanen med tillhörande instruktioner efterlevs.

Informationssäkerhetsplanen är formulerad med hänsyn till:

- Rekommendationen ”Basnivå för informationssäkerhet (BITS)” från Myndigheten för samhällsskydd och beredskap (MSB).
- ISO/IEC 27000-serien.
- Lagar, förordningar och föreskrifter som gäller för kommunens verksamheter.
- Avtal.
- Tekniska förutsättningar.
- Den etiska plattform som har utvecklats över tiden genom olika politiska beslut samt förhållningssätt i den kommunala verksamheten.
- Tidigare erfarenheter från arbete med informationssäkerhet.

MSB:s rekommendationer och mallar har anpassats till de förhållanden som gäller för Eskilstuna kommun.

Med *informationstillgångar* avses:

- All information, oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Informationssäkerheten omfattar Eskilstuna kommuns informationstillgångar utan undantag.

Med *informationssäkerhet* avses:

- Att rätt information är tillgänglig för rätt person när den behövs.
- Att endast behöriga personer får ta del av konfidentiell information.
- Att offentlighetsprincipen kan upprätthållas.
- Att informationen är och förblir riktig och relevant.
- Att system som hanterar information fungerar väl och i enlighet med sitt syfte.
- Att användningen av informationssystem och Internet kan spåras.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar. Alla verksamheter inom Eskilstuna kommun är bundna av denna informationssäkerhetsplan. Detta innebär att det inte finns utrymme att besluta om lokala regler som är svagare än planen, men det är däremot tillåtet att med lokala regler förstärka planen avseende skydd av informationstillgångarna.

Den som använder Eskilstuna kommuns informationstillgångar på ett sätt som strider mot denna plan kan bli föremål för sanktioner.

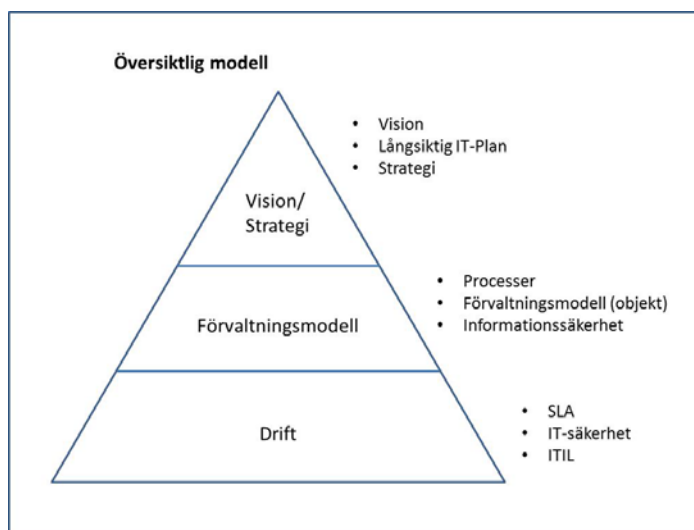
4. Avgränsning - samband och gränssnitt med andra processer

Verksamhetens behov och krav på information innebär oftast att flera system behövs för att genomföra det dagliga uppdraget.

Varje enskilt system:

- Ingår även i den förvaltningsplan över samtliga informationsobjekt som ska stödja den årliga verksamhetsplanen
- Ingår i de ramverk för service och support som hanterar bland annat incidenter (ITIL) som KoU-IT hanterar i den dagliga driftverksamheten, vilket också beskrivs i respektive SLA.

En modell för Eskilstuna kommuns informationshantering kan översiktligt beskrivas enligt bilden nedan



Det föreligger således en skillnad mellan:

- Informationssäkerhetsinstruktion förvaltning (del av systemförvaltningsplan) - som berör själva informationen/data, hur kritisk informationen i systemet är ur aspekterna sekretess, riktighet, tillgänglighet och spårbarhet för att kunna bedriva verksamheten
- Förvaltningsmodellen – som inbegriper samtliga system som verksamheten (förvaltningsorganisationen) behöver för uppgiften. Resultatet, förvaltningsplanen beskriver en årlig plan för vilka åtgärder som planeras av förbättringar eller inköp av funktioner, nya utgåvor, effektiviseringar, nya processer med mera.

5. Mål och strategier

I detta kapitel anges såväl övergripande som årliga mål för informationssäkerhetsarbetet inom Eskilstuna kommun. Vidare anges strategier för att uppnå dessa mål.

Övergripande mål

För Eskilstuna kommuns kontinuerliga informationssäkerhetsarbete gäller att:

- Informationens *tillgänglighet* ska säkerställas.
- Informationens *konfidentialitet* ska säkerställas.
- Informationens *riktighet* ska bibehållas och säkerställas.
- Informationens *spårbarhet* ska säkerställas.
- Ökat funktionalitet och ekonomi ska säkerhetsarbetet alltid beaktas.

Målet är att minimera riskerna för störningar i förvaltningarnas verksamheter, på grund av fel i eller felaktig användning av ett eller flera informationssystem samt att offentlighet, sekretess och medborgarnas rätt till integritet är säkerställd. Vår omvärld, lagkrav, ny teknologi och verksamheternas behov medför kontinuerlig följsamhet att skydda kommunens information vilket ställer krav på såväl förändringar i befintliga rutiner som etablera nya processer. Denna revision hanteras inom ramen för den organisationsstruktur som beskrivs under kapitel 6 nedan.

Strategier för att nå målen

- Att kommunens informationstillgångar klassificeras.
- Att informationen ses som en tillgång och skyddas i paritet med dess värde.
- Lagar, förordningar och föreskrifter följs.
- All personal får kunskap om gällande informationssäkerhetsregler.
- All personal ska vara förvissad om att informationsförsörjningen är säker och effektiv samt bidrar till ökat skydd och stöd för medarbetare, samverkande parter och tredje man.
- Ingångna avtal ska vara kända och följas av de som berörs av avtalen.
- Alla investeringar i form av informationshantering och teknisk utrustning ska skyddas i tillräcklig grad, exempelvis genom brandskydd, skalskydd, IT-säkerhetssystem, serviceavtal och garantier. Rutiner ska finnas för hur investeringarna ska ske.
- Det ska finnas en gemensam, säker och väl definierad infrastruktur för extern och intern data-kommunikation.
- Hotbilden för varje enskilt informationssystem som är av vikt för kommunens verksamhet ska analyseras fortlöpande genom klassificering samt risk- och sårbarhetsanalyser.
- Händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs. Incidenter av betydelse för informationssäkerheten ska loggas.
- Dokumentation ska finnas för alla IT-system.
- Att krishanteringsförmågan upprätthålls.
- Följsamhet till att på sikt bygga en struktur liknande LIS-system (Ledningssystem för informationssäkerhet) för Eskilstuna kommun där kontinuerliga förbättringar av informationssäkerheten sker genom tillämpning av PUFF. Adekvata processer och rutiner införs vid planering av årliga målen.

Årliga mål

Årliga mål för informationssäkerhetsarbetet ska formuleras. Ansvarig är kommunstyrelsen genom dess förvaltningsorganisation. För de årliga målen anges:

- Vad som ska göras under året och hur detta ska genomföras.
- Tidsplanen för åtgärderna.
- Behov av personella och ekonomiska resurser.
- När och hur uppföljning samt avrapportering ska ske.
- När och hur kommunens medarbetare ska informeras och utbildas.

Vid upprättande av de årliga målen ska avstämning/samordning ske med personuppgiftsombuden och stadsarkivet utifrån deras tillsynsroller.

För verksamhetsåret 2013 etableras bl.a. rutiner för:

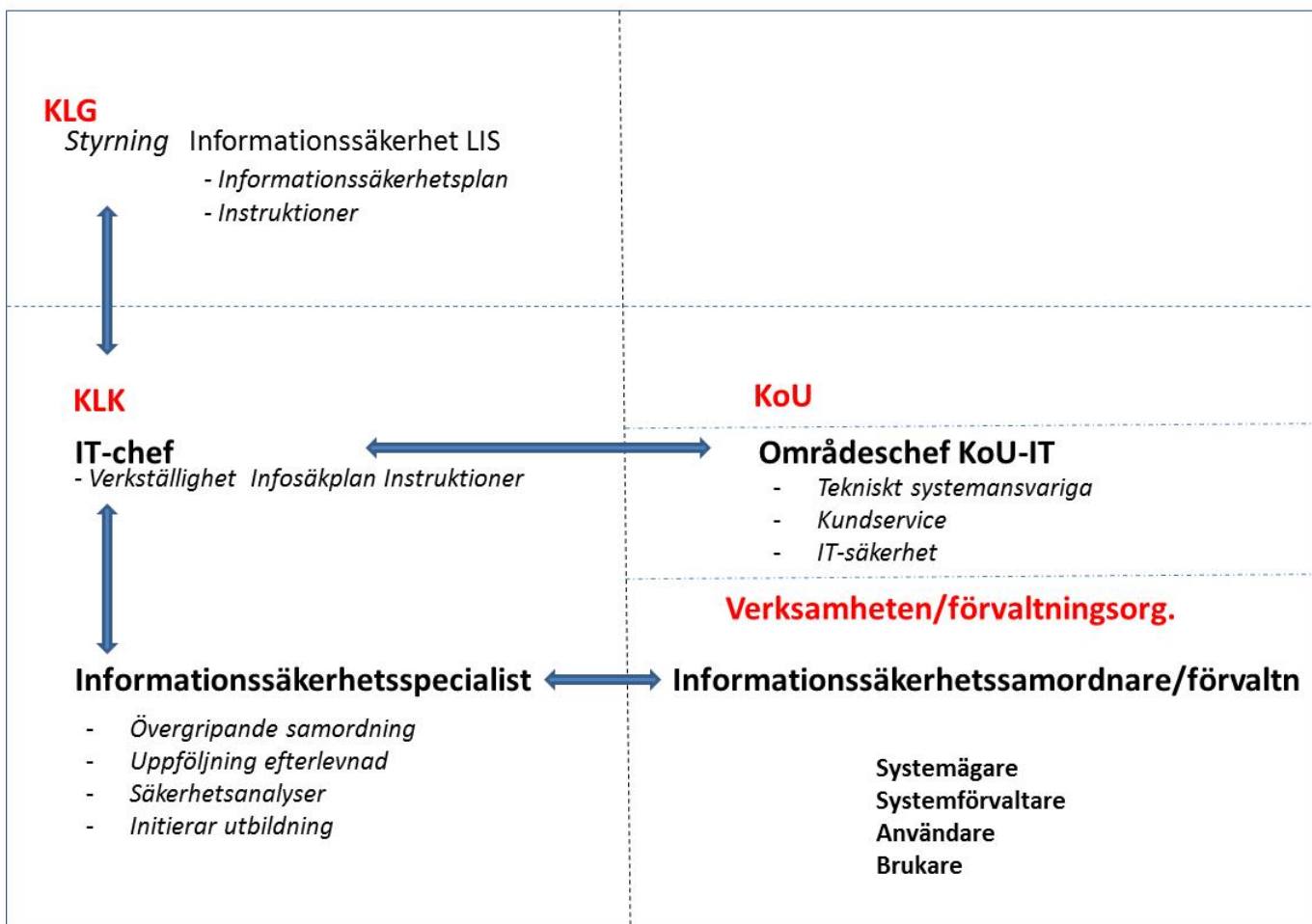
- Regler för hantering av loggar
- Lathund för lösenord
- Ansvarsförbindelse Informationssäkerhet
- Begäran om tillgång till användares e-post och hemkatalog

Rutinerna, alternativt processerna, är ingående delar i de instruktioner som gäller för Användare, Förvaltning och/eller Drift/Kontinuitet. Dokumentationen är tillgänglig på internportalen. Ändringar eller nytillkomna processer/rutiner delges förvaltningarnas Informationssäkerhets-samordnare för spridning av informationen.

6. Organisationsstruktur informationssäkerhet

Rollerna i strukturerna beskrivs i efterföljande kapitel.

Organisationsstruktur - informationssäkerhet



7. Roller och ansvar

Detta kapitel beskriver de centrala rollerna i informationssäkerhetsarbetet inom Eskilstuna kommun. Tänk på att en befattning kan ha flera olika roller.

Kommunfullmäktige

Kommunfullmäktige beslutar om informationssäkerhetsplanen och har det övergripande ansvaret för informationssäkerheten inom Eskilstuna kommun.

Kommunstyrelsen

Kommunstyrelsen bereder ärendet inför kommunfullmäktiges ställningstagande och verkställer sedan kommunfullmäktiges beslut. Kommunstyrelsen beslutar om informationssäkerhetsinstruktionerna. Kommunstyrelsen har också det övergripande ansvaret (personuppgiftsansvar) för de informationssystem och den information som ryms inom dess ansvars- och verksamhetsområde.

Kommunstyrelsen har utifrån kommunallagens regler ett tillsynsansvar över kommunens verksamheter.

Nämnder

Varje nämnd har ansvaret (personuppgiftsansvar) för de informationssystem och den information som finns inom det egna ansvars- och verksamhetsområdet. Nämnden har ett ansvar att se till att dess beslut verkställs.

IT-chef

Kommunens IT-chef ansvarar för informationssäkerhetsplanen med tillhörande instruktioner och för att driften av Eskilstuna kommuns informationssystem sköts enligt framtagna plan och instruktioner.

Områdeschef KoU IT

Områdeschef KoU IT ansvarar för att IT-säkerheten är anpassad till den riskexponering som kommunens dataverksamhet är utsatt för och berör själva driftverksamheten. Vidare så föreligger ansvar att effektivisera det SLA ur aspekten informationssäkerhet som verksamheten beskrivit i sin systemsäkerhetsanalys. Funktionen IT-kundtjänst är den instans dit incidenter anmäls för vidare åtgärd. Tekniskt ansvariga inom KoU IT har djupare förståelse för hur verksamhetssystemet fungerar ur driftperspektivet (ej logiskt, användarrelaterat).

Förvaltningschef

Förvaltningschefen har det verkställande ansvaret för förvaltningens informationssystem. Avdelningschefer eller motsvarande inom kommunstyrelsens förvaltningsorganisation är likvärdiga med förvaltningschefer i detta hänseende.

Informationssäkerhetsspecialist

Informationssäkerhetsspecialisten ansvarar för övergripande samordning av informationssäkerhetsarbetet och övervakar att informationssäkerhetsplanen och tillhörande instruktioner följs. Detta inkluderar att se till att det finns administrativa och tekniska åtgärder för informationssäkerhet samt att utföra säkerhetsanalyser. Informationssäkerhetsspecialisten initierar utbildningar och andra aktiviteter som stärker informationssäkerheten. Informationssäkerhetsspecialisten arbetar gentemot förvaltningarna med frågor om informationssäkerhet. Rollen finns inom kommunstyrelsens förvaltningsorganisation (ledningsfunktion).

Informationssäkerhetssamordnare - förvaltning

Respektive förvaltning utser en funktion för samordning av informationssäkerhetsfrågorna inom sin verksamhet såsom sprida och följa upp anvisningar/riktlinjer, hålla samman förvaltningens dokumentationssystem inom området, informera om säkerhetsfrågor, koordinera nödvändiga utbildningsinsatser.

Beredskapssamordnare

Beredskapssamordnaren har hand om kommunens kris- och säkerhetsarbete samt beredskapen kring information, egendom vid katastrofer, kriser, översvämningar med mera.

Personuppgiftsombud

Personuppgiftsombudet ska, enligt personuppgiftslagen (1998:204), se till att personuppgifter behandlas på ett lagligt och korrekt sätt och i enlighet med god sed. Det innebär att ombudet måste förvissa sig om att den personuppgiftsansvarige följer bestämmelserna i personuppgiftslagen och i anknytande lagstiftning.

Varje nämnd och kommunalt bolag ska ha ett eget personuppgiftsombud.

Offentlighetsansvarig

Samordnar samtliga frågor inom respektive förvaltning som rör offentlighetsprincipen det vill säga bevakning av hantering utifrån tryckfrihetsförordningen, offentlighets- och sekretesslagen, arkivlagen (handlingsoffentligheten), kommunallagen och förvaltningslagen, speciallagstiftning (som i delar berör offentlighetsprincipen för respektive myndighet) samt personuppgiftslagen.

Kundserviceansvarig - IT-kundtjänst

Kundserviceansvarig (IT-kundtjänsten) är Eskilstuna kommuns tekniska support för dator – och IT-relaterade frågor. IT-kundtjänst svarar på frågor om datorer, nätverk, användarkonton, programvaror med mera. Det är även till IT-kundtjänst misstänkta incidenter eller virusangrepp anmäls. Dessutom är det dit användarna ska vända sig med IT-relaterade frågor.

Drifts- och kontinuitetsansvar IT

Konsult och uppdrag IT (KoU-IT) har den tekniska kompetensen och ansvaret att leverera tillgänglighet till informationen i enlighet med SLA-överenskommelse. Ett SLA kan även innehålla större åtaganden i form av ändrings- och rättningshantering, utökad övervakning av datormiljö, funktionstester etc. Vid extern leverans (outsourcat, ”molntjänst”) styr SLA-avtalet åtagandet kundleverantör. En driftsansvarig ansvarar för den tekniska driften av ett informationssystem, medan systemägaren och systemförvaltaren ansvarar för användningen av systemet. För ytterligare förtydligande av instruktion Drift och kontinuitet – se internportalen.

Kontinuitetsansvaret innebär ett åtagande att säkra organisationens förmåga att upprätthålla och återstarta erforderlig teknik och tjänster inom överenskommen tid och med bibehållen kvalitet.

Systemägare/Informationsägare

Alla informationssystem har i sin förvaltningsplan en beskrivning av vem som är systemägare med det yttersta ansvaret för systemet. Systemägaren är den person som har det övergripande ansvaret för ett specifikt informationssystem.

I förvaltningsplanen reglerar systemägaren kommande verksamhetsårs insatser med syfte att säkerställa informationssystemets uppgift och tillgänglighet i vardagen.

Systemägarskapet gäller för ett specifikt informationssystem och dess användning inom hela Eskilstuna kommun. Systemägarskapet ska inte förväxlas med personuppgiftsansvaret som åligger respektive nämnd. Systemägaren har det övergripande ansvaret för användningen, utvecklingen och avtalshantering för ett specifikt informationssystem och dess informationssäkerhet. Systemägaren ansvar också för att en systemsäkerhetsanalys görs för verksamhetskritiska system.

Systemägaren är också informationsägare, det vill säga ansvarar för de informationstillgångar som finns i informationssystemet. Det här ansvaret kan dock åligga annan person än systemägaren, vilket i så fall hanteras i förvaltningsplanen för respektive system.

Frågor om applikation/system och behörighetshantering ansvarar respektive systemägare för. För ytterligare förtydligande av instruktion Förvaltning av informationssystem.

Systemförvaltare/Informationsförvaltare

Systemförvaltaren är underställd systemägaren och ansvarar för den operativa användningen av det specifika informationssystemet.

Leverantör

Leverantör är den som levererar IT-system till Eskilstuna kommun och i förekommande fall sköter driften av dessa. Se drifts- och kontinuitetsansvar ovan,

Användare

Användare är varje person som använder ett informationssystem och/eller IT-stöd tillhandahållet av Eskilstuna kommun. Medarbetare, förtroendevalda, elever, brukare, kunder och extern personal kan vara användare. Extern personal kan bland annat vara användare hos en privat entreprenör som levererar upphandlad tjänst enligt lagen om offentlig upphandling eller användare hos en privat utförare som utför tjänst enligt lagen om valfrihetssystem.

Behörighet till kommunens informationstillgångar ges av respektive systemägare. Användarnas ansvar och skyldigheter beskrivs i användarinstruktionerna.

8. Generella krav

I detta kapitel redovisas de generella krav som gäller för användning av Eskilstuna kommuns informationssystem och IT-stöd.

Eskilstuna kommuns informationssystem

Samtliga informationssystem ska vara identifierade och förtecknade i samband med upprättande av förvaltningsplanen samt enligt personuppgiftslagen. Av förteckningen ska bland annat framgå vem som är systemägare, systemförvaltare samt driftsansvarig (intern eller extern funktion).

Det ska också framgå vilka informationssystem som betraktas som verksamhetskritiska. Alla informationssystem ska minst uppfylla den basnivå för informationssäkerhet som rekommenderas i BITS/ISO 27 000 och i kommunens informationssäkerhetsplan med tillhörande instruktioner.

Verksamhetskritiska system

Med verksamhetskritiska system avses informationssystem vars korrekta funktion är en förutsättning för att undvika förlust av liv, skada på hälsa och miljö, säkra informationsflöden,

garantera organisationens överlevnad eller undvika stora ekonomiska förluster. Det är också informationssystem vars informationstillgångar behandlar sekretessbelagda och/eller känsliga personuppgifter samt känslig ekonomisk information.

Informationsklassificering

Vissa informationssystem är en grundförutsättning för att kunna bedriva den kommunala verksamheten på ett effektivt sätt. Alla system som inom 48 timmar påverkar organisationen/verksamheten/säkerheten menligt är att betrakta om verksamhetskritiska.

För dessa informationssystem samt de system som innehåller känsliga personuppgifter enligt personuppgiftslagen (1998:204), sekretessbelagda uppgifter enligt offentlighets- och sekretesslagen (2009:400) eller person- eller samordningsnummer nummer ska följande dokumenteras:

- Klassificering av informationstillgångarna, enligt Eskilstuna kommuns klassificeringsmodell, utifrån sekretess, riktighet, tillgänglighet och i förekommande fall spårbarhet.
- Systemsäkerhetsanalys utifrån den modell som kommunen använder.
- Informationssäkerhetsinstruktion förvaltning (som en del av systemförvaltningsplan) ska upprättas.
- SLA ska upprättas.
- Prioritering av systemet vid ett stillastående.

Analyserna ovan utgör underlag för driftgodkännande.

Arbetsmetod

All information som är av vikt för kommunens verksamhet ska klassificeras.

En systemsäkerhetsanalys ska genomföras av alla verksamhetskritiska system. I det fall det behövs ska fördjupande användar-, drift/kontinuitet- och förvaltningsinstruktion tas fram för respektive system. Till dokumentationen ska också finnas förteckning enligt personuppgiftslagen. Alla som använder kommunens IT-resurser ska genomgå den utbildning som behövs för att informationssäkerheten ska upprätthållas. Utbildningen ska även följas upp och kompletteras vid behov.

Distansarbete

För att medarbetare ska kunna arbeta effektivt kan möjlighet finnas till distansarbete (arbete utanför ordinarie arbetsplats med åtkomst till IT-system). Förutsättningar och restriktioner för detta ska bestämmas och dokumenteras. Riktlinjer för distansarbete utifrån informationssäkerhetsaspekt avgörs i systemsäkerhetsanalysen där systemägaren är ytterst ansvarig.

Användning av Internet

När en användare nyttjar Internet sker det med Eskilstuna kommun som avsändare.

Vid användning av Internet ska därför Eskilstuna kommuns värdegrund gälla. Dessa regler finns beskrivna i *Informationssäkerhetsinstruktion för användare, medarbetare och förtroendevalda – en sammanfattning*. Det finns också tydliga restriktioner som definierar vilken typ av webbplatser som *inte* får besökas.

Undantag från förbudet kan beviljas om informationen på sådana sidor kan ha relevans för arbetsuppgifterna, detta förankras med närmaste chef.

Till begreppet webbplats räknas allt material på Internet som har en IP-adress, det vill säga hemsidor, communities, sociala medier, forum, webbutiker, servrar med mera.

För mer information se *Informationssäkerhetsinstruktion för användare, medarbetare och förtroendevalda – en sammanfattning*.

E-post

Av all e-post till och från e-postadresser i Eskilstuna kommuns organisation är merparten allmänna handlingar och ska behandlas som sådana. Varje användare som hanterar sådan e-post ansvarar för att den diarieförs enligt gällande regler och lagar. Sekretessbelagd eller integritetskänslig information får inte skickas via e-post med mindre än att epost-meddelandet är krypterat på godkänt sätt. Kommunala e-postadresser är avsedda för tjänstebruk så undvik att använda den kommunala e-postadressen i privat syfte. Behöver du tillfälligtvis skicka och/eller läsa privat e-post ska detta i första hand göras från ditt privata e-postkonto.

För mer information se *Informationssäkerhetsinstruktion för användare – medarbetare och förtroendevalda*.

Tjänsteanvändning och privat användning

Datorutrustning och system inom Eskilstuna kommun är inköpta och avsedda för kommunens verksamhet. Det är inte tillåtet att använda datorn i privat syfte (t ex sidoverksamheter) på arbetstid. Det är dessutom inte lämpligt att använda en kommunal dator för privat bruk då kommunen inte ansvarar för privat material.

Sociala medier (sidor med användargenererat innehåll) har fått en allt större genomslagskraft på Internet inom många områden. Sociala medier är tillåtet att använda i professionellt syfte, exempelvis som en kanal för kommunens information och marknadsföring. För sociala medier finns riktlinjer antagna av kommunfullmäktige den 28 april 2011, § 65.

För mer information se *Informationssäkerhetsinstruktion för användare – medarbetare och förtroendevalda*.

Kontinuitetsplanering

En kontinuitetsplan beskriver hur verksamheten ska bedrivas i händelse av kris eller katastrof och är av central betydelse för att man ska kunna bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära situationer. Kontinuitetsplanen för driften av IT-verksamheten är baserad på respektive informationssystemets krav. Dessa krav beskrivs i systemets förvaltningsplan.

9. Sanktioner

Överträdelser mot informationssäkerhetsplanen och tillhörande instruktioner kan leda till sanktioner. Sanktioner mot medarbetare och elever ska hanteras på samma sätt som vid andra problem eller överträdelser på arbetsplatsen/skolan.

10. Uppföljning och översyn

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att

- Beslutade åtgärder är genomförda.
- Årliga mål är uppfyllda.
- Regler följs.

Informationssäkerhetsplanen med tillhörande instruktioner ska årligen ses över. Informationssäkerhetsspecialisten ansvarar för revisionen och kontakterna med förvaltningssamordnarna.

Kommunfullmäktige har det övergripande ansvaret för informationssäkerhetsarbetet. Betydande ändringar informationssäkerhetsplanen ska beslutas av kommunfullmäktige. Beslut om vissa mindre ändringar i planen och instruktionerna som inte strider mot grundidén, kan fattas av kommunstyrelsen.

Införande av förändringar, anpassningar, nya instruktioner och motsvarande genomarbetas med Informationssäkerhetsspecialist som sammankallande av samordnare och bereder ärendet för beslut i PLG-IT. Styrande direktiv i kvalitetsutvecklingen av informationssäkerhetsplanen sker via huvudman/beställare på KLG för att inarbetas i PUFF-snurran.

11. Publicering

Denna informationssäkerhetsplan med tillhörande instruktioner ska alltid finnas publicerade i sin senaste version på Eskilstuna kommuns internportal och på kommunens webbplats eskilstuna.se. Ansvar för detta har kommunstyrelsens förvaltningsorganisation. Varje nämnd genom dess förvaltning har ansvaret att informera sina användare på lämpligt sätt. Det gäller även för verksamheter med brukare, elever och externa användare.

Det är tillåtet att ta fram populärversioner riktade till olika målgrupper, under förutsättning att det tydligt framgår att de bygger på den fullständiga informationssäkerhetsplanen med tillhörande instruktioner. Det ska också framgå var man kan hitta de fullständiga dokumenten.

Varje chef är skyldig att informera sina medarbetare om var denna informationssäkerhetsplan och aktuell informationssäkerhetsinstruktion kan läsas.

I lokaler (till exempel bibliotek) där allmänheten nyttjar Eskilstuna kommuns system ska denna informationssäkerhetsplan finnas tillgänglig.

Ingen användare ska kunna säga att man inte kände till innehållet i denna informationssäkerhetsplan eller aktuell informationssäkerhetsinstruktion.