Ängelholms kommun

[Publiceringsdatum]

Riktlinje om informationssäkerhet och personuppgiftsbehandling

för Ängelholms kommun 2021-2025

Dokumentnamn	**Dokumenttyp**	**Fastställd/upprättad**	**Beslutsinstans**
Riktlinje om informations-säkerhet och personuppgifts-behandling	Riktlinje	2021-06-02	Kommunstyrelsen
Dokumentansvarig	**Diarienummer**	**Senast reviderad**	**Giltig till**
Säkerhetsenheten	KS 2021/261	Klicka eller tryck här för att ange datum.	2026-12-31

Dokumentinformation
Riktlinjerna beskriver hur policy för informationssäkerhet och personuppgiftshantering ska genomföras.
Dokumentet gäller för
Ängelholms kommun, Ängelholm Stadshus AB, AB Ängelholmshem och AB Ängelholmslokaler.

Ängelholm kommuns struktur för styrdokument framgår av Riktlinjer för styrdokument 2020-2024 (beslutad av Kommunstyrelsen den 12 augusti 2020, dnr 2015/864).

V*ision, framtidsförklaring och kommunfullmäktiges mål* - *Visionen ska peka ut en riktning och ett framtida önskvärt tillstånd.*

Plan - *Ett översiktligt och aktiverande dokument.*

Handlingsplan - *Ett detaljerat och aktiverande dokument.*

Policy - *Ett översiktligt och normerande dokument.*

Riktlinje - Ett detaljerat och normerande dokument. Riktlinjen ska ge konkret stöd för hur uppgifter ska utföras. Den koncentrerar sig på **hur** en åtgärd görs, inte på vad den innehåller. Riktlinjen kan lägga ett ”golv” för vilken nivå som verksamheten ska uppnå och ofta också ett ”tak” för vilken service som ska erbjudas. Denna typ av riktlinje påminner om kvalitetsdeklarationer. Riktlinjen kan också vara inriktad på metod och tillvägagångssätt. Riktlinjen måste vara tydlig. Typiska ord och uttryck i sådana dokument är ”ska”, ”måste” och ”får inte”. Kommundirektör driver och ansvarar för samordning i arbetet med framtagandet av en kommunövergripande riktlinje. Chef för huvuduppdrag och servicestödschef,

alternativt dess delegat, ansvarar på motsvarande sätt för en riktad riktlinje. Riktlinjen beslutas av kommunstyrelsen.

Innehållsförteckning

1. Sammanfattning av dokumentets sakliga innehåll

Riktlinjerna om informationssäkerhet och personuppgiftshantering utgör grunden för hur de övergripande målen i policyn om informationssäkerhet och personuppgiftshantering ska uppnås samt beskriver hur Ängelholms kommun och dess helägda bolag ska strukturera arbetet.

Kommunstyrelsen har det övergripande ansvaret för informationssäkerhet inom Ängelholms kommun. Ansvaret för det dagliga informationssäkerhetsarbetet ska däremot följa det ordinarie verksamhetsansvaret.

Riktlinjerna om informationssäkerhet och personuppgiftshantering utgör grunden för hur de övergripande målen i policyn om informationssäkerhet och personuppgiftshantering ska uppnås och det systematiska arbetet med informationssäkerhet ska genomföras.

Policyn och riktlinjerna om informationssäkerhet och personuppgiftsbehandling ska tillämpas i alla situationer där Ängelholms kommun, Ängelholm Stadshus AB, AB Ängelholmshem och AB Ängelholmslokaler, fortsättningsvis benämnt Ängelholms kommun eller kommunen, hanterar information med eller utan personuppgifter.

2. Inledning

2.1. Dokumentets innehåll och disposition

Inledningsvis finns allmänna utgångspunkter och information om informationssäkerhet och dataskydd som berör alla medarbetare i Ängelholms kommun.

Dokumentet innehåller sedan detaljerade riktlinjer för följande grupper

- samtliga medarbetare - kapitel 5
- de medarbetare som arbetar med upphandling och inköp - kap 6
- de medarbetare och chefer som ansvarar för rekrytering och anställningsförhållandet - kap 7
- samtliga medarbetares skyldighet att rapportera misstänkta och inträffade incidenter - kap 8

Härefter följer information riktad till verksamhetsledning om arbete med systematiskt informationssäkerhetsarbete i enlighet med Myndigheten för

samhällskydd (MSB) metodstöd samt information om införande av ledningssystem för informationssäkerhet.

Slutligen specificeras organisation, särskilda roller av relevans för informationssäkerhet och dataskydd och ansvar, samt ansvar för uppföljning och rapportering.

2.2. Varför informationssäkerhet?

Ängelholms kommun ska skydda och bevara information som kommunen har att ta ansvar för så att lagstadgade, etiska, verksamhetsrelaterade och avtalade krav upprätthålls. En god informationssäkerhet och personuppgiftshantering bidrar till att skapa förtroende för kommunen och dess bolag hos kommuninvånare och avtalsparter

Att hitta rätt nivå på säkerhetsåtgärder innebär inte bara att kommunen ger informationen ett adekvat säkerhetsskydd, det säkerställer också att kommunen är kostnadseffektiv. Ett alltför omfattande skydd kan vara alltför kostsamt och ett för lågt skydd kan innebära dels en förlust av förtroende från kommuninvånare, samarbetspartners eller andra intressenter samt dels ekonomiska kostnader i form av sanktionsavgifter, viten och skadeståndsansvar. I arbetet med informationshantering som rör personuppgifter ska den enskildes rätt till integritet och lagstadgade rättigheter särskilt beaktas. Dataskyddsförordningen ställer höga krav på informationssäkerhet - såväl fysisk säkerhet som administrativ säkerhet och IT-säkerhet.

2.3 Avgränsning i förhållande till andra riktlinjer

Övriga riktlinjer, instruktioner, rutiner eller dylikt (här benämnt ”riktlinjer”), av relevans för informationssäkerhetsarbetet och som kompletterar dessa Riktlinjerför informationssäkerhet och dataskydd, är nödvändiga. Bland annat gäller det följande riktlinjer;

- För närmare instruktioner kring kravställning för utformning av fysisk miljö i form av lås, larm och brandskydd hänvisas till separata riktlinjer på detta område.
- För arbete med IT-säkerhet och i systemförvaltarorganisationen finns separata riktlinjer framtagna av Digitaliseringsenheten.
- För arbete med upphandling finns separata riktlinjer framtagna av Upphandlingsenheten.
- För riktlinje avseende kommunikation och användning av sociala medier hänvisas till Kommunikationsenheten.
- Kommunarkivets verksamhet styrs av Arkivreglementet.

Vid den händelse att riktlinjernas innehåll strider mot varandra ska denna riktlinje äga företräde under förutsättning att den ger information och den registrerade det högsta skyddet.

3. Vad är informationssäkerhet?

3.1 Allmänt om informationssäkerhet

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Detta innefattar information i alla dess former så som text, ljud, bilder, film, och oavsett hur information lagras, bearbetas och kommuniceras. Informationssäkerhet inkluderar alltså förutom information i IT-system även pappersbaserad information och information som finns i våra huvuden.

Informationssäkerhet utgörs av tre aspekter; att informationstillgångar ska vara konfidentiella, riktiga och tillgängliga. Olika typer av händelser (incidenter), som kan vara avsiktliga eller oavsiktliga så som stöld, radering eller obehörig tillgång kan försämra konfidentialiteten, riktigheten eller tillgängligheten hos informationstillgångar. Beroende på vilken information det rör sig om kan de olika aspekterna vara olika viktiga. Information på hemsidan är inte konfidentiell men har däremot höga krav på riktighet och framför allt tillgänglighet. Kraven som uppställs kan komma från verksamhetens eget behov, externa förväntningar från medborgare och leverantörer samt från rättsliga krav.

Vad som är lämplig nivå av skydd för en viss informationsmängd beror på dessa krav, på vilken hotbild som finns, och i vilka situationer informationen hanteras det vill säga hur den lagras, bearbetas, kommuniceras osv.

För viss typ av information gäller särskilt höga krav på säkerhetsåtgärder. Denna information benämns Konfidentiell information och utgörs bland annat av känsliga personuppgifter och information som omfattas av krav på sekretess.

3.2 Lagstiftning som ställer krav på informationssäkerhet

Offentlighetsprincipen, allmänna handlingar och sekretess

Som en del av offentlighetsprincipen har allmänheten rätt att ta del av allmänna handlingar i offentlig verksamhet. Huvudregeln är att den information som finns hos myndigheter ska vara offentlig. Dokument som inkommer till kommunen och kommunala bolag eller upprättas där ska diarieföras eller hållas ordnade på annat sätt så att det går att söka fram information som allmänheten vill ta del av. Det är naturligtvis mycket viktigt att allmänna handlingar och den information som finns där är såväl riktig som tillgänglig. Annars kan myndigheten inte uppfylla de krav som uppställs i grundlag. Naturligtvis ska också konfidentialiteten beaktas.

Allmänna handlingar kan vara både i form av analog och digital information och ska hanteras, bevaras och gallras i enlighet med den dokumenthanteringsplan som beslutats för verksamheten av nämnd eller bolagsstyrelse.

Information som är allmän handling kan vara sekretessbelagd. Bestämmelser om sekretess finns framför allt i offentlighets- och sekretesslagen[1]. Syftet kan vara att skydda en enskild, en verksamhet eller Sveriges säkerhet. Sekretessen kan vara av olika slag, från ett svagare skydd till absolut sekretess. Information som omfattas av sekretess får inte lämnas ut utan att det prövas noggrant.

Säkerhetsskydd och samhällsviktiga tjänster

Ytterligare lagstiftning som påverkar arbetet med informationssäkerhet och personuppgiftshantering är Säkerhetsskyddslagen[2], med mycket höga säkerhetskrav på behandlingen av information som rör Sveriges säkerhet samt Lag om informationssäkerhet för samhällsviktiga och digitala tjänster[3] där det bland annat anges att verksamheter som tillhandahåller samhällsviktiga tjänster ska implementera ett ledningssystem för informationssäkerhet som ett led i att säkerställa att informationen skyddas för att förhindra avbrott i verksamhetens kontinuitet.

Bevarande av information

Av arkivlagstiftningen framgår hur offentliga verksamheter ska bevara sin information. För att möjliggöra ett korrekt bevarande krävs att hänsyn tas till arkivreglerna redan i samband med exempelvis upphandling av ett nytt IT-system. Systemen ska stödja bland annat att informationen kan exporteras på korrekt vis och att dokument sparas i rätt format.

Av Ängelholms kommuns Arkivreglemente framgår att Riksarkivets föreskrifter inom följande områden ska tillämpas när det gäller tekniska krav på:

- arkivlokaler
- krav gällande papper, mikrofilm, ritfilm, skrivmedel, kopiatorer, faxar, skrivare, digitala lagringsformat
- bindning av handlingar

---

[1] Offentlighet- och sekretesslagen (2009:400)
[2] Säkerhetsskyddslagen (2018:585) var det bland annat anges i 2 kap 2 § att *Informationssäkerhet ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.*
[3] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster vari det bland annat anges i 11 § att *Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.*

- elektroniska handlingar, i tillämpliga delar och efter arkivmyndighetens anvisningar

3.3 Digitaliseringen fram och baksidor

Digitaliseringen skapar helt nya möjligheter att utföra tjänster och dela information. Den har medfört att de flesta idag förväntar sig att myndigheter, företag och andra organisationer ska erbjuda digitala tjänster på Internet. Digitaliseringen handlar nu om så mycket mer än kommunens IT-drift. De ökade möjligheterna ställer emellertid också krav på ändrade arbetssätt. Hotbilden förändras också när informationen går från att vara inlåst i närarkiv eller tillgängliga på lokala servrar till att vara åtkomlig när som helst var som helst.

Informationsflödet mellan organisationer, individer och länder med olika rättssystem medför risk för att ansvaret för informationen blir oklar vilket i sin tur medför ökade sårbarheter. Tydlig ansvarsfördelning, ett aktivt informationssäkerhetsarbete och god informationssäkerhet är en förutsättning för att kunna dra nytta av de fördelar som digitaliseringen medför i form av effektivisering, ökad service och tillgänglighet. Motsatsen medför stora risker för såväl kommunens egen interna verksamhet och Sveriges säkerhet som för de medborgare kommunen har i uppdrag att värna och leverera till.

4. Särskilt om behandling av personuppgifter

4.1 Allmänt om dataskydd

Skyddet för personuppgifter är en del av rätten till integritet som en mänsklig rättighet. För personuppgifter finns det ett särskilt skydd. Detta gäller oavsett om det är personuppgifter som omfattas av sekretess eller inte. Att behandla personuppgifter förutsätter därför särskild försiktighet.

Med behandling av personuppgifter avses varje åtgärd eller serie av åtgärder som görs med personuppgifter. Det kan t. ex. vara insamling av personuppgifter, registrering, läsning, överföring eller lagring. Med personuppgifter avses all information som på ett eller annat sätt kan kopplas till en levande individ.

Dataskyddsförordningen[4] (GDPR) och kompletterande svensk lagstiftning i bland annat Dataskyddslagen[5], lag om behandling av personuppgifter inom

[4] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) ofta förkortad GDPR

[5] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

socialtjänsten[6] samt Patientdatalagen[7] ställer särskilda krav på behandling av personuppgifter, med målet att värna och skydda den personliga integriteten. Förordningen, som utgår från ett antal principer, ställer höga krav på säkerheten för de uppgifter som behandlas. En god informationssäkerhet är en förutsättning för att uppfylla de krav som dataskyddsförordningen ställer upp.

4.2 Principer för dataskydd

Dataskyddsförordningen bygger på ett antal principer som ska vara styrande i all personuppgiftshantering. Principerna innebär bland annat att nämnder och bolagsstyrelser, i egenskap av personuppgiftsansvariga:

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter.
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål.
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen.
- ska se till att personuppgifterna är riktiga.
- ska radera personuppgifterna när de inte längre behövs, vilket i offentlig verksamhet innebär att dataskyddsförordningen ska beaktas vid fastställande av gallringsfrister.
- ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs.
- ska kunna visa att och hur personuppgiftsansvarig lever upp till dataskyddsförordningens krav.

Ett systematiskt informationssäkerhetsarbete bidrar till säker hantering även av personuppgifterna. Lagstiftningens ställer emellertid också krav på verksamheten genom att varje behandling av information som omfattar personuppgifter också ska uppfylla ytterligare rättsliga krav.

4.3 Känsliga personuppgifter

Känsliga personuppgifter är alltid klassade som konfidentiell information. Till känsliga personuppgifter räknas uppgifter som avslöjar

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- personuppgifter som rör hälsa eller sexualliv, eller
- genetiska och biometriska uppgifter

[6] Lag (2001:454) om behandling av personuppgifter inom socialtjänsten
[7] Patientdatalagen (2008:355)

4.4 Dataskydd och offentlighetsprincipen

Dataskyddsförordningen innehåller ett uttryckligt undantag för sådan behandling av personuppgifter som följer av offentlighetsprincipen. Det innebär att dataskyddsförordningen aldrig hindrar att personuppgifter lämnas ut i samband med en begäran om allmän handling. Däremot gäller naturligtvis reglerna om sekretess som vanligt, varför en sekretessprövning ska göras. Dataskyddsförordningen kan också medföra att det är inte är tillåtet att lämna ut allmänna handlingar som innehåller personuppgifter via oskyddad e-post.

5. Informationssäkerhet och dataskydd för dig som medarbetare

5.1 Medarbetarens viktiga roll för informationssäkerheten

Information är en viktig resurs för kommunen. Alla som arbetar i kommunen hanterar dagligen information såväl digitalt som på papper, i samtal med kollegor och medborgare, vid genomförandet av sina arbetsuppgifter. Felaktig information eller bristande tillgång till informationen när vi behöver den kan få stora konsekvenser. Privatpersoner, företag och andra har förväntningar på och behov av att du som medarbetare hanterar information på ett säkert sätt. Viss information är känslig och skyddas av regler om sekretess och dataskydd, av hänsyn till den personliga integriteten. För hantering av sådan information ställs särskilda krav.

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för att motsvara dessa krav. Information behöver olika slag av skydd. Det kan vara tekniskt såsom en brandvägg i ett IT-nätverk. Eller administrativt i form av regler (som dessa riktlinjer). Eller fysiskt hur man skyddar utrymmen med dörrar, lås, skåp m.m. Även medarbetares kunskap och medvetenhet är ett nog så viktigt skydd. Till exempel att arbeta på rätt sätt med pappersdokument och i IT-system och att vara försiktig med känslig information som t.ex. personuppgifter.

Mycket av skydd för information ska byggas in i de system som används i verksamheten att det är lätt att göra rätt i det dagliga arbetet. Du som medarbetare har en central roll att spela. Det har nämligen ingen betydelse vilken säkerhet som byggs in och vilka rutiner som tas fram om du inte följer det som anges. Säkerhet är inte bättre än den svagaste länken, och det är viktigt att alla typer av skydd fungerar på ett bra sätt tillsammans. En stor del av informationssäkerheten beror därför på hur du hanterar informationen.

Medarbetare inom Ängelholms kommun och bolag ska följa dessa riktlinjer för informationssäkerhet. Riktlinjerna gäller även, i tillämpliga delar, för förtroendevalda som har IT-utrustning från kommunen, e-postadress i kommunen,

eller som på annat sätt agerar inom kommunens analoga och digitala informationssystem. Brott mot riktlinjerna kan innebära brott mot såväl avtal som lagstiftning och Ängelholms kommun kommer då att vidta åtgärder så som att anmäla lagbrott till polisen.

5.2 Loggning

Loggning sker i kommunens datorer och nätverk. Loggarna används för felsökning och för utredning av incidenter eller för att förhindra brott. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer. Spårbarhet genom loggning är för viss information ett krav. Det innebär att man genom loggning kan identifiera vem som har gjort vad och när och följa förloppet för olika händelser på datorn. All Internettrafik och e-post loggas centralt. Kommunen har som arbetsgivare rätt att, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och riktlinjer. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

5.3 Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänkts kunna medföra negativ påverkan på kommunens information. Det kan röra sig om t.ex. IT-angrepp/intrång, skadlig kod, oskyddad känslig information, brister i efterlevnad av dessa riktlinjer för informationssäkerhet, med mera.

Incidenter och brister ska omedelbart rapporteras till Digitaliseringsenheten. Meddela även din chef. Om en misstänkt incident omfattar personuppgifter ska anmälan göras avsedd e-tjänst som återfinns på intranätet.

5.4 Säkert beteende

1. Var mycket varsam med konfidentiell information så att obehöriga inte får del av den. Det gäller både skriftlig och muntlig information. Det är endast de som måste ha del av informationen för sitt arbete som har rätt att ta del av den. Tala bara om konfidentiell information i stängda utrymmen och försäkra er om att det inte går att höra utifrån. Konfidentiell information får överhuvudtaget inte kommuniceras muntligt i publika lokaler.
2. Skriftligt material som innehåller konfidentiell information får inte ligga framme så att obehöriga kan läsa den. Materialet ska låsas in i godkända skåp när man lämnar arbetsplatsen, även för kortare stunder.
3. Konfidentiell information på datorskärmen ska vara skyddad från obehöriga. Datorn ska låsas när du lämnar den, även för en kortare stund. Om du har ett så kallat smart kort till datorn ska detta tas ut då du lämnar arbetsplatsen.

4. Besökare ska bära besöksbricka och får inte vistas på egen hand i lokalerna. Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler. Obekanta personer i sådana lokaler ska tillfrågas vem de söker och hjälpas tillrätta.
5. Vid utskrift ska Säker utskrift/Follow me print användas. Det vill säga att utskrift sker först efter att användaren identifierat sig vid skrivaren.
6. Vid fysisk posttjänst ska förslutna brev användas för intern information och rekommenderade försändelser ska användas om brev innehåller konfidentiell information.
7. Pappersdokument som innehåller konfidentiell information måste vid kassering strimlas eller kastas i godkända säkerhetskärl.

5.5 Hantering av lösenord

8. Lösenorden är personliga och får inte göras kända för andra.
9. Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person, och dessutom ha en viss längd och komplexitet.
10. Lösenord ska vara minst 8 tecken långt, gärna längre och innehålla minst en gemen, en versal och en siffra. Tips på bra lösenord som är enkla att minnas är att tänka ut en mening. Justera sedan stora och små bokstäver och bilda lösenordet. Exempel:
    Jag vill aldrig vara 20 igen! Jvav20i!
    Min kusin Adam fyller 40 och firar stort MkAf40ofs
11. Olika lösenord ska användas. Samma lösenord ska inte användas privat och i jobbet. Ha olika lösenord för olika tjänster även i arbetet.
12. Lösenord ska bytas regelbundet, minst tre gånger om året om inget annat framgår. Lösenord ska bytas direkt om misstanke finns att det har röjts.
13. Lösenord får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. Man kan i så fall bli ansvarig för något som någon annan har gjort. I de fall en dator delas av flera ska ändå personliga inloggningar göras. Detta är viktigt för spårbarheten, för att kunna veta vem som har gjort vad i systemen.
14. Använd inte automatisk minnesfunktion för lösenordet. Låt inte webbläsare spara lösenordet. Detta är särskilt viktigt då en dator delas av flera.

5.6 Hantering av IT-utrustning och mobila enheter

Närmare riktlinjer vad gäller IT-utrustning, så som datorer, mobiltelefoner, surfplattor, USB-minnen m.m., anges i riktlinjer för IT-säkerhet. Följande

grundläggande regler gäller dock för samtliga medarbetare. Mobil enhet avser bärbara enheter.

15. IT-utrustning är arbetsredskap och får inte lånas ut eller överlåtas om det inte är enheter som delas av flera.
16. Enheternas säkerhetsinställningar får inte ändras.
17. Endast godkända programvaror får installeras på enheten. Vilka programvaror som är godkända beslutas av Digitaliseringsenheten.
18. Installerad programvara får inte kopieras eller installeras på annan enhet.
19. Mobila enheter ska låsas med lösenord.
20. Konfidentiell information måste vara krypterad på mobila enheter.
21. Endast av kommunen godkänd enhet och programvara får anslutas till kommunens nät.
22. Privat utrustning kan anslutas till kommunens gästnät.
23. Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade.
24. Anslutning med kommunens VPN-anslutning från en privat dator är ej tillåtet.
25. Arbete med konfidentiell information får inte ske i publika miljöer.
26. Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme, i övrigt vårdas och hanteras på det sätt som föreskrivs, t.ex. skyddas mot värme och fukt
27. Förlust av enhet ska omedelbart anmälas till Digitaliseringsenheten. I vissa fall finns möjligheter att fjärradera information.
28. Vid avslut av anställning eller vid byte till en annan enhet ska mobila enheter återlämnas i enlighet med de rutiner som finns, och får inte behållas privat eller av en verksamhet.

5.7 Motverka skadlig kod

Med skadlig kod avses exempelvis trojaner som avlyssnar lösenord eller öppnar ”bakdörrar” så att andra kan komma åt informationen utan att det syns, olika typer av spionprogram och så kallat ransomeware där filer eller diskar krypteras varvid verksamheten sedan krävs på lösensumma för att åter få tillgång. Det kan vara mycket svårt att upptäcka skadlig kod och det gäller att vara vaksam. Även om kommunens utrustning skyddas så är den tekniska utvecklingen mycket snabb och det är svårt att hålla jämna steg. Följande gäller alla medarbetare:

29. Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.

30. Anslut endast godkänd IT-utrustning till kommunens nätverk. Det är exempelvis inte tillåtet att koppla in privat telefon i arbetsdatorns USB-kontakt, eller att ansluta USB-minnen som inte är skyddade och kontrollerade.
31. Var misstänksam. Undvik att klicka på konstiga länkar eller fylla i irrelevanta uppgifter.
32. Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad. Låt dig inte luras av att avsändarens namn stämmer med en kollegas eller chef. Granska så att avsändarens e-postadress stämmer med vad du förväntar dig.
33. Om IT-utrustning beter sig långsamt eller konstigt ska du kontakta Digitaliseringsenheten.

5.8 Användning av Internet och Sociala medier

För riktlinjer kring användning av sociala medier, se Ängelholms kommuns riktlinjer för sociala medier.

34. Det är inte tillåtet att använda sociala medier eller privata e-postadresser för att exempelvis genomföra avlämningar mellan medarbetare eller diskutera och lösa arbetsuppgifter. Detta gäller även i slutna grupper på exempelvis Facebook.

5.9 Användning av e-post

Varje dag inkommer och skickas stora mängder information med e-post. Försök att se din e-post som en vanlig brevlåda som ska tömmas, och sorteras. E-posten är inte ett lämpligt ställe att lagra information. Det är också lätt hänt att information som är allmän handling inte hanteras i enlighet med kraven på registrering och god offentlighetsstruktur. E-posten uppfyller inte heller kraven på bevarande. Det blir dessutom mycket svårt för dina kollegor att få del av informationen du lagrar där. Se istället till att allt hamnar på rätt ställen, det vill säga i ärendehanteringssystem, diarium, avsedda mappar, eller i soptunnan om det finns gallringsbeslut som stödjer det.

Att skicka e-post okrypterat är som att skicka vykort. Det är därför mycket viktigt att du använder e-posten på ett medvetet sätt och följer riktlinjerna för hur den får användas.

35. Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den e-post som skickas från kontot.
36. Medarbetare är ansvarig för att löpande öppna, läsa och ta omhand inkommande e-post.

37. E-post som skickas till personliga brevlådor är allmän handling om innehållet är arbetsrelaterat. Vid arbetsrelaterad e-post ska alltid regler för registrering och hantering av allmänna handlingar följas.

38. Vid frånvaro, t.ex.semester, sjukfrånvaro eller föräldraledighet, ska autosvar användas, och en behörig representant så som kollega eller chef ska regelbundet kontrollera e-postkontot och ta hand om de allmänna handlingar som kommer in dit. Skyndsamhetskravet gäller även för post med allmänna handlingar som inkommer till medarbetare som är frånvarande.

39. Vid avslut av anställning eller vid tjänstledighet ansvarar närmsta chef för att informationen på kontot tas omhand innan kontot tas bort.

40. E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga.

41. E-post som är allmän handling får gallras, dvs raderas, först när e-posten diarieförts. Vissa e-postmeddelanden som är allmänna handlingar är av uppenbar ringa eller tillfällig betydelse och är undantagna från kravet på registrering. Dessa får gallras i enlighet med kommunens gallringsbeslut för allmänna handlingar av ringa eller tillfällig betydelse.

42. Använd inte ditt e-postkonto för privata ändamål, och använd inte din privata e-post för arbetsmaterial.

43. Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postadresser.

44. Konfidentiell information får endast skickas med e-post som använder godkänd kryptering.

45. Klassningen samt distributionssätt avgör om det är lämpligt att skicka/överföra personuppgifter digitalt. Möjlighet till kryptering ska beaktas. Skicka aldrig fler personuppgifter i e-post än nödvändigt, inte ens intern. Tänk på att fullständiga personnummer är särskilt skyddsvärda enligt dataskyddslagstiftningen och ska användas mycket restriktivt.

5.10 Lagring och säkerhetskopiering

46. Den information du hanterar i ditt arbete är verksamhetens information, som behöver finnas tillgänglig även i de fall du är sjuk eller frånvarande av annan anledning. Se till att information som lagras lokalt på din dator kopieras över till nätverket så att den inte försvinner om din dator går sönder eller blir stulen.

47. Information ska i första hand lagras i för ändamålet avsedda verksamhetssystem. I annat fall lagras den på nätverket så att den säkerhetskopieras.

48. Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, kontakt Digitaliseringsenheten som förhoppningsvis kan återskapa den senaste säkerhetskopian.
49. Konfidentiell information får endast lagras i därför avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan.
50. Lokal lagring av konfidentiell information, t.ex. på en dator, får endast ske efter att Digitaliseringsenheten säkerställt att lagringsenheten eller filerna är krypterade med godkänd metod. för
51. Fysiska dokument som innehåller konfidentiell information ska förvaras inlåsta.
52. Endast godkända molntjänster är tillåtna. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.)

6. För dig som arbetar med Upphandling och inköp

6.1 Analysera informationen innan upphandlingen påbörjas

Innan ett inköp eller utveckling av ett IT-system eller en digital tjänst ska förutsättningarna för att hantera informationen i enlighet med kraven i dataskyddsförordningen och kompletterande lagstiftning analyseras. Utgångspunkten är den klassning och genomförda risk- och sårbarhetsanalys som ska ha genomförts samt en eventuell konsekvensbedömning enligt artikel 35 i dataskyddsförordningen.

6.2 vid upphandling gäller följande

53. Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Ängelholms kommuns modell för informationsklassning. Kravkatalogen ska kunna användas som stöd vid upphandling av IT-tjänster så som system och molntjänster.
54. Vid upphandling och inköp av digitala system och tjänster som avses innehålla eller omfatta personuppgifter ska alltid principerna om dataskydd som standard och inbyggt dataskydd beaktas.
55. Riksarkivets föreskrifter ska i tillämpliga delar utgöra en del av underlaget vid upphandling och inköp. När det gäller IT-system som hanterar allmänna handlingar som ska bevaras, ska förutsättningar för långsiktigt digitalt bevarande, med stöd av kommunarkivet, beaktas när systemen upphandlas eller utvecklas.

56. Behörighetskontroll ska finnas på samtliga system som behandlar personuppgifter och konfidentiell information. Rutinen för åtkomstbehörighet ska dokumenteras skriftligt. Loggning i systemet ska tillämpas.
57. Systemet ska stödja principen om lagringsminimering genom att alltid ge stöd för gallring av handlingar och i de fall det är lämpliga säkerhetsåtgärder även för pseudomymisering och anonymisering.¨
58. Systemet ska stödja och underlätta exportering av information till e-arkiv.
59. Det ska finnas en vägledning som beskriver hur en kontroll av en IT-tjänst ska genomföras. Den ska kunna användas som stöd inför användandet av en ny tjänst eller vid kontroll av en befintlig tjänst. Syftet med vägledningen ska vara att säkerställa att IT-tjänsten kan skydda verksamheten och dess information under hela dess livscykel

6.3 Personuppgiftsbiträde

Ett personuppgiftsbiträde är en aktör som utför behandling av personuppgifter för den personuppgiftsansvariges räkning. Rollen är osjälvständig och bygger på att personuppgiftsansvarig är den som styr ändamål och huvudsakliga medel, även om biträdet själv har visst utrymme att styra över tekniska lösningar. Biträdet har i uppdrag att behandla uppgifterna för ansvarigs räkning och har alltså inte rätt eller möjlighet att behandla uppgifterna för annan verksamhet. Typiska biträden är molntjänstleverantörer och andra IT-leverantörer. En aktör som behandlar personuppgifter som ett led i att bedriva en egen affärsverksamhet, exempelvis privata vårdboenden eller privata skolor, är inte biträden till myndigheten utan fristående personuppgiftsansvariga. Vägledning kring behov och innehåll av avtal ges av den centrala dataskyddssamordnaren.

Anlitas ett personuppgiftsbiträde för att utföra en del i en personuppgifts-behandling ska alltid ett personuppgiftsbiträdesavtal tecknas. Avtalet kan ligga som en bilaga till huvudavtalet eller ingå som klausuler i huvudavtalet. Innehållet i avtalet regleras av dataskyddsförordningen, artikel 28. Avtalet tecknas av den som är behörig att teckna huvudavtalet. Upphandlingsavdelningen ansvarar för att avtalet förses med biträdesavtal eller annan rättsakt.

60. Bedöm om avtalet omfattar behandling av personuppgifter.
61. Bedöm om ett personuppgiftsbiträdesavtal eller en rättsakt för gemensamt personuppgiftsbiträdesavtal ska tecknas.
62. Ansvarig upphandlare ska se till att biträdesavtalet eller rättsakten är en del av upphandlingsunderlaget och finns med som bilaga vid avtalstecknande.

7. Personalsäkerhet som en del av informationssäkerhetsarbetet

Som ett led i det systematiska informationssäkerhetsarbetet gäller att den personal som arbetar i verksamheten informeras om innebörden av informationssäkerhet och vikten av att tänka säkert. De ska också få tillräckliga förutsättningar att utbilda sig inom informationssäkerhet, behandling av allmänna handlingar och dataskydd.

Vid anställning av ny personal gäller följande:

63. Vid anställning till tjänster som faller under lagstiftningen om registerkontroll för skydd av barn och unga ska lagstiftningen tillämpas.
64. För befattningar som har betydelse för Sveriges säkerhet, och således omfattas av Säkerhetsskyddslagen (2018:585), ska anställningsförfarandet omfatta en säkerhetsprövning i enlighet med bestämmelserna i den lagen. Närmare vägledning kring efterlevnaden av säkerhetsskyddslagen lämnas i instruktion utfärdad av Säkerhetsskyddschefen.
65. Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras och referenser hämtas in.
66. Anställning av kritiska roller ska genomgå förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister.
67. Nyanställda ska få information och utbildning gällande informationssäkerhet, dataskydd samt regelverk kring hantering av allmänna handlingar. Alla medarbetare och i förekommande fall externa aktörer ska löpande få lämplig utbildning för att kunna efterleva kommunens policy och riktlinjer för informationssäkerhet och personuppgiftsbehandling och fullgöra sina arbetsuppgifter på ett säkert sätt.
68. Roller som har särskilda uppgifter inom informationssäkerhet och dataskydd ska får lämplig fortbildning inom området som är relevant för deras befattning.
69. Nyanställda ska i samband med anställningen få information om arbetsgivarens behandling av deras personuppgifter i enlighet med artikel 13 dataskyddsförordningen. Informationen ska också finnas tillgänglig på kommunens intranät.
70. Det ska finnas en formell och kommunicerad disciplinär process för att vidta åtgärder mot anställda som har brutit mot gällande informationssäkerhetsregler.
71. Anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal. Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och

kommuniceras vid anställningstillfället eller tillträdande av roll och framgå i sekretessavtal.

72. Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.

8. Incidenthantering

8.1 Incidenter som ett tecken på brister och chans till bättring

Ett uttalat syfte med ett systematiskt arbetssätt för informationssäkerhet och personuppgiftshantering är att arbeta förebyggande och riskbaserat. En incident är en störning, säkerhetsbrist eller händelse som inverkar negativt informationssäkerheten eller skyddet för personuppgifter. Incidenter ska hanteras skyndsamt för att begränsa skada, åtgärda brister och utreda eventuell brottslighet. En väl fungerade rapportering och hantering av incidenter hjälper oss att prioritera och att hitta rätt nivå på de säkerhetsåtgärder vi vidtar. Det är informationsägarens/den personuppgiftsansvariges ansvar att säkerställa att incidenten rapporteras till tillsynsmyndigheter enligt gällande lagstiftning.

8.2 Rapportering till tillsynsmyndighet

Incidentrapportering för leverantörer av samhällsviktiga tjänster

Incidenter som har en betydande inverkan på kontinuiteten i samhällsviktiga och digitala tjänster som levereras av Ängelholms kommun ska säkerställa förmåga att utan onödigt dröjsmål rapportera incidenter till sektorsansvarig tillsynsmyndighet.[8]

Incidentrapportering av personuppgiftsincidenter

En personuppgiftsincident är en incident som negativt har påverkat integritet, konfidentialitet, riktighet eller tillgänglighet till personuppgifter.
Är det inte osannolikt att incidenten kan medföra en risk för den enskildes rättigheter och friheter ska anmälan till Integritetsskyddsmyndigheten inom 72 timmar. [9]

Dataskyddsombudet ska meddelas i de fall anmälan till Integritesskyddsmyndigheten ska upprättas.

[8] Se vidare om incidentrapportering i MSBFS 2018:9/10 Föreskrifter och allmänna råd för rapportering av incidenter för leverantörer av samhällsviktiga tjänster
[9] Artikel 33 dataskyddsförordningen

73. Ängelholms kommun och bolag ska säkerställa god kännedom hos samtliga medarbetare om vad som kan utgöra incidenter och hur de ska hanteras.
74. Det ska finnas ett IT-system för rapportering av incidenter för att säkerställa effektiv rapportering och uppfyllande av kraven på dokumentation.
75. Det ska finnas en process för handläggning, beslut och anmälan av incidenter till tillsynsmyndigheter.
76. Ytterligare vägledning om incidenter meddelas i särskild instruktion.

9. Ledningssystem för informationssäkerhet (LIS)

Av Policy för informationssäkerhet och personuppgiftsbehandling framgår att Ängelholms kommun ska bedriva ett systematiskt informationssäkerhetsarbete som baseras på standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS). Att planera och införa ett LIS är ett stort arbete som kommer att pågå under flera år.

Statliga myndigheter har sedan 2009 krav på LIS enligt MSBs föreskrifter MSBFS 2020:6 (tidigare 2016:1) om informationssäkerhet för statliga myndigheter. Det är numera också ett krav för sådan verksamhet som levererar samhällsviktiga tjänster enligt Lag om informationssäkerhet för samhällsviktiga och digitala tjänster.

Ett LIS är ett etablerat begrepp för ett systematiskt arbete med informationssäkerhet och innebär en metodik som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. LIS avser här inte ett IT-baserat system, även om IT-stöd kan användas i delar av ett LIS.

Ett systematiskt arbete med informationssäkerhet med ett LIS syftar i stort till att informationssäkerheten över tid anpassas efter interna och externa förutsättningar, och som därigenom upprätthåller en lämplig skyddsnivå över tid.

Standardserien SS-ISO/IEC 27000 tar sin utgångspunkt i ett verksamhets- och riskorienterat arbete snarare ett teknikorienterat. Standardserien är väletablerad i hela världen vilket medför stora fördelar bland annat genom gemensam terminologi i samverkan med andra.

I SS ISO/IEC 27000 Översikt och terminologi beskriver de standarder som ingår i 27000-serien. Här finns också de termer som används i de övergripande standarderna på informationssäkerhetsområdet samlade. Förutom översikt och terminologi förs även ett resonemang kring betydelsen av att arbeta strukturerat

med informationssäkerhet och vilken nytta en organisation har av att ta stöd i 27000-standarderna.

SS-EN ISO/IEC 27001:2017 Ledningssystem för informationssäkerhet – Krav är den standard som beskriver ledningssystemet och som man kan certifiera sig mot.

SS-EN ISO/IEC 27002:2017 Ledningssystem för informationssäkerhet – Riktlinjer beskriver vilka säkerhetsåtgärder ledningssystemet generellt ska innehålla. Kapitlen i 27002 har fokus på säkerhetsåtgärder men omfattar även frågor om styrning av informationssäkerhet såsom regelverk för informationssäkerhet (policy), organisation och efterlevnad.

ISO/IEC 27003:2017 Information Technology – Security Techniques – Information Security Management Systems – Guidance ger vägledning i hur en organisation kan uppfylla kraven i 27001.

MSB har på uppdrag av regeringen utarbetat ett metodstöd med syfte att stötta organisationer i att bedriva ett systematiskt informationssäkerhetsarbete.[10] Metodstödet kompletterar styrdokument för informationssäkerhet och personuppgiftsbehandling som relevant stödmaterial till kommunens verksamheter i hur det systematiska arbetet kan bedrivas i kommunen.

Metodstödet är uppdelat i de fyra metodstegen:

- Identifiera och analysera.
- Utforma.
- Använda.
- Följa upp och förbättra.

10. Metod för systematiskt arbete med informationssäkerhet och personuppgiftshantering

10.1. Systematiskt informationssäkerhetsarbete i fyra steg

Av Ängelholm kommuns policy för Informationssäkerhet och personuppgiftsbehandling framgår att arbete med informationssäkerhet ska bedrivas på ett systematiskt och riskbaserat sätt med fokus på förebyggande åtgärder. Samtliga punkter nedan förtydligas i instruktioner som riktar sig till ansvariga och till de medarbetare som ska arbeta med informationssäkerhetsfrågor.

[10] Metodstödet bygger på standarder i SS-EN ISO/IEC 27000-serien.

1. Information ska klassas avseende aspekterna konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få.
2. Risker för information ska identifieras, analyseras och värderas. Dessa ska dokumenteras i en risk- och konsekvensanalys. Om information omfattar personuppgifter ska en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen genomföras i de fall det finns hög risk för de registrerades rättigheter och friheter.
3. Behov ska identifieras samt ändamålsenliga och proportionella säkerhetsåtgärder ska införas utifrån genomförd informationsklassing och riskbedömning.
4. Säkerhetsåtgärderna ska utvärderas och skyddet av informationen anpassas efter förändrade förutsättningar.

10.2 Informationsklassning

Informationsklassning är grundläggande för informationssäkerhetsarbetet. Genom klassningen skapas förståelse för vilka informationsmängder som finns i verksamheten. Skyddet ska naturligtvis vara tillräckligt utifrån lagkrav och övriga krav men det gäller också att undvika kostsamma överskydd. Viss information är mer känslig än annan. Behovet av skydd skiljer sig därför mellan olika typer av information och i olika situationer. Skyddsbehovet beror på legala krav och vilka konsekvenser det skulle få för verksamheten eller för enskilda individer om informationen sprids till obehöriga.

Det är informationen som ska klassas, och som sedan styr vilka skyddsåtgärder de olika nivåerna av skyddskrav medför. Klassningen används sedan för att ställa rätt krav på de resurser som används för att hantera informationen, t.ex. programvaror, tjänster och fysiska tillgångar. Ett IT-system ska klassas utifrån den information som hanteras i systemet, där den mest känsliga informationen kommer att styra vilka säkerhetskrav som uppställs.

Identifiering och klassificering av information ska ske innan ett system upphandlas/köps in men också som ett led i löpande förbättring eller vid förändringar av verksamheter eller IT-system.

Ängelholms kommuns modell för klassning av information bygger i huvudsak på en modell framtagen av Svenska institutet för standarder (SIS) och Myndigheten för beredskaps (MSB). Liksom SKR:s verktyg ”Klassa” har modellen utökats med konsekvensnivån 4 – Synnerligen allvarlig skada. Nivå 4 omfattar säkerhetsskyddsklassificerade uppgifter och rör rikets säkerhet. Uppgifterna som bedöms hamna på nivå 4 ska dokumenteras och hanteras enligt särskild instruktion. Kommunens säkerhetsskyddschef ska kontaktas om uppgifter hamnar på nivå 4.

Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet	Skyddsnivå
Synnerligen allvarlig skada	K4	R4	T4	Mycket höga skyddskrav
Allvarlig skada	K3	R3	T3	Höga skyddskrav
Betydande skada	K2	R2	T2	Förhöjda skyddskrav
Måttlig skada	K1	R1	T1	Normala skyddskrav
Ingen/försumbar skada	K0	R0	T0	Låga skyddskrav

Ansvaret för att information klassas följer verksamhetsansvaret. Beroende på hur klassningen av informationen utfaller kommer det att ställas olika säkerhetskrav för skydd av informationen som sedan utgör underlag vid verksamhetens kravställning av tjänster, exempelvis IT-tjänster, både internt och externt.

Informationsklassning är ett pågående arbete inom Ängelholms kommun. Kompletterande instruktion avsedd för de som arbetar med klassning av information kommer att tas fram för närmare tillämpningsanvisningar kring hur arbetet med informationsklassning och risk- och konsekvensanalys ska genomföras.

11. Efterlevnad och granskning

Efterlevnad av de styrande dokumenten ska följas upp. I synnerhet gäller detta de särskilda säkerhetsåtgärder som gäller för information, objekt och IT-resurser med höga skyddskrav. Granskning och uppföljning av informationssäkerhet, inklusive dess styrning, kommer att utvecklas i och med det ledningssystem för informationssäkerhet (LIS) som ska införas i kommunen, då det är en mycket viktig del i ett LIS.

77. Efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet ska följas upp.
78. Granskning av IT-säkerhet för IT-resurser ska ske regelbundet med syftet att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls.
79. Informationssäkerheten ska utsättas för oberoende extern granskning.
80. Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. förvaltningsplaner.
81. Akuta sårbarheter och brister ska åtgärdas omedelbart.
82. Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet.

12. Säkerställa de registrerades rättigheter i enlighet med dataskyddsförordningen

En fysisk person vars personuppgifter behandlas kallas för en registrerad. Registrerade är anställda, förtroendevalda, brukare, kunder, elever, leverantörer, externa kontakter med flera. Dataskyddsförordningen tillskriver den registrerade vissa rättigheter (se nedan). I offentlig förvaltning gäller emellertid flera av rättigheterna endast i begränsad omfattning eftersom det inte är tillåtet att ändra eller slänga allmänna handlingar hur som helst.

12.1 **Rätten till information**

Personuppgiftsansvarig är skyldig att informera en registrerad om en personuppgiftsbehandling. Vilken information som ska omfattas regleras i lag. På vilket sätt informationen ska lämnas bedöms utifrån vad som är lämpligt för den aktuella personuppgiftsbehandlingen.

83. Information till anställda lämnas vid anställningen samt på intranätet.

84. Information till medborgare lämnas genom en tydlig redovisning på externa webben av den personuppgiftsbehandling som genomförs.

85. I e-postsignaturen ska en länk finnas med hänvisning till information om behandling av personuppgifter på externa webben.

Rätten till registerutdrag På begäran av en registrerad är personuppgiftsansvarig skyldig att tillhandahålla ett registerutdrag över vilka personuppgifter som behandlas om den registrerade i den personuppgiftsansvariges verksamhet. Närmare information kring registerutdrag ges i instruktion för framställande av registerutdrag.

86. Begäran kan endast avse den registrerade själv eller barn som står under dennes vårdnad.

87. Begäran om registerutdrag kan antingen göras via kommunens digitala e-tjänst eller skriftligen.

88. Legitimering ska ske både vid begäran om utdrag och vid utlämnandet.

89. En sekretessprövning enligt offentlighets- och sekretesslagen ska göras innan uppgifterna lämnas ut.

90. Utlämnandet kan ske via den digitala e-tjänsten eller avhämtas i reception. Sker utlämnandet via post skickas utdraget till folkbokföringsadressen. Registerutdrag som innehåller känsliga uppgifter ska skickas med rekommenderat brev.

91. Registerutdrag ska aldrig skickas via e-post.

Rättelse av personuppgifter Den personuppgiftsansvarige ska inom rimlig tid rätta uppgifter som innehåller sakliga fel eller personuppgifter som inte får behandlas. Rättelse kan ske på begäran av den registrerade, men den personuppgiftsansvarige ska även självmant vidta rättelse när ett fel enligt ovan upptäcks. I samband med att felet rättas ska tidigare felaktiga uppgifter tas bort.

Ytterligare rättigheter Enligt dataskyddsförordningen har den registrerade rätten att begära att uppgifter raderas samt att få ut sina uppgifter i ett allmänt läsbart format (portabilitet). Radering är sällan aktuellt eftersom informationen oftast finns i allmän handling varvid den tas bort i samband med gallring i enlighet med gallringsplanen. Dataportabilitet aktualiseras i huvudsak när den registrerade själv tillfört information eller lämnat information med stöd av samtycke.

12.2 Prövning av en begäran från registrerad

Inkommer en begäran från en registrerad som vill utöva sina rättigheter ska begäran prövas. Om begäran nekas helt eller delvis har den registrerade rätten till ett motiverat beslut med överklagandehänvisning. Vilka beslut som kan överklagas framgår av dataskyddslagen

12.3 Klagomål

Den registrerade kan lämna klagomål som rör en personuppgiftsbehandling till personuppgiftsansvarig, till dataskyddsombudet och till Integritets-skyddsmyndigheten (tillsynsmyndighet).

13. Personuppgiftsansvarigs övriga skyldigheter enligt dataskyddslagstiftningen

Följande ska genomföras inför att en personuppgiftsbehandling påbörjas:

92. Fastställ ändamålet och den lagliga grunden för personuppgiftsbehandlingen.
93. Säkerställ att verksamheten inte samlar in och behandlar mer personuppgifter i behandlingens olika steg än vad som är nödvändigt i förhållande till ändamålet och den lagliga grunden.
94. Personuppgifterna ska klassas enligt kommunens klassningsmodell. Behandlingen ska vidare analyseras i en risk- och konsekvensanalys och analysen ligger sedan till grund för vilka säkerhetskrav som ska ställas på behandlingen. Säkerhetsåtgärderna kan vara fysiska, administrativa eller tekniska säkerhetsåtgärder.

95. Visar risk- och konsekvensanalysen att personuppgiftsbehandlingen kan innebära hög risk för de registrerades rättigheter och friheter så ska en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen genomföras. Dataskyddsombudet ska alltid rådfrågas.

96. Personuppgiftsbehandlingen ska registreras i kommunens registerförteckning över personuppgiftsbehandlingar.

14. Organisation, roller och ansvar

Huvudprincip - Ansvaret för informationssäkerhet och dataskydd följer verksamhetsansvaret på alla nivåer inom kommunorganisationen. Ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten och dataskyddet inom verksamhetsområdet.

Informationssäkerhetsansvariga och övriga som arbetar specifikt med informationssäkerhet, dataskydd, IT-säkerhet eller andra relaterade frågor, utgör stödfunktioner.

Kommunstyrelsen ansvarar för en kommungemensam förteckning över intern ansvarsfördelning mellan personuppgiftsansvarig och interna biträde samt delat personuppgiftsansvar inom kommunorganisationen.[11] Förteckningen ska uppdateras löpande men ska minst en gång årligen godkännas av kommunstyrelsen.

14.1 Dataskyddsombudet

Dataskyddsombudets ansvar och ställning styrs utifrån Dataskyddsförordningen. Ombudet bedriver sitt arbete på ett självständigt och oberoende sätt fritt från styrning av personuppgiftsansvariga. Ombudet har inte ett formellt ansvar för dataskydd och hanteringen av personuppgifter hos personuppgiftsansvarig. Det huvudsakliga syftet med dataskyddsombudets roll och arbete är att stödja ledningen och verksamheterna samt kontrollera efterlevnaden av Dataskyddsförordningen.

Detta innebär att dataskyddsombudet ska:

- ge råd och information gällande informationssäkerhet och dataskydd till personuppgiftsansvarig.
- arbeta med omvärldsanalys avseende dataskydd.
- ge stöd genom att planera och genomföra utbildningsinsatser.

[11] Inom kommunorganisationen förekommer det situationer där medarbetare som svarar under en nämnd eller styrelse behandlar personuppgifter på uppdrag åt en annan nämnd eller styrelse Eftersom kommunen är en och samma juridiska person kan inte ett personuppgiftsbiträdesavtal tecknas mellan parterna. Det kan även förekomma situationer där personuppgiftsansvaret är delat mellan två nämnder.

- bistå lokala och centrala dataskyddssamordnare genom att vägleda dem i deras frågor gällande dataskydd.
- bjudas in till och vara delaktig vid konsekvensbedömningar.
- med stöd av artikel 39 i Dataskyddsförordningen, kontrollera och följa upp personuppgiftshantering genom att utföra interna och externa revisioner.
- samarbeta med Integritetsskyddsmyndigheten och fungera som kontakt till myndigheten.
- vara kontaktyta för de registrerade vars personuppgifter hanteras i verksamheterna.

14.2 IT-säkerhetsansvarig

IT-säkerhetsansvarig ansvarar för IT-säkerheten i kommunens IT-infrastruktur, IT-drift och tjänster genom att tillse att dessa hanterar verksamhetens information enligt krav på IT-säkerhetsåtgärder.

Detta innebär att IT-säkerhetsansvarig ska:

- ansvara för att ta fram riktlinjer och rutiner för IT-säkerhet, inklusive adekvat uppföljning.
- stödja systemägare vid anskaffning, administration, utveckling, drift och avveckling.
- tillse att medarbetare och konsulter på IT-avdelningen följer gällande riktlinjer och rutiner för informationssäkerhet.
- tillse att medarbetare och konsulter på IT-avdelningen får den utbildning i informationssäkerhet och dataskydd som krävs.
- ta fram och underhålla regler för IT-användning till kommunkoncernens medarbetare.
- säkerställa en tydlig och effektiv ansvarsfördelning för systemägare, systemförvaltare och systemadministratörer.

14.3 Systemförvaltarorganisation

Informations- och systemägare samt informations- och systemförvaltarrollerna ingår alla i Ängelholm kommunens systemförvaltarorganisation. Systemförvaltarorganisationen fyller en viktig funktion i att upprätthålla en god informationssäkerhet i de informationssystem och digitala tjänster som kommunens verksamheter hanterar information i. Informations- och systemägare samt informations- och systemförvaltarrollerna ska ha ett mycket nära samarbete med dataskyddssamordnare, informationssäkerhetssamordnare och arkivfunktioner. För kommungemensamma informationssystem kan flera informationsägare kravställa mot en systemägare.

14.4 Informationsägare

Informationsägare är den som har behov av informationen. Informationsägare är nämnd eller bolag. Ansvaret följer verksamhetsansvaret, och i kommunintern dokumentation ska huvuduppdragschef/servicestödschef/verkställande direktör eller den verksamhetschef som svarar mot nämnd anges som informationsägare. Kommundirektören ska anges som informationsägare för information som rör kommunledningens stab samt de verksamheter/enheter som ligger under kommundirektören.

Informationsägaren

- ska säkerställa en tillräcklig konfidentialitet, riktighet, tillgänglighet och spårbarhet till information i förhållande till verksamhetens behov och gällande lagkrav.
- ansvarar för att klassning av information genomförs, beslutar om skyddsnivå, krav på säkerhetsåtgärder och om vilka risker som måste hanteras och vilka som är acceptabla för verksamheten.
- ansvarar för att systemägaren informeras om informationens klassning och kravställer utifrån behov av säkerhetsnivå.

Varje myndighet har ett ansvar iför att hanteringen av allmänna handlingar styrs och planeras effektivt och ändamålsenligt. För detta ändamål ska dokumenthanteringsplaner upprättas. Planen ska revideras vartannat år. Dokumenthanteringsplanen ska bland annat utvisa när handlingar får/ska gallras.

Verksamhetssystem som innehåller elektronisk information som ska långtidslagras eller föras över till annat medium ska dokumenteras enligt Riksarkivets föreskrifter för systemdokumentation. För dokumentationen ansvarar den myndighet som har arkivansvar.

Beslut om gallring kan fattas av myndigheten efter samråd med kommunarkivet.

14.5 Informationsförvaltare

Informationsförvaltaren ingår i informationsägarens organisation och är den som aktivt förvaltar informationen på informationsägarens uppdrag.

Informationsförvaltaren

- ska ha en djup och bred förståelse för varför information registreras på sättet det görs, flödet av informationen och användandet av informationen i till exempel informationssystem och kringliggande system.
- är kontaktperson mot CISO och rapporterar till informationsägare. Den ska arbeta utifrån informationsägarens mål i mycket nära kontakt med verksamheten.

- ansvarar för informationen och registrerar, förändrar och tar bort information i verksamhetssystemen.
- arbetar i nära samarbete med arkivfunktioner.
- deltar vid upphandlingar för att säkerställa att informationssäkerhetens alla aspekter beaktas.
- ansvarar för myndighetens/bolagets dokumenthanteringsplan.

För verksamhetssystem/IT-verktyg finns systemförvaltare. Ett verksamhetsstöd kan betjäna flera informationsägare, exempelvis ett diarium som används av flera nämnder.

14.6 Systemägare

Systemägaren har det övergripande ansvaret för ett informationssystem eller en digital tjänst. Rollen som systemägare vilar ytterst och formellt sett på ansvarig nämnd/styrelse. Ansvaret följer dock verksamhetsansvaret och i kommunintern dokumentation ska huvuduppdragschef/servicestödschef/verkställande direktör eller den verksamhetschef som svarar mot nämnd anges som systemägare.

För kommungemensamma system ansvarar kommunstyrelsen och i dokumentationen anges lämplig servicestödschef som systemägare. Kommundirektören är systemägare för system som förvaltas av verksamheter/enheter som ligger under kommundirektören. Samtliga informationssystem, oavsett intern eller extern drift, ska ha en utsedd systemägare.

Systemägaren
- ska säkerställa att informationssystemet/den digitala tjänsten tekniskt uppnår en adekvat skyddsnivå utifrån de krav som informationsägaren ställt på informationshanteringen. Systemägaren ska därför genomföra en riskanalys av systemet.
- tecknar avtal kring drift och förvaltning av system.

14.7 Systemförvaltare

Systemförvaltarens ingår i systemägarens organisation och är den som aktivt förvaltar informationssystemet på systemägarens uppdrag.

Systemförvaltaren

- har övergripande ansvar för verksamhetssystem och samordnar verksamhetssystemfrågor (till exempel planering av systemuppgradering).
- deltar vid upphandlingar och i systemförvaltningsforum.

14.8 Samordningsfunktioner informationssäkerhet

Informationssäkerhetssamordnare, CISO

CISO arbetar på uppdrag av kommunledningen och ska

- ansvara för att leda, samordna och följa upp det kommunövergripande systematiska arbetet med informationssäkerhet.
- utgöra stöd för kommunens verksamheter i deras utformning och arbete med systematisk informationssäkerhet.
- rapportera årligen, på lämpligt sätt, till kommunledningen.
- leda informationssäkerhetsrådet och vara systemförvaltare för kommunens klassificeringsverktyg.

Lokal informationssäkerhetssamordnare

Funktionen är underställd huvuduppdragschef inom respektive huvuduppdrag, servicesstödschef samt VD i respektive bolag.

Den lokala informationssäkerhetssamordnaren

- leder, samordnar och följer upp det systematiska informationssäkerhetsarbetet inom huvuduppdraget/servicesstödsverksamhet/bolaget
- utgör det primära stödet för huvuduppdragets/ servicesstödets/bolagets verksamheter i dess utformning och arbete med systematisk informationssäkerhet.
- genomför klassning av information samt risk- och sårbarhetsanalyser på uppdrag av Informationsägaren.
- är huvuduppdragets/ servicesstödsverksamhetens/bolagets kontaktperson gentemot den centrala informationssäkerhetssamordnaren.
- representerar huvuduppdraget/ servicesstödsverksamheten/bolaget i kommungemensamma nätverk och samarbetsforum.

Lokal kontaktperson informationssäkerhet

Inom samtliga verksamheter samt inom större enheter där det bedöms lämpligt ska det finnas en särskilt utsedd kontaktperson. Kontaktpersonen känner väl förutsättningarna i verksamheten och jobbar aktivt med informationssäkerhetsfrågor i verksamheten. Är den lokala informationssäkerhetssamordnarens och CISOs kontakt ute i verksamheten.

14.9 Samordningsfunktioner personuppgiftshantering (dataskydd)

Central dataskyddssamordnare vid Säkerhetsenheten

Kommunstyrelsen har samordningsansvar för det systematiska arbetet med personuppgiftshantering (dataskydd) på kommunövergripande nivå.

Den centrala dataskyddssamordnaren

- leder, samordnar och följer upp det systematiska arbetet kring behandling av personuppgifter på uppdrag av kommunstyrelsen.
- ska vara väl insatt i regelverket kring dataskydd och hålla sig uppdaterad kring utvecklingen på området.
- utgör stöd för kommunens verksamheter och bolag i juridiska avvägningar kring dataskydd så som ändamål, laglig grund, registrerades rättigheter, dokumentationsskyldighet, skyldighet att anmäla incidenter etc.
- är systemförvaltare för informationssystem och digitala tjänster gällande personuppgiftshantering t.ex. kommunens registerförteckning.
- sammankallar och leder dataskyddsnätverket.
- rapporterar till kommunledning och är dataskyddsombudets huvudsakliga kontaktperson.

Lokal personuppgiftssamordnare

Den lokala personuppiftssamordnaren är en stödfunktionen och är underställd huvuduppdragschef inom huvuduppdrag, verksamhetschef inom servicestöd samt VD inom bolag.

Den lokala personuppgiftssamordnaren

- leder, samordnar och följer upp det systematiska dataskyddsarbetet inom huvuduppdraget/verksamheten/bolaget.
- utgör det primära stödet för huvuduppdragets/verksamhetens/bolagets verksamheter i deras utformning och arbete med personuppgiftshantering.
- är huvuduppdragets/verksamhetens/bolagets kontaktperson gentemot dataskyddsombudet och mot den centrala samordningsfunktionen under kommunstyrelsen.
- registrerar pågående personuppgiftsbehandlingar i registerförteckningen och följa upp så att dessa är aktuella
- stödjer verksamheten vid begäran av registerutdrag
- stödjer verksamheten i upprättade av skriftliga avtal med personuppgiftsbiträden
- stödjer verksamheterna och medarbetarna i frågor som rör dataskydd

- initierar, planerar och följer upp arbetet med dataskydd.
- ska ha en löpande dialog med verksamhetens ledning angående dataskydd.
- ska omvärldsbevaka inom verksamhetsområdet och informera verksamheten samt vara kontaktyta mot dataskyddsombudet.

Lokal kontaktperson personuppgiftshantering

Inom samtliga verksamheter samt inom större enheter där det bedöms lämpligt ska det finnas en särskilt utsedd kontaktperson. Kontaktpersonen känner väl till förutsättningarna i verksamheten och jobbar aktivt med personuppgiftshantering i verksamheten. Kontaktpersonen utgör verksamhetens kontakt i personuppgiftsfrågor.

14.10 Kommunövergripande nätverk/samarbetsråd

Dataskyddsnätverk

Kommunens dataskyddsnätverk leds och sammankallas av dataskyddsombudet, om dataskyddsombud rekryteras internt. I annat fall av central dataskyddsamordnare. Nätverket består minst av kommunens lokala dataskyddssamordnare. Mål och syfte med nätverket är att underlätta kunskapsutbytet inom kommunorganisationen samt att aktivt bidra i arbetet med att identifiera behov samt utarbeta kommungemensamma rutiner, tjänster och arbetssätt.

I det fall funktionen som dataskyddsombud upphandlas externt bör dataskyddsombudet hållas underrättad samt vid behov bjudas in.

Informationssäkerhetsråd

Rådets medlemmar kan variera över tid beroende på identifierade behov i kommunen, men ska minst bestå av CISO, dataskyddsombud eller central dataskyddssamordnare, säkerhetsskyddschef, digitaliseringschef och stadsarkivarie. Ytterligare roller som kan vara aktuella i rådet, antingen som ordinarie medlemmar eller adjungerade, är till exempel driftschef samt lokala informationssäkerhetssamordnare. Rådet samverkar kring informationssäkerhetsfrågor som kräver en bred förankring och samordning inom kommunorganisationen. Rådets arbete ska bidra till att ge ledningen underlag, stöd och råd i dess arbete med att leda kommunens övergripande informationssäkerhetsarbete. Informationssäkerhetsrådet leds av CISO som också är sammankallande.

Externt dataskyddsombud bör hållas underrättad i frågor som rör personuppgiftshantering/dataskydd och vid behov bjudas in.

14.11 Systemförvaltningsforum

Digitaliseringsenheten ansvarar för Systemförvaltningsforum. Deltagare är systemförvaltare och kompetenser från digitaliseringsenheten. Syftet är att

- skapa förutsättningar för en hållbar, säker och tillgänglig digital miljö.
- kvalitetssäkra system.
- avhandla driftsfrågor.
- informera om centrala frågor.
- tydliggöra roller som knyter an till IT/digitalisering så som systemägare, systemförvaltare och e-samordnare inom samtliga verksamheter.

14.12 Arkiv

Kommunstyrelsen är Arkivmyndighet och ansvarar för den kommunala arkivverksamheten som framgår av arkivlagen (SFS 199:782), arkivförordningen (SFS 1991:446) och Arkivreglementet. Arkivmyndigheten utövar tillsyn över att kommunens myndigheter fullgör sina skyldigheter beträffande arkivbildningen och dess syften samt över arkivvården i kommunen.

Kommunarkivet fullgör arkivmyndighetens uppgifter och är dess beredande och verkställande organ. Kommunarkivet ska:

- vårda och tillhandahålla till arkivmyndigheten överlämnade arkivhandlingar.
- säkerställa vården, skyddet och hanteringen av de handlingar som omgärdas av sekretess/PuL och som överlämnats till arkivmyndigheten.
- utöva tillsyn och ge kommunens myndigheter råd i arkivfrågor.
- ta initiativ till åtgärder för att utveckla arkivvården.
- främja arkivens tillgänglighet och dess användning i kulturell verksamhet, forskning och utbildning.

Kommunarkivet kan regelbundet inspektera myndigheterna och får i samband med detta förelägga myndighet att åtgärda brister som konstaterats. Kommunarkivet kan till kommunens revisorer anmäla missförhållanden som konstaterats.

Högsta ansvarig tjänsteman inom respektive nämnd är arkivansvarig för sitt område och svarar mot respektive nämnd/nämnder.

Arkivansvarig ska utse ett eller flera arkivombud för varje nämnd respektive för de enheter som sysslar med personalfrågor, ekonomi och administration. Dessa ska i samråd med den arkivansvarige vårda myndighetens arkiv.