Åmåls Kommun

Regler för digital informationshantering

- informationssäkerhet och dataskydd

Beslutat av: Kommunstyrelsen
Datum: Den 12 april 2023, § 89, dnr 2023-00124
Dokumentets giltighet: År 2023–2026
Dokumentet gäller för: Kommunstyrelsen, bolag, nämnder samt deras förvaltningar och verksamheter
Dokumentansvarig: Kansli- och utredningsenheten

Strategi Program Plan Policy Riktlinjer **Regler**

Digital informationshantering i Åmåls kommun

Digitala informationshantering innebär att samla in, organisera, dela och lagra information så att denna kan användas på ett ändamålsenligt och kontrollerat sätt. Dessa regler beskriver på ett överskådligt och kortfattat sätt hur digital informationshantering ska fungera utifrån informationssäkerhet och dataskydd i Åmåls kommun.

Var och hur du ska hantera information och handlingar styrs av din förvaltnings dokument-hanteringsplan, gällande lagstiftning samt Åmåls kommuns IT- och informationssäkerhetspolicy. I denna policy beskrivs, på övergripande nivå, hur arbetet med att skydda vår information och våra IT-system ska bedrivas. Två av de övergripande mål som slås fast i policyn är:

- 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.

En av de primära åtgärder som finns för att garantera att målen ovan uppnås, är system för behörighetsstyrning. När du blir anställd eller får ett uppdrag i Åmåls kommun får du ett så kallat AD-konto (Active Directory), som är ett grundkonto att använda för all inloggning. Till ditt konto kopplas de program eller andra resurser som behövs för att du ska kunna utföra ditt arbete. Du får också licens för att använda programsviten M365, en digital plattform med ett antal olika funktioner för att kommunicera via e-post och chatt, dela och lagra dokument och information.

Informationssäkerhet handlar om åtgärder för att skydda information. Om du exempelvis arbetar utanför Åmåls kommuns nätverk eller på distans skyddas informationen bland annat genom att du använder kommunens skyddade nätverksanslutning (VPN).

Allmänna riktlinjer

- Uppgifter som omfattas av sekretess eller informationssäkerhets- och dataskyddslagar får inte hanteras i Microsoft 365 (Outlook, OneDrive, Teams, Sharepoint online, Planner med flera), Googles verktyg eller andra amerikanska molntjänster .
- Personuppgifter som inte är känsliga eller sekretessbelagda kan hanteras i Microsoft 365, Googles verktyg eller andra amerikanska molntjänster.

Det innebär bland annat:

- Att du hanterar information och uppgifter på ett lagenligt sätt. Den viktigaste lagen är offentlighets- och sekretesslagen som reglerar om informationen är offentlig eller sekretessbelagd.
- Att du behöver veta när en handling blir en allmän handling och vilka skyldigheter detta innebär (registrering, arkivering, utlämning av handlingar som är offentliga).
- Att du måste veta vilka uppgifter i din verksamhet som är sekretessbelagda och hur dessa ska hanteras.
- Att det finns även särskilda krav på behandling av personuppgifter enligt dataskyddsförordningen.

Information i Outlook

I Outlook kan du ta emot och skicka e-post, dela information och dokument samt boka möten. När du tar emot e-post har du begränsad kontroll på vad som kommer in. Det innebär att du behöver tänka på hur du ska hantera din e-post genom att bedöma innehållet och förmedla det vidare på det sätt som är lämpligt.

Du får ha mejlkonversationer med interna och externa parter fritt från sekretessbelagd och känslig information.

Du ska inte skicka sekretessbelagd eller känslig information i form till exempel utredningar, journaler, beslut som rör individer, information om exempelvis elever, brukare och patienter eller vidarebefordra inkommande mejl som innehåller sådant utan använd säkra kanaler som finns i din verksamhet.

Dokument och chatt i Teams/Google

Teams används för att kommunicera via chatt enskilt och i grupp, dela information och interna dokument. Dessa kan vara arbetsmaterial inom olika frågor, minnesanteckningar med beslut som rör interna arbetssätt och gemensamma interna rutiner, exempelvis rutin för bilbokning.

Du får chatta och dela information med dina medarbetare enskilt och i grupp så länge det är fritt från sekretessbelagd och känslig information.

Du ska inte chatta eller dela information om exempelvis elever, brukare och patienter och inte heller dela utredningar, tjänsteskrivelser, föra minnesanteckningar eller dela annan dokumentation som omfattas av sekretess eller känsliga uppgifter.

SharePoint/Ånet

SharePoint används för att dela information inom organisationen via kommunens intranät, Ånet, där även olika typer av dokument finns tillgängliga. Det kan vara fastställda dokument, både verksamhetsdokument och politiskt antagna styrdokument.

Du får dela fastställda dokument, både verksamhetsdokument och politiskt antagna styrdokument, fritt från sekretessbelagd och känslig information.

Du ska inte dela information om exempelvis elever, brukare och patienter eller dela utredningar, tjänsteskrivelser och minnesanteckningar eller annan dokumentation innehållande sekretessbelagd eller känslig information.

OneDrive

OneDrive är din personliga lagringsplats och är inte tillgänglig för andra. Det innebär att när ditt konto tas bort då du avslutar din tjänst på kommunen, blir all lagring knuten till kontot borttaget och allt på din OneDrive raderat.

Du får skapa, lagra och dela arbetsdokument fritt från sekretessbelagd och känslig information. Du bör dock överväga att lagra informationen i en annan tjänst om du har ett stort behov av att dela den med andra eller samarbeta i dokument.

Du ska inte skapa, lagra och dela information om exempelvis elever, brukare och patienter eller dela utredningar, tjänsteskrivelser, föra minnesanteckningar eller annan dokumentation innehållande sekretessbelagd eller känslig information.

G: mappar

I G: mapparna kan du lagra egna eller gemensamma dokument som kräver högre säkerhet/sekretess, men endast om det inte finns något verksamhetssystem som täcker behovet. Dessa mappar skapas med behörighetsstyrning, och denna administreras av IT-enheten. Du kan lagra dokument/filer som innehåller personuppgifter enligt GDPR, exempelvis från tredje part (Västra Götalandsregionen, andra

myndigheter), interna uppgifter som anhöriguppgifter, minnesanteckningar i personalärenden med mera.

Du får skapa och lagra egna eller gemensamma dokument som kräver högre säkerhet/sekretess där inget verksamhetssystem finns som täcker behovet. Din möjlighet att skapa mappar och katalogstrukturer kan dock vara begränsad och kan behöva beställas av IT-enheten.

Du ska hålla dig informerad om vilka mappar som gäller för vad och att rensa mappar med känsliga uppgifter så fort de inte längre behövs, enligt dokumenthanteringsplanen, eller lägga in dem i aktuellt verksamhetssystem.

Du ska inte spara informationssäkerhetsklassad information i G: mappar eller lagra och spara saker för att de är "bra att ha".

Du som lämnar behörighet till G: mappar

Som chef eller ansvarig för en eller flera G-mappar är det mycket viktigt att du regelbundet och systematiskt säkerställer behörighet till G-mappar med sekretessuppgifter, känslig information eller personuppgifter. Endast de medarbetare/handläggare som måste ha tillgång till informationen, ska ha rätt att läsa eller lagra information.

Du måste vara tydlig i din kommunikation när du ger en ny användare tillgång till G-mappar att den information som lagras där inte får delas fritt utan anses som känslig eller skyddsvärd information.

Lokalt på din dator

Information som du sparar genom dokument och filer som laddas ner från olika platser lagras lokalt på din dators hårddisk. Det är ditt eget ansvar att ha en övergripande koll på var på din dator dessa filer och dokument lagras så att du kan undvika att känslig information blir liggande oskyddad.

Du ska regelbundet gå igenom och rensa din dator från temporärt sparade filer minst 1 till 2 ggr/vecka.

Du ska inte spara känsligt material eller väsentlig information lokalt på din egen dator, både av säkerhetsskäl och för risken att information försvinner om din dator går sönder eller förloras.

Verksamhetssystem

Verksamhetssystem är designade för att kunna skydda all den information som dokumenteras, hanteras, lagras och diarieförs utifrån olika eller flera sammanlänkande lagstiftningar. Innehåller handlingarna sekretessbelagda eller känsliga uppgifter skall de skydden aktiveras på lämpligt sätt.

Du ska använda verksamhetssystem för att dokumentera och, där det är möjligt, kommunicera kring ärenden som rör individer där innehållet ska skyddas.

Du ska dokumentera, hantera, lagra och diarieföra olika typer av handlingar och dokument enligt de rutiner som finns för respektive verksamhet.

Säkra meddelanden

Genom säkra meddelanden kan du som är anställd i Åmåls kommun skicka och svara på meddelanden med känslig information på ett säkert och lagenligt sätt. Säkra meddelanden använder du när du ska kommunicera med någon runt känsliga, extra skyddsvärda och eventuellt sekretessbelagda uppgifter. Då minskar risken att uppgifterna hamnar på villovägar, och skyddet för den du kommunicerar med ökar. Det krävs inloggning både för att skicka och läsa meddelanden.

Du ska bedöma hur personuppgifterna ska behandlas för den fortsatta behandlingen när du läst ett meddelande. Personuppgifter som du får fortsätta att behandla i exempelvis ett ärendehanteringssystem bör du överföra dit.

Sekretess i möten och samtal i molntjänster

I situationer där sekretessreglerade uppgifter eller känsliga personuppgifter förekommer ska du säkerställa att du följer reglerna i dataskyddsförordningen och offentlighets- och sekretesslagen.

Du får hålla ett möte via Teams eller annan jämförbar molntjänst om du har de praktiska och fysiska förutsättningar som krävs för att säkerställa sekretess.

Du ska inte hålla ett möte via Teams eller annan jämförbar molntjänst om du inte kan säkerställa sekretessen. Då måste mötet istället hållas fysiskt eller genom telefonsamtal.

Verksamhetsspecifika regler/undantag

Dessa regler markerar en generell basnivå för alla verksamheter i kommunkoncernen.

I tillägg till dessa principer kan det finnas *kompletterande regler* i just din verksamhet, som du ska bli informerad om av din chef när du börjar din anställning. Sådana regler gäller då i tillägg eller som komplement till reglerna i detta dokument.

I förekommande fall där verksamheten inte kan efterleva dessa regler ska ansvarig chef genomföra en bedömning, upprätta en åtgärdsplan samt besluta om *tillfälligt undantag* för en särskild digital informationshantering.

Vill du veta mer?

Om personuppgifter Vad är personuppgifter? (imy.se)
Om hur verktyg i Microsoft365 fungerar ÅKE - Microsoft 365
Om Regler för digital informationshantering - informationssäkerhet och personuppgifter (infocaption.com)