

Riktlinje för lagring av information i Ronneby kommunkoncern

Dokumenttyp: Riktlinje
Antaget av: Kommundirektören
Antagen: 2 september 2020
Giltighetstid: Tills vidare

Diarienummer: KS 2020/421

Ansvarig för dokumentet: Informationssäkerhetsansvarig och IT-chef

Tidpunkt för senaste aktualitetsprövning:

Tidpunkt för senaste revidering: 2 juni 2021

Relaterade styrdokument: Informationssäkerhetspolicy

Sökord: informationssäkerhet, lagring, säkerhetsklass, personuppgifter, riktlinjer för lagring

Innehåll

1. Syfte	4
2. Allmänt.....	4
3. Ansvar	4
4. Definitioner	4
4.1 Molntjänster.....	4
4.2 Publik information (säkerhetsklass 0).....	4
4.3 Personuppgifter (säkerhetsklass 1)	4
4.4 Konfidentiell information (säkerhetsklass 2)	5
4.5 Känsliga personuppgifter (säkerhetsklass 3).....	5
4.6 Information med högt skyddsvärde (säkerhetsklass 4).....	5
5. Lagringsnivåer	6
5.1 Publik information (Säkerhetsklass 0).....	6
5.2 Personuppgifter (Säkerhetsklass 1).....	6
5.3 Konfidentiell information (Säkerhetsklass 2).....	7
5.4 Känsliga personuppgifter (Säkerhetsklass 3)	7
5.5 Information med högt skyddsvärde (Säkerhetsklass 4)	8

1. Syfte

Riktlinjen syftar till att främja en säker lagring av information inom Ronneby kommunkoncern. Det innebär att förhindra att information obehörigt röjs, modifieras, avlägsnas eller förstörs. Informationen ska skyddas utifrån sitt värde.

2. Allmänt

Information som lagras behöver oberoende av lagringsplats klassas så att användaren vet var och hur informationen får hanteras och lagras, samt huruvida informationen får delas med någon annan.

Avsteg från kraven i riktlinjen ska lyftas till informationssäkerhetsansvarig. Riskanalys med konsekvensbedömning ska genomföras inför beslut.

3. Ansvar

Det är varje enskild medarbetares ansvar att känna till eller ta reda på värdet på uppgifterna som den enskilde medarbetaren behandlar samt vilka föreskrifter och riktlinjer som gäller.

4. Definitioner

4.1 Molntjänster

Endast av Ronneby Kommuns IT-enhet tillhandahållna och godkända molntjänster som hanteras i privata eller partners moln får användas inom verksamheterna. En godkänd molntjänst ska vara inköpt eller upphandlad, vara avsedd för de uppgifter den ska lagra samt uppfylla samtliga krav på säkerhet som motsvarar värdet av informationen. Avtal och personuppgiftsbiträdesavtal ska finnas.

4.2 Publik information (säkerhetsklass 0)

Publik information är information/data som är offentlig och som inte innehåller några personuppgifter.

4.3 Personuppgifter (säkerhetsklass 1)

Personuppgifter är enligt dataskyddsförordningen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Även bilder/foton och ljudupptagningar på individer kan vara en personuppgift även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som t.ex. IP-nummer, räknas som personuppgift om de kan kopplas till fysiska personer som är i livet. Personuppgifter i denna säkerhetsklass är allmänt kända och tillgängliga.

I många fall är personuppgifter offentliga och finns tillgängliga via publika källor. Beroende på situation kan de trots detta vara extra skyddsvärda eller sekretessbelagda enligt annan lagstiftning, t.ex. personer med skyddad identitet eller i kombination med känsliga personuppgifter.

4.4 Konfidentiell information (säkerhetsklass 2)

Konfidentiell information är enligt dataskyddsförordningen extra skyddsvärd eller integritetskänslig information. Det kan innefatta personnummer, löneuppgifter, uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler, uppgifter om sociala förhållanden eller andra uppgifter som inte är särskilt reglerade som känsliga men som kan vara mer skyddsvärda än andra uppgifter.

Konfidentiell information är också information som är avsedd att hållas hemlig inom en viss grupp av personer och därmed inte avsedd att göras allmänt känd. Exempel på konfidentiell information som inte innehåller personuppgifter, men som ändå räknas som konfidentiell, är arbetsmaterial för strategier, ekonomiska rapporter, tekniska beskrivningar, lösenord och nätarkitekturskisser.

4.5 Känsliga personuppgifter (säkerhetsklass 3)

Känsliga personuppgifter är enligt dataskyddsförordningen uppgifter som avslöjar:

- Etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i en fackförening
- Hälsa, t.ex. uppgifter som sjukfrånvaro, graviditet och läkarbesök
- En persons sexualliv eller sexuella läggning
- Genetiska uppgifter
- Biometriska uppgifter som används för att entydigt identifiera en person, t.ex. fingeravtryck

Denna typ av uppgifter är i grunden förbjudna att behandla. Det krävs därför ett undantag enligt dataskyddsförordning. Exempelvis har hälso- och sjukvården ett undantag för att behandla uppgifter om hälsa. Uppgifterna är som regel sekretessbelagda.

4.6 Information med högt skyddsvärde (säkerhetsklass 4)

Information med högt skyddsvärde är t.ex. säkerhetsskyddsklassad information som rör Sveriges säkerhet.

5. Lagringsnivåer

Lagring av Ronneby kommunkoncerns information är endast tillåten på enheter som tillhör eller är godkända av Ronneby Kommuns IT-enhet.

Nedan beskrivs var information får lagras, i de fall det finns krav står de specificerade för varje lagringsplats.

5.1 Publik information (Säkerhetsklass 0)

Gemensam lagringsyta Exempelvis: G, S, T, L:	Inga krav
H: personlig lagringsyta	Inga krav
Samarbetsyta Exempelvis: Öppna grupprum på Intranät	Inga krav
Särskild samarbetsyta Exempelvis: Behörighetsstyrda grupprum på intranätet	Inga krav
Intranät (Exempelvis nyheter, microblogg)	Inga krav
Molntjänster godkända av IT-enheten (Exempelvis verksamhetssystem)	Inga krav
Molntjänster ej godkända av IT-enheten	Inga krav
365 (Onedrive, Teams, mail m.m.)	Inga krav ¹

5.2 Personuppgifter (Säkerhetsklass 1)

Gemensam lagringsyta Exempelvis: G, S, T, L:	Inga krav
H: personlig lagringsyta	Inga krav
Samarbetsyta Exempelvis: Öppna grupprum på Intranät	Inga krav
Särskild samarbetsyta Exempelvis: Behörighetsstyrda grupprum på intranätet	Inga krav
Intranät (Exempelvis nyheter, microblogg)	Inga krav
Molntjänster godkända av IT-enheten (Exempelvis verksamhetssystem)	Inga krav
Molntjänster ej godkända av IT-enheten	Inga krav
365 (Onedrive, Teams, mail m.m.)	Inga krav ¹

¹ Se aktuell risk- och sårbarhetsanalys för berörd nämnd eller bolag.

5.3 Konfidentiell information (Säkerhetsklass 2)

Gemensam lagringsyta Exempelvis: G, S, T, L:	Informationen får lagras på en särskild utsedd lagringyta som är behörighetsstyrd.
H: personlig lagringsyta	Informationen får lagras på en särskild utsedd lagringyta som är behörighetsstyrd.
Samarbetsyta Exempelvis: Öppna grupper på Intranät	Informationen får inte lagras på en generell samarbetsyta.
Särskild samarbetsyta Exempelvis: Behörighetsstyrda grupper på intranätet	Informationen får lagras på en särskild utsedd lagringyta som är behörighetsstyrd.
Intranät (Exempelvis nyheter, microblogg)	Informationen får inte publiceras på Intranät.
Molntjänster godkända av IT-enheten (Exempelvis verksamhetssystem)	Inga krav
Molntjänster ej godkända av IT-enheten	Informationen får ej lagras i molntjänst.
365 (Onedrive, Teams, mail m.m.)	Informationen får ej lagras/hanteras i 365.

5.4 Känsliga personuppgifter (Säkerhetsklass 3)

Gemensam lagringsyta Exempelvis: G, S, T, L:	Informationen får lagras på en särskild utsedd lagringyta som är behörighetsstyrd, inloggning med stark autentisering (multifaktorsautentisering) och spårbarhet krävs.
H: personlig lagringsyta	Informationen får lagras på en särskild utsedd lagringyta som är behörighetsstyrd, inloggning med stark autentisering (multifaktorsautentisering) och spårbarhet krävs.
Samarbetsyta Exempelvis: Öppna grupper på Intranät	Informationen får inte lagras på en generell samarbetsyta.
Särskild samarbetsyta Exempelvis: Behörighetsstyrda grupper på intranätet	Informationen får lagras på en särskild utsedd lagringyta som är behörighetsstyrd, inloggning med stark autentisering (multifaktorsautentisering) och spårbarhet krävs.
Intranät (Exempelvis nyheter, microblogg)	Informationen får inte publiceras på Intranät.
Molntjänster godkända av IT-enheten (Exempelvis verksamhetssystem)	Inga krav
Molntjänster ej godkända av IT-enheten	Informationen får ej lagras i molntjänst.
365 (Onedrive, Teams, mail m.m.)	Informationen får ej lagras/hanteras i 365.

5.5 Information med högt skyddsvärde (Säkerhetsklass 4)

Gemensam lagringsyta Exempelvis: G, S, T, L:	Informationen får inte lagras på gemensam lagringsyta Exempelvis: G, S, T, L:
H: personlig lagringsyta	Informationen får inte lagras på H.
Samarbetsyta Exempelvis: Öppna grupprum på Intranät	Informationen får inte lagras på en generell samarbetsyta.
Särskild samarbetsyta Exempelvis: Behörighetsstyrda grupprum på intranätet	Informationen får inte lagras på särskild samarbetsyta.
Intranät (Exempelvis nyheter, microblogg)	Informationen får inte publiceras på Intranät.
Molntjänster godkända av IT-enheten (Exempelvis verksamhetssystem)	Inga krav
Molntjänster ej godkända av IT-enheten	Informationen får ej lagras i molntjänst.
365 (Onedrive, Teams, mail m.m.)	Informationen får ej lagras/hanteras i 365.
Filserver	Informationen får lagras på en krypterad lagringsyta med godkänd krypteringsteknik.

Denna riktlinje gäller från och med den 2 september 2020 och tills vidare enligt beslut av kommundirektör.

Tommy Ahlquist
Kommundirektör