Åmåls kommun

IT- och informationssäkerhetspolicy

Antagen av kommunfullmäktige 2020-12-15 § 211

Dnr KS 2020/399

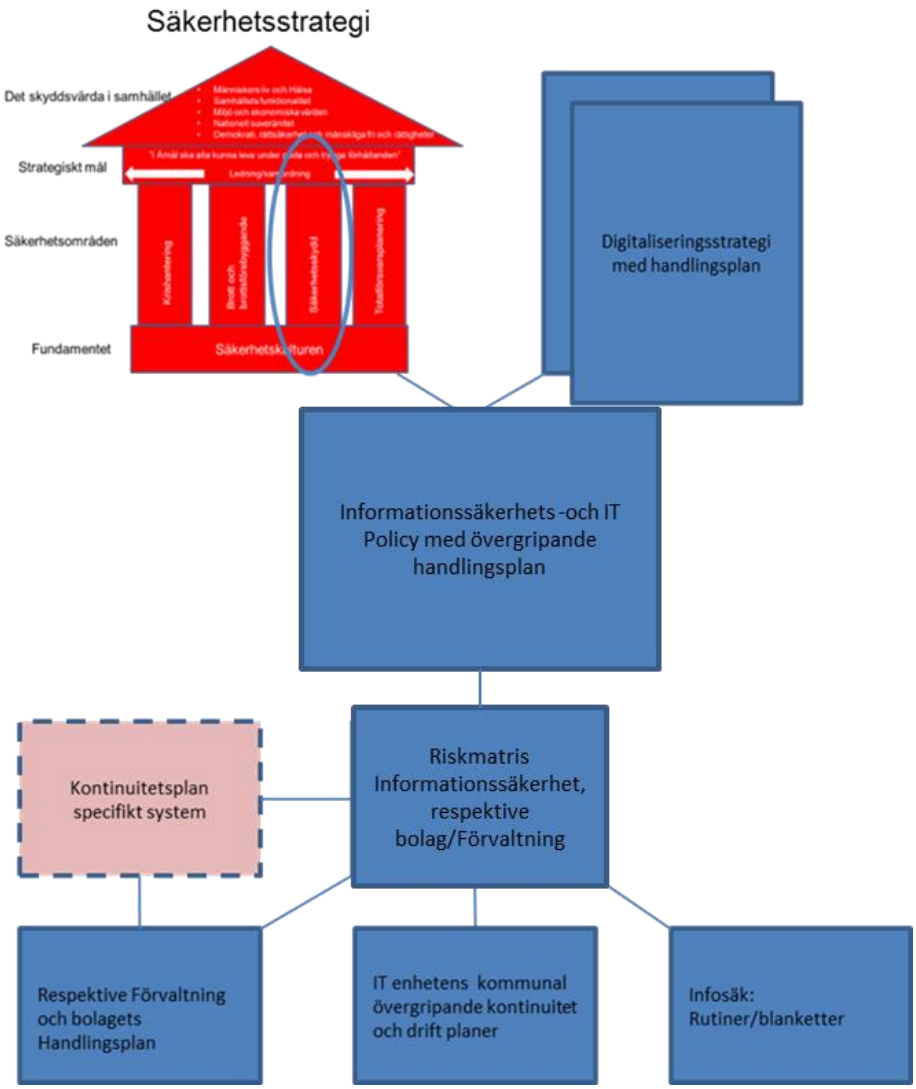
Innehåll

1. Allmän information

IT- och informationssäkerhetspolicy med handlingsplan beskriver grundläggande principer för IT-användning och informationssäkerhet i Åmåls kommun. Policyn är en del av Åmåls kommuns säkerhetsstrategi[1] och IT-verksamhet och ska stödja all verksamhet i kommunen.

IT- och informationssäkerhetspolicyn bildar grunden för kommunens ledningssystem för informationssäkerhet (LIS) och är en förutsättning för förvaltningarnas, bolagens och IT-enhetens fortsatta arbete med informationssäkerhetsanalyser, kontinuitetsplaner och rutiner.

Bilden nedan visualiserar kopplingen till styrdokumenten och uppbyggnaden av kommunens principer för informationssäkerhetsarbete.



[1] *Åmåls kommuns säkerhetsstrategi 2020-2023*, antagen av kommunfullmäktige 2020-03-31, § 44.

2. Informationssäkerhet och IT

Information är en central byggsten. Utan tillgång till relevant, tillförlitlig och korrekt information kan medarbetarna få svårigheter att utföra arbetet, vilket i förlängningen kan försvåra för bolag, förvaltningar och enheter att bedriva sin verksamhet med god kvalitet.

Information ger kunskap till individer och organisationer och kan både inhämtas, lagras, kommuniceras och bearbetas i olika former. I och med den ökande digitaliseringen ökar informationsmängden och därmed verksamheternas beroende av fungerande informationssystem. Det medför att en verksamhetsutövare behöver identifiera och skydda den information som är värdefull (skyddsvärd information).

Det kan få stora negativa konsekvenser för kommunen om information röjs till obehörig, obehörigen förändras eller inte finns till hands när den behövs.

Informationssäkerhet handlar om åtgärder för att skydda information. En effektiv och säker informationshantering kräver att informationssäkerhetsarbete bedrivs systematiskt och i enlighet med gällande säkerhetsstrategi.

Denna IT- och informationssäkerhetspolicy ska gälla alla medarbetare och förtroendevalda inom Åmåls kommun. Därutöver kan lokala rutiner/regler finnas som kompletterar. Dessa återfinns i förekommande fall i förvaltningarnas eller bolagens egna handlingsplaner.

Den som använder Åmåls kommuns informationstillgångar på ett sätt som strider mot denna eller andra gällande policys i kommunen ska utredas och kan bli föremål för disciplinära åtgärder.

Definition av informationssäkerhet och dess omfattning

IT- och informationssäkerhetspolicyn omfattar alla verksamheter, förvaltningar och bolag i Åmåls kommun. Informationssäkerhet gäller för all informationshantering i kommunen.

Med information avses all information oavsett dess form, exempelvis fysisk lagring på papper, elektroniskt lagrad information av digitala dokument, inspelningar av tal och/eller rörlig bild. All information som skapas eller används i Åmåls kommun ska värderas och vid behov skyddas enligt gällande bestämmelser och lagar. Med informationssäkerhet avses att:

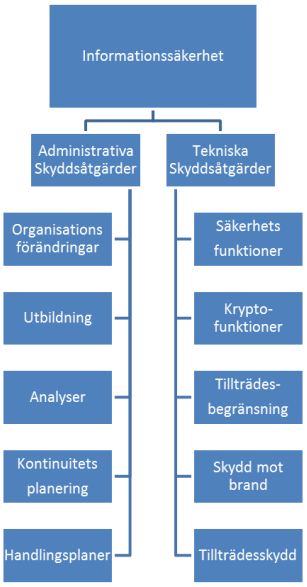
- rätt information är tillgänglig för rätt person när den behövs och i vissa fall är loggningsbar,
- informationen är och förblir riktig, samt
- att informationen skyddas från otillbörlig åtkomst och spridning.

Skyddet av vår information

Informationssäkerhet handlar om att skydda information mot skadlig inverkan. Det kan exempelvis vara skydd av informationssystem som styr viktiga samhällsfunktioner eller system som hanterar sammanställningar av uppgifter där uppgifternas tillgänglighet eller riktighet är av betydelse för Åmåls kommun, andra myndigheter, personskydd etcetera.

Informationssäkerhet är också skyddet mot att säkerhetsskyddsklassificerade uppgifter av betydelse för Sveriges säkerhet röjs, ändras, görs otillgängliga eller förstörs av obehöriga.

Exempel på skyddsåtgärder inom informationssäkerhet
Bilden nedan visar schematiskt hur administrativa och tekniska skyddsåtgärder kan genomföras för att förbättra informationssäkerheten. Exakt vilka av dessa åtgärder som respektive förvaltning eller bolag är i behov av ska framgå av verksamheternas egna informationssäkerhetsanalyser och handlingsplaner.



Övergripande mål för informationssäkerhet i Åmåls kommun
Det övergripande målet för Åmåls kommuns informationssäkerhet är att säkerställa tillräckligt skydd för myndighetens informationstillgångar, så att rätt information finns tillgänglig för rätt person i rätt tid. Det innebär i Åmåls kommun att:

- Alla medarbetare ska ha kunskap om var man hittar gällande IT- och informationssäkerhetspolicy.
- På central nivå ska säkerställas att processen enligt den övergripande säkerhetsstrategin följs.
- Alla investeringar både i form av information och i teknisk utrustning ska ha skydd i tillräcklig grad.
- Hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet ska analyseras fortlöpande i en informationssäkerhetsanalys.
- Händelser i informationssystem som kan leda till negativa konsekvenser ska förebyggas och rapporteras i enlighet med gällande rutiner.
- All information ska finnas tillgänglig när den behövs samt vara och förbli riktig.
- Information ska endast vara tillgänglig för dem som är behöriga att ta del av och använda den, samt att hanteringen av sådan informationen ska vara spårbar.

Övergripande mål för IT i Åmåls kommun
Det övergripande målet för IT i kommunen är att möjliggöra effektivisering samt ge kvalitetshöjande effekter. IT ska ses ur ett helhetsperspektiv för kommunen med en gemensam inriktning på IT-användandet för att uppnå bästa möjliga verksamhet åt kommuninvånarna. Detta innebär att:

- Användandet av IT ska medverka till att ge medborgarna en god och effektiv samhällsservice.
- Användandet av IT ska ge beslutsfattare på alla nivåer ett bra beslutsunderlag med data av god kvalitet.
- Användandet av IT ska tillgodose de anställdas behov av en god arbetsmiljö samt främja personalutvecklingen och ge motivation och effektivitet i arbetet.
- Användandet av IT ska vara ett hjälpmedel för bra verksamhetsstyrning och bidra till effektivt resursutnyttjande och kostnadseffektivitet samt skapa enklare och effektivare rutiner.
- Lagstadgade krav för offentlighet och sekretess samt behandling av personuppgifter ska uppfyllas.

3. Roller och ansvarsområden
Det finns ett behov av att ha tydliga roller och ansvar i en kommun då olika myndigheters informationssystem beskriver och namnger de olika rollerna och ansvaren olika. Att förstå roller och ansvar blir också en viktig del av informationssäkerhet då det måste vara tydligt vem som är ansvarig för att åtgärda säkerhetsproblem. Nedanstående roller och ansvar ska gälla i Åmåls kommun.

Kommunstyrelsen
Åmåls kommun är en politiskt styrd organisation där det yttersta ansvaret vilar på de politiska organen med dess förtroendevalda. För IT och informationssäkerhet är det kommunstyrelsen som är ansvarig nämnd. I praktiken bedrivs dock mycket av den praktiska hanteringen och utvecklingsarbetet på området, av sakkunniga tjänstepersoner inom kommunstyrelsens förvaltning.

Nämnder och bolagsstyrelser
Nämnder och bolagsstyrelser är tillika systemansvariga (se punkten sidan 7). Nämnd/bolags-styrelse ansvarar för respektive förvaltnings/bolags egna handlingsplaner och för att en sådan antas varje mandatperiod.

Nämnd/bolagsstyrelse ska implementera denna policy och följa upp sin handlingsplan minst en gång under mandatperioden.

E-rådet är ett centralt forum för IT-frågor i Åmåls kommun.

Det är skapat av kommundirektören för att ge förutsättningar för en kvalitativ, framsynt och inkluderande IT-verksamhet i Åmåls kommun. Då IT i dag genomsyrar all verksamhet i det moderna samhället, såväl i privat som i offentlig sektor, är det avgörande att verksamhetens behov, kompetens och perspektiv tas till vara. Genom E-rådet säkerställs att Åmåls kommuns förvaltningar ges möjlighet att påverka de förslag till strategiska vägval och inriktningsbeslut som förvaltningen därefter lägger fram till politiken.

Det är kommundirektören som utser ordförande i E-rådet. Brukligt är att IT-chefen är ordförande men även annan funktion kan ges denna uppgift.

I E-rådet ska, förutom ordföranden, ingå representanter från samtliga kommunala förvaltningar och bolag. Dessa representanter ska utses av respektive förvaltningschef/VD och kan vid behov förstärkas av ytterligare verksamhetsföreträdare om så krävs för att hantera frågor som anvisas E-rådet. Förvaltningarna ansvarar för att representanten i E-rådet har kunskap och mandat att ge inspel som leder E-rådets arbete framåt på ett konstruktivt sätt. I E-rådet ingår även säkerhetsstrategen i sin roll som säkerhetskyddschef och övergripande samordningsansvarig för kommunens säkerhetsskydd.

E-rådets ordförande ansvarar för att rådet kallas samman vid behov, dock minst fyra gånger per år och för att en dagordning upprättas. E-rådets möten ska dokumenteras genom minnesanteckningar som diarieförs. E-rådet ska hantera alla typer av frågor som berör aspekter av IT inom kommunens verksamhetsområden. E-rådet är konsultativt och rådgivande. Beslutsmandaten i IT-frågor ligger orubbat kvar i befintlig organisation för politik och förvaltning.

Säkerhetsskyddschefen är tillika säkerhetsstrateg och leder hela säkerhetsprocessen, samt ansvarar för att säkerhetsskyddet i sin helhet upprätthålls. Säkerhetsskyddschefen ingår i E-rådet. Det är säkerhetsskyddschefen som har i uppdrag att bevaka frågor av övergripande informationssäkerhetskaraktär i Åmåls kommun och säkerställa att denna IT- och informationssäkerhetspolicy uppdateras och görs tillgänglig.

Biträdande signalskyddschef ingår i Länsstyrelsens signalskyddsorganisation, ansvarar för Åmåls kommuns signalskyddsorganisation och är informationsägare av kommunens kryptosystem Signe. Biträdande signalskyddschef upprättar signalskyddsinstruktion för hantering av säkerhetsklassad information.

Systemägare är ägaren av systemet där informationen hanteras, ofta ett privat mjukvaruföretag. Ofta är systemägaren också leverantör och utvecklare av själva systemet, men dessa roller kan vara uppdelade. Det är systemägaren som ansvarar för systemet samt dess syfte och ändamål.

Systemägaren ansvarar för att det finns adekvat skydd för den information som hanteras, lagras eller bearbetas och ska utifrån riskanalysen och informationens krav på skydd tillse att så finns. Systemägaren är oftast juridiskt ansvarig för systemet i teknisk bemärkelse. Systemägaren ska garantera att systemet som kommunen använder uppfyller de krav på säkerhet som kommunen har ställt i samband med upphandling eller tjänsteköp.

Systemansvarig är den nämnd, styrelse eller myndighet som ansvarar för den verksamhet där systemet används som ett medel att fullfölja uppdraget. Det är den systemansvarige som bär det yttersta juridiska ansvaret för användningen av systemet.

I praktiken har den systemansvarige utsett en **ansvarig chef** i sin förvaltning. Det är denne som har ansvar för att det system som används är det bäst lämpade, utifrån förutsättningarna. Ansvarig chef ansvarar för att systemet är förvärvat på ett korrekt sätt, att gällande avtal finns på plats, att beställningar, uppdateringar och underhåll sker på ett adekvat sätt. Ansvarig chef har också ett ansvar för den ekonomiska hållbarheten och utvecklingen. Ansvarig chef ska tillse att rollen **systemförvaltare** tillsätts och har rätt förutsättningar för att klara sitt uppdrag. Ansvarig chef ska vid behov informera såväl relevanta delar av den kommunala förvaltningsorganisationen som systemansvarig om förändringar eller incidenter som berör systemet och den information som behandlas.

Systemförvaltaren utses av ansvarig chef och ska vara dennes förlängda arm och den lokala experten på systemet inom den kommunala verksamheten, avseende funktionalitet och handhavande. Systemförvaltaren ska vara verksamhetens expert på respektive system och vara den som inom kommunen har störst förtrogenhet med systemet. Systemförvaltaren ska ha full tillgång med samtliga behörigheter i systemet och ha möjlighet att styra behörigheter och användarkonton för andra användare inom kommunen.

Innan systemförvaltaren tillträder sin roll ska denne genomgå utbildning i aktuellt system. Systemförvaltaren ska i sin tur kunna ge introduktion och utbildning på basnivå till andra användare inom verksamheten.

Systemförvaltaren har dock inget ansvar för själva driften av systemet, det åligger leverantören och i vissa fall Åmåls kommuns IT-enhet (i de fall kommunen själv är utvecklare eller driftsansvarig av systemet på egna lokala maskiner/nätverk/servrar). Det är dock viktigt att systemförvaltaren har en direkt kontaktväg till systemägaren för att kunna rapportera exempelvis buggar och andra problem och snabbt kunna få support och handledning.

Det är även systemförvaltaren som ska vara behjälplig vid migrering, buggtestning vid versionsuppgradering etcetera. Systemförvaltaren har en viktig roll i relation till systemansvarig och den chef som utsetts att vara beställare/avtalsansvarig, med att påtala behov av utveckling, avveckling eller anpassning.

Användaren är den som är inne i systemet och arbetar som en del av sin uppgift som medarbetare i Åmåls kommun. Det kan finnas olika nivåer av användare eftersom olika befattningar kan ha varierade rättighet att skriva in information eller ändra i befintlig information. Användare kan vara olika typer av handläggare, nämndsekreterare, administratörer, vårdanställda, lärare med flera som dokumenterar i sitt arbete.

Den som tillför eller ändrar information i systemet är ansvarig för att informationen är riktig och korrekt. Det är respektive chefs ansvar att säkerställa att alla medarbetare som ges tillgång till ett system som användare också har fått adekvat och tillräcklig utbildning i systemet och den information som systemet ska hantera. Användarens ansvar är att hålla sig till den anvisade användningen och de eventuella riktlinjer eller rutiner som arbetsgivaren har tagit fram.

Brukaren är den som har tillgång till hela eller delar av informationen i ett system men utan direkt rätt eller möjlighet att påverka innehållet eller lägga till nytt innehåll. Brukare kan exempelvis vara medarbetare i kommunen som använder systemet som referens eller kunskapskälla eller invånare som själva har insyn i sina uppgifter, exempelvis sina journaler.

Även allmänheten kan således vara brukare av kommunala IT-system med tillhörande information, exempelvis genom e-arkiv eller förtroendemannaregister med möjlighet att självständigt söka fram och hämta information. I den mån brukaren självständigt kan lägga till information i systemet rör det sig om noteringar eller organisation av den egna informationen i syfte att underlätta sitt informationsinhämtande. Ett exempel kan vara att ”favorit-markera” delar av information för snabb åtkomst. Brukaren kan i vissa fall också kommunicera med kommunen via kommunikationstjänster eller meddelandetjänster som ingår i systemet.

Brukaren är ansvarig för att den information som denne har fått tillgång till hanteras med rätt konfidentialitet och inte sprids på ett otillbörligt sätt. Om brukaren är en anställd i Åmåls kommun – eller agerar på uppdrag av Åmåls kommun – är det respektive chefs ansvar att säkerställa att brukaren fått kunskap om informationens konfidentialitet och på vilket sätt informationen får spridas.

Bolag och förvaltningar
Bolag och förvaltningar ska regelbundet genomföra informationssäkerhetsanalys, minst en gång per mandatperiod. Informationssäkerhetsanalysen ska rapporteras till nämnd eller styrelse.

IT-enheten
IT-enheten ska upprätta och förvalta det övergripande dokumentet *Handlingsplan IT - kontinuitet och drift* och övergripande rutiner och riktlinjer relaterade till detta dokument.

Personalenheten
Personalenheten ska upprätta riktlinjer för hantering av individ med skyddad identitet. Vid behov ska enheten även upprätta en kontinuitetsplan för enskilt system, exempelvis löne-systemet.

Informationssäkerhetsutbildning
Den som har chefsbefattning ska ansvara för att medarbetarna regelbundet får den utbildning som är behövlig för att informationssäkerheten ska upprätthållas.

Distansarbete
Distansarbete är tillåtet efter överenskommelse mellan chef och medarbetare. Vid användning av internet/nätverk eller teknisk utrustning som tillhör Åmåls kommun ska medarbetare även vid distansarbete följa kommunens olika policys och riktlinjer.

Användning av informationskällor i strid med policys
Om behov finns av att besöka informationskällor som bryter mot gällande policys och regler, eller möjligen kan uppfattas vara av olämplig karaktär men behövs för arbetet, ska berörd chef informeras innan informationskällan används. Chefen kan göra undantag om information från sådana källor bedöms vara relevant för arbetsuppgiften. Chefen ska då göra tjänsteanteckning om detta undantag.

Elektronisk post
Säkerhetsklassad eller sekretessbelagd information eller annan av medarbetare bedömd känslig information får inte skickas via e-post. För den typen av information ska funktionen ”säkra meddelanden” användas, alternativt kontakt tas med biträdande signalskyddschef eller säkerhetsskyddschef som kan skicka via kryptosystemet.

Elektronisk post kan vara föremål för diarieföring, som är en viktig del i att informationen ska vara tillgänglig när den behövs. Det är därför chefens ansvar att medarbetarna har tillräcklig kompetens om vad som är sekretessbelagd och/eller känslig information och hur sådan ska kommuniceras, diarieföras eller raderas. Även information som inte innehåller känsliga uppgifter kan vara föremål för diarieföring.

Informationsklassning av kommunens, förvaltningarnas och bolagens informations-system

Alla informationssystem som hanteras i Åmåls kommuns förvaltningar och bolag ska dokumenteras i informationssäkerhetsanalysen och klassificeras enligt nedanstående tabell för informationsklassning.

Säkerhetsaspekt Konsekvensnivå	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**
Allvarlig	Information där förlust av konfidentialitet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Betydande	Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Måttlig	Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Ingen eller försumbar*	Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där det inte föreligger krav på riktighet, eller där förlust av riktighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. **	Information där det inte föreligger krav på tillgänglighet, eller där förlust av tillgänglighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild. **

**Då information som bedöms höra till ingen eller försumbar nivå inte medför någon eller endast försumbar negativ påverkan, ska dessa system inte analyseras vidare i riskmatrisens del 2. Av samma anledning blir information som hör till denna nivå inte föremål för några särskilda skyddsåtgärder. Nivån finns med i riskmatrisen för att den ska vara komplett och omfatta alla olika informationssystem i syfte att kunna spåra roller och ansvar.*

Information i begränsat hemlig och högre

Säkerhetsklassad information i säkerhetskyddsklass begränsad hemlig eller högre, ska endast handhas av kommunens signalskyddsorganisation. Påträffas en sådan handling ska den skyndsamt lämnas eller rapporteras till säkerhetskyddschefen eller biträdande signalskyddschef för bedömning och åtgärd.

Säkerhetsklassad personal

Vilka befattningar som innebär placering i säkerhetsklass bestäms på central nivå. Om förvaltningar, bolag eller enheter anser sig ha det behovet ska kontakt tas med säkerhetskyddschefen eller HR-avdelningen. Säkerhetsklassning sker i normalfallet vid nyanställning.

Säkerhetsskyddad upphandling (SUA)

Innan molntjänster eller andra tjänster av informationshantering läggs ut på tredje part ska en analys göras om säkerhetsskyddad upphandling krävs. Denna fråga ska förvaltning eller bolag ta upp i E-rådet för vidare bedömning.

Ekonomi, inköp, planering
Upphandling av system ska göras i samråd med kommunens IT-enhet. IT-investeringar ska därför ske genom en samordnad planering med IT-enheten. Inköp av datorutrustning såsom datorer, skrivare, skanners, digitalkameror, licenser etc. ska ske via IT-enheten. Kostnaderna för kommunens gemensamma resurser inom IT-området ska bäras av de verksamheter som använder resurserna.

Underhåll av system
För att upprätthålla en god säkerhets- och funktionsnivå av IT-miljön ska kontinuerliga uppdateringar och uppgraderingar ske. Dessa ska ske enligt rutiner för underhåll av system. Alla systemuppgraderingar som påverkar verksamheters dagliga drift ska planeras i samråd mellan IT-enheten, systemägaren och systemförvaltaren. Den verksamhet som använder systemet, eller är beroende av informationen i systemet, ska i god tid informeras så att verksamheten kan planeras utan risk för skada eller incidenter.

Standardiserad systemplattform och enhetsflora
Kommunen ska eftersträva en så standardiserad och homogen miljö som möjligt. Genom att begränsa antalet olika enhetsmodeller, operativsystem och andra system kan kommunen minska kostsam förvaltning och förenkla sin kravställning.

Hantering av klient med skyddad identitet
Kunskap om sådan identitet ska begränsas till så få individer som möjligt. Vid frågor eller behov ska HR-avdelningen kontaktas.

Revidering och uppföljning
E-rådet ska ansvara för uppföljning av denna policy och ska bevaka att beslutade åtgärder är genomförda samt påminna förvaltningar och bolag om revideringar enligt Åmåls säkerhetsstrategi. Inom E-rådet har säkerhetssamordnaren ett särskilt ansvar för revidering och uppföljning.

Bilagor

Bilaga 1: Övergripande kommunal handlingsplan IT- och informationssäkerhetspolicy

Bilaga 2: Mall övergripande kommunal informationssäkerhetsanalys

Åmåls kommun

Bilagor till

IT- och informationssäkerhetspolicy

Dnr KS 2020/399

Bilaga 1 till IT- och informationssäkerhetspolicy

Övergripande kommunal handlingsplan

Nedanstående styrning ska ses som en minsta gemensam nämnare. Handlingsplanerna hindrar inte att förvaltningar och bolag kan komplettera med lokala bestämmelser (som ej strider mot styrdokumenten). Det finns en skyldighet att agera om det ökar informationssäkerheten eller medvetandegör risker i våra informationssystem.

Styrning handlingsplan förvaltningar och bolag:

- Förvaltningar och bolag ska genomföra en riskmatris för informationssäkerhet i enlighet med den kommunövergripande mallen (se bilaga).
- Riskmatrisen ska innehålla en förteckning av samtliga informationssystem och ange vem som är systemägare, systemansvarig, systemförvaltare, användare och brukare (del 1).
- Av förteckningen ska också framgå detaljer kring systemets driftsform.
- Förvaltningar och bolag ska ta fram en egen handlingsplan för informationssäkerhet kopplat till den egna riskmatrisen. Planen ska ha tidsperspektivet av en mandatperiod.
- Riskmatris, handlingsplan över samtliga informationssystem ska godkännas av respektive nämnd/styrelse.
- Följande ärenden ska minst ingå och vara definierade i handlingsplanerna: Digitaliseringsbehov, behov av administrativa åtgärder, behov av tekniska skyddsåtgärder samt övergripande tidsplan.

Handlingsplan IT - kontinuitet och drift ska minst innehålla:

- Villkor för aktivering av kontinuitetsplan
- Inledande aktiviteter
- Åtgärder avbrottsplan
- Aktivering av reservdrift
- Återgång till normaldrift
- Informationsspridning och informationskanaler
- Kontaktpersoner

Följande IT-rutiner och riktlinjer ska tas fram:

- Rutiner vid anställning och avslut av anställning
- IT-användaravtal och åtkomsthantering
- Incidentrapportering avseende IT
- Beställning till IT-enheten
- Riktlinjer vid anskaffning av IT-system och IT-utrustning
- Rutiner vid underhåll av system
- Riktlinjer för dataskydd, lösenord och kryptering
- Rutiner för licenshantering

Bilaga 2 till IT- och informationssäkerhetspolicy

Mall övergripande kommunal informationssäkerhetsanalys

Denna mall finns digitalt kontakta säkerhetsstrategen