Program Plan Policy Riktlinje

Riktlinje informationssäkerhet – lagring av information

Beslutad av: Kommunstyrelsen
Datum och paragraf: 2024-02-06, § 25
Revisionsdatum:
Dnr: 23KS48

Innehåll

1. Inledning

Kommunens administration är i stor utsträckning digital. När vi arbetar i verksamhetssystem eller i generella system (som till exempel M365) lagras information på olika lagringsytor. Informationen är olika känslig ur informationssäkerhetssynpunkt och lagringsytorna är olika säkra. Det är därför viktigt att ha koll på vilken information som lagras var.

2. Ansvar för informationsklassning

Olika information behöver klassificeras utifrån hur känslig den är. Olika informationsmängder ska ges en informationssäkerhetsklass. Detta dokumenteras i nämndernas informationshanteringsplaner (IHP). Det är informationsägaren som ansvarar för att säkerhetsklassning sker.

3. Ansvar för informationssäkerhet i system och lagringsytor

Ansvaret för att verksamhetssystem/lagringsytor håller rätt säkerhetsnivå utifrån den information de är avsedda att hantera åligger den verksamhetsnära systemförvaltningen, dvs respektive objektägare enligt gällande systemförvaltningsmodell.

4. Syfte med de här riktlinjerna

Riktlinjernas viktigaste funktion är att de reglerar var medarbetare i verksamheten får spara olika information. I de här riktlinjerna finns också förklaringar till de olika säkerhetsklasserna. De förklaringarna kan vara till vägledning för att bestämma informationssäkerhetsklass för en viss informationsmängd.

5. Avgränsningar och förtydliganden

De här riktlinjerna tar sin utgångspunkt i krav på informationens konfidentialitet, dvs att inte informationen röjs för utomstående. Det kan finnas krav på tillgänglighet och riktighet som ställer andra och högre krav på lagringsytor.

6. Var lagrar jag min digitala information?

Innan du arbetar med ett dokument måste du bestämma var det ska sparas. En viktig aspekt är hur känslig informationen är. Informationshanteringsplanen kan innehålla information om vilken säkerhetsklass den typ av dokument du arbetar med har. Den säkerhetsklassen kommer att vara avgörande för hur informationen får sparas. Kopplingen mellan säkerhetsklass och tillåtna lagringsytor framgår av tabellen.

I tabellen finns också förklaringar och exempel på information som kan hänföras till olika säkerhetsklasser. Det kan också vara till ledning då du ska åsätta ditt dokument en säkerhetsklass.

Det finns också andra aspekter att väga in när det gäller var information ska sparas, till exempel vilken åtkomst som kollegorna ska ha till dokumentet.

Klass/Nivå	Förklaring	Exempel på information	Var lagra
Öppen	Allmänna offentliga handlingar som inte innehåller några personuppgifter	• Publik information avsedd att spridas externt. • Informationsmaterial • Planer och policys • Webbinnehåll	• Alla kommunens lagringsytor är ok.
Begränsat öppen	Allmänna offentliga handlingar som kan innehålla personuppgifter som inte är känsliga personuppgifter	• Presentationer och andra dokument som inte innehåller någon känslig information • Mejl som inte innehåller någon känslig information	• Gemensam katalog (G:) • Utforskarens Dokument i datorn • Office 365, Teams, SharePoint, OneDrive • Lokalt på dator, USB, telefon, etc. • Samtliga tjänster och lagringsytor som tillhandahålls av kommunen och är avsedda för aktuell behandling
Känslig / sekretess	Sekretessbelagd information under svag sekretess samt känsliga personuppgifter.	• Alla typer av handlingar som innehåller någon form av information som kan antas omfattas av sekretess eller känsliga personuppgifter	• Verksamhetssystem som är godkända för hantering av känslig information och avsedd för aktuell behandling • Lokalt på dator och telefon under förutsättning att filerna är krypterade och enheten är utfärdad av kommunen med multifaktorsinloggning (MFA)
Hög sekretess	Sekretessbelagd information under stark och/eller absolut sekretess.	• Journalanteckningar • Information gällande elevhälsa • Ekonomiskt bistånd enligt SOL • Känsligare uppgifter gällande anställda	• Ska lagras i för behandlingen avsett verksamhetssystem.
Säkerhetsskydds-klassificerad	Information som är skyddsvärd utifrån Sveriges säkerhet, totalförsvar och/eller terrorism. Kallas ibland hemliga uppgifter.	Uppgifter som rör säkerhetskänslig verksamhet och omfattas av OSL eller skulle ha omfattats av sekretess enligt den lagen om den hade varit tillämplig.	Ska hanteras utifrån de bestämmelser som säkerhetsskyddslagen anger. Vid osäkerhet, kontakta säkerhetsskyddschef.