



Program

Strategi

Policy

➤ **Riktlinje**

Rutin

Riktlinjer för lagring av digital information





Dokumentnamn:

Fastställd av:

Gäller från:

Riktlinjer för lagring av digital information

Kommunstyrelsen 2019-09-10, §216

2019-10-01

Berörd verksamhet:

Dokumentansvarig:

Gäller till:

Alla nämnder och förvaltningar

IT-Chef

2020-09-30

1. Inledning

I Östersunds kommun används ett flertal olika program för att skapa information och dokument. Det gör att det också finns ett flertal ställen att lagra information på. Sedan 2018 används Office 365 inom Östersunds kommun. Det är en molntjänst som möjliggör samarbete och att dela dokument med andra. Det innebär att vi måste vara medvetna om vart vi lagrar vår information och dokument. Riktlinjerna beskriver hur och vart verksamheterna kan lagra information på ett effektivt och säkert sätt.

2. Syfte

Riktlinjerna beskriver vart olika typer av information/dokument ska lagras för att det ska vara rätt säkerhetsnivå utifrån informationens känslighet och konfidentialitet.

3. Avgränsningar/förtydliganden

Riktlinjerna beskriver vart information/dokument ska lagras. Riktlinjerna ersätter inte dokumenthanteringsplanerna.

Riktlinjerna kan komma att revideras när dokumenthanteringssystemet införs.

4. Var lagrar jag min digitala information

När man arbetat med ett dokument måste man bestämma vart det ska sparas. Är det i Teams, Onedrive, (Office 365) gemensam filserver L: eller din personliga H: Vilket ställe som ska väljas beror på vilken åtkomst som kollegorna ska ha till dokumentet, vilket syfte och hur känslig informationen är i dokumentet. I tabellen beskrivs några exempel på olika känslighet och vart det bör lagras.

Klass/Nivå	Förklaring	Exempel på information	Var lagra
Öppen	Huvudsak allmänna offentliga handlingar som inte innehåller några personuppgifter.	<ul style="list-style-type: none">• Publik information avsedd att spridas externt.• Informationsmaterial• www.ostersund.se	<ul style="list-style-type: none">• Alla lagringsytor är ok.
Intern	Information som inte betraktas som allmänna handlingar, eller information som i huvudsak är avsedd för internt bruk, samt icke känsliga personuppgifter som gäller anställda enligt GDPR.	<ul style="list-style-type: none">• Icke känsliga arbetshandlingar• Presentationer, word-/Exceldokument, etc. som inte innehåller någon känslig information• Mejl som inte innehåller någon känslig information• Bilder, filmer, musik, etc. som kommunen äger upphovsrätt till	<ul style="list-style-type: none">• Gemensam katalog (L:)• Hemkatalog (H:)• Office 365, Teams, OneDrive• Lokalt på dator, USB, telefon, etc.• Samtliga tjänster och lagringsytor som tillhandahålls av Östersunds kommun och avsedda för aktuell behandling
Känslig	Sekretessbelagd information under svag sekretess samt känsliga personuppgifter.	<ul style="list-style-type: none">• Uppgifter som är föremål för sekretess enligt Offentlighets- och sekretesslagen.• Bilder på barn• Mail som innehåller känslig information. Är oklart hur vi ska jobba med det. Arbetas med tekniska lösningar	<ul style="list-style-type: none">• Gemensam katalog (L:)• Hemkatalog (H:)• Lokalt på kommundator, USB, telefon, etc. under förutsättning att filerna är krypterade och enheten är utfärdad av kommunen• Tjänster som är godkända för hantering av känslig information och avsedd för aktuell behandling• Pydio för skolan



ÖSTERSUNDS
KOMMUN

Dokumentnamn:

Riktlinjer för lagring av digital information

Berörd verksamhet:

Alla nämnder och förvaltningar

Fastställt av:

Kommunstyrelsen 2019-09-10, §216

Dokumentansvarig:

IT-Chef

Gäller från:

2019-10-01

Gäller till:

2020-09-30

Sekretess	<p>Sekretessbelagd information under stark och/eller absolut sekretess.</p> <p>Information som faller under särskilt lagrum och kräver för det lagrummet särskild hantering. Ställer ofta ytterligare krav på spårbarhet. Exempelvis PDL, SOL och LSS.</p>	<ul style="list-style-type: none">• Journalanteckningar• Information gällande elevhälsa• Ekonomiskt bistånd enligt SOL• Känsligare uppgifter gällande anställda, ex. uppgifter som förekommer i personalsocial verksamhet.• Förskolan	<ul style="list-style-type: none">• Ska lagras i för behandlingen avsett verksamhetssystem.• Annan lösning kräver gemensamt ställningstagande mellan verksamhet, Dataskyddsgruppen och IT-enheten.
Säkerhets- skydds- klassificerad	<p>Information som är skyddsvärd utifrån Sveriges säkerhet, totalförsvaret och/eller terrorism. Kallas ibland hemliga uppgifter.</p>	<ul style="list-style-type: none">• Uppgifter som rör säkerhets känslig verksamhet och omfattas av OSK eller skulle ha omfattats av sekretess enligt den lagen om den hade varit tillämplig.	<ul style="list-style-type: none">• Ska hanteras utifrån de bestämmelser som säkerhetsskyddslagen anger. Vid osäkerhet, kontakta säkerhetsskyddschef.

Observera att denna tabell endast avser krav på informationens konfidentialitet. Krav på tillgänglighet och riktighet kan innebära högre krav på lagringsytan än vad som anges i tabellen nedan.

I de fall det är tillåtet att använda lagringsutrymmen som ej är tillhandahållna av kommunen ansvarar informationsägaren för att gällande lagar och regler efterlevs.

5. Ansvarig

Denna riktlinje beslutas av Kommunstyrelsen. Kommunledningsförvaltningen, IT-enheten är dokumentansvarig och har ansvaret för att förvalta riktlinjerna vilket innebär att säkerställa tillämpning, följa upp och revidera vid behov. Varje chef inom den verksamhet som berörs av riktlinjen ansvarar för att dess innehåll är känt och att riktlinjen efterlevs.

6. Uppföljning

Riktlinjen följs upp årligen av dokumentansvarig som vid behov lyfter frågan till kommunstyrelsen.