Piteå kommun

Anvisning för hantering och lagring av digital information

Dokumentnamn	Dokumenttyp	Senast reviderad	Beslutsinstans
Anvisning för hantering och lagring av digital information	Anvisning	2020-11-13	Kommunchef
Dokumentansvarig/processägare	**Version**	**Diarienummer**	**Giltig till**
Kommunledningsförvaltningen	1	20KS545	2024-12-31
Dokumentinformation	Anvisning för hantering och lagring av digital information i väntan på införande av Ledningssystem för Informationssäkerhet (LIS)		
Dokumentet gäller för	Samtliga kommunala verksamheter		

Anvisningens syfte

Anvisningen beskriver ramar och principer för informationshantering vid lagring i egen regi, eller hos externa tjänsteleverantörer.

Syftet med anvisningen är att skapa struktur och goda förutsättningar för en säkrare informationshantering genom att tydliggöra ansvar, krav och förväntningar på centrala funktioner och verksamheter inom Piteå kommun och de kommunala bolagen.

Under rådande omständigheter behöver kommunen en anvisning som vägleder verksamheter och centrala funktioner, i avvaktan på nationella riktlinjer och införandet av **L**edningssystem för **I**nformations**s**äkerhet (LIS).

Utgångspunkt för anvisningen

Det systematiska arbetet kommer i framtiden att hanteras av kommunens LIS. Anvisningen utgår från samma principer som LIS, nedan punkt 1 och 2. Dessutom finns vägledning för hur verksamhetens informationsbedömning ska genomföras i väntan på att LIS införs.

Följande tre delar ingår:

1. Verksamhetens informationsansvar
2. Systemägarens ansvar
3. Vägledning för verksamhetens informationsbedömning i väntan på att LIS införs

1. Verksamhetens informationsansvar

Kommunens förvaltningar och bolag är informationsägare för sina respektive verksamheter.
Med det följer ett ansvar att:

- Bedöma känsligheten i den information som verksamheten hanterar.
- Utforma rutiner för verksamhetens informationshantering
- Säkerställa tillförlitliga systemlösningar
- Arbeta med ständiga förbättringar

2. Systemägarens ansvar

Kommunens förvaltningar och bolag är systemägare för sina respektive verksamhetssystem, men nyttjar också system som tillhandahållas av andra verksamheter. Det kan handla om övergripande centrala system men också mer verksamhetsspecifika system.
Med systemägarskapet följer ett ansvar att:

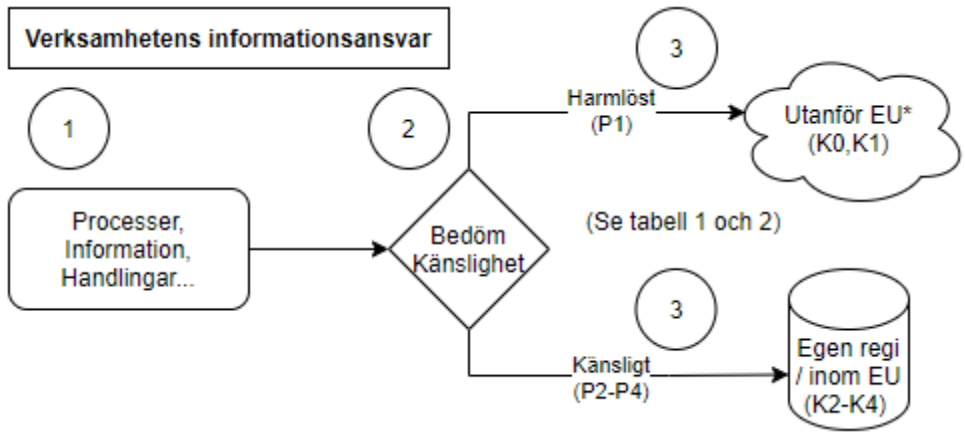
- Säkerställa systemförvaltning
- Göra risk- och sårbarhetsanalyser av systemfunktionaliteten
- Utforma regelverk för systemlösningen
- Säkerställa överenskommelse med verksamhet
- Arbeta med ständiga förbättringar

3. Vägledning för verksamhetens informationsbedömning i väntan på att LIS införs

Verksamheten ska bedöma känsligheten i sin information.
Innan man gjort denna bedömning så ska man inte lagra informationen i externa drifttjänster.
Det är resultatet från bedömningen som avgör vilka lagringsalternativ som är möjliga.

Själva bedömningen går till så här:

1. Identifiera verksamhetens processer och tillhörande information/handlingar.
2. Bedöm informationens känslighet.
   Detta kan genomföras med hjälp av SKR:s verktyg ”Klassa”. Kategorisera informationens innehåll mot lämplig känslighetsnivå. Se tabell 1.
3. Välj lämpligt lagringsalternativ. Se tabell 2.



* M365 bedöms i nuläget som tjänst med hantering och lagring utanför EU/EES, se tabell 2.

Tabell 1 – Informationens bedömda känslighetsnivå

Skyddsnivå	**Sekretess**	**Personuppgifter**	**Konsekvensnivåer i KLASSA**
Öppen	-	-	försumbar skada (K0)
Låg	-	Interna harmlösa (P1)	måttlig skada (K1)
Medel	Svag (S1)	Externa harmlösa (P2)	betydande skada (K2)
Hög	Stark (S2), Absolut (S3)	Extra skyddsvärda (P3) Känsliga (P4)	allvarlig skada (K3)
Mycket hög	Rikets säkerhet (S4)	Rikets säkerhet	synnerligen allvarlig skada (K4)

Tabell 2 – Drift och lagringsalternativ utifrån informationens känslighet

Bedömd status på digital information (skyddsnivå)	**Ej klassad** (Okänd)	**Känslig** (Medel – Mycket hög)	**Harmlös** (Öppen - Låg)
Möjliga drifts- och lagringsalternativ	• Egen regi	**Medel - Hög** • Egen regi • Molntjänst – leverantör med säte i EU/EES** **Mycket hög** • Enligt separat rutin	• Egen regi • Molntjänst – leverantör med säte i EU/EES** • Molntjänst – leverantör med säte utanför EU/EES

** Leverantör med säte i EU/EES som kan garantera att information inte lagras, hanteras eller kontrolleras utanför EU/EES.

STÖD FÖR INFORMATIONSBEDÖMNING I TABELL 1 OCH KONSEKVENSER ENLIGT KLASSA

EXEMPEL SEKRETESS

Sekretess delas in i svag, stark och absolut sekretess samt sekretess för rikets säkerhet

S1 svag sekretess: offentlighet gäller i första hand, men uppgiften kan sekretessbeläggas om det kan antas att den enskilde eller någon närstående kan lida skada (ekonomiskt) eller men (intrång i den personliga integriteten) om uppgiften röjs. Svag sekretess gäller t ex inom personaladministrationen och inom skolans elevstödjande verksamhet (ej utförd av psykolog, kurator el specialpedagog)

S2 stark sekretess: sekretess gäller i första hand men uppgiften kan bli offentlig om det står klart att den kan röjas utan att den enskilde eller någon närstående lider skada eller men. Stark sekretess gäller t ex inom socialförvaltningen och omvårdnadsförvaltningen

S3 absolut sekretess: uppgifterna lämnas inte ut, ingen sekretessprövning sker. Uppgifterna enbart tillgängliga för de som behöver uppgifterna för att utföra sitt arbete. Absolut sekretess gäller t ex pågående upphandlingsärenden

S4 rikets säkerhet: skydd av hemliga uppgifter och personuppgifter som rör rikets säkerhet

EXEMPEL PERSONUPPGIFTER

Personuppgifter delas in i harmlösa, känsliga och extra skyddsvärda.

P1 interna harmlösa personuppgifter: anställdas, elevers och förtroendevaldas arbetsrelaterade personuppgifter, t ex namn, e-postadress, telefonnummer, befattning (ej privata, känsliga och extra skyddsvärda, t ex personnummer)

P2 externa harmlösa personuppgifter: allmänhetens, kunders, leverantörers, samarbetspartners personuppgifter, t ex namn, adress, telefonnummer, e-postadress; OBS! anställdas privata kontaktuppgifter

P3 extra skyddsvärda personuppgifter: personnummer, samordningsnummer, skyddad identitet, lagöverträdelser, ekonomiska förhållanden, omdömen och värderingar, provresultat och tester

P4 känsliga personuppgifter: ras eller etniskt ursprung, politiska åsikter (t ex förtroendevaldas privata kontaktuppgifter), religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, sexualliv eller sexuell läggning, genetiska uppgifter (t ex dna-analys), biometriska uppgifter som entydigt identifierar en person (t ex fingeravtryck)

KONSEKVENSNIVÅER I KLASSA

Klassa är SKR:s verktyg för informationsklassning av information och system.
Beskrivning av vilka konsekvenser (vilken skada) det får om informationen kommer i orätta händer:

K0 Försumbar skada (0): Ingen eller endast försumbar skada för individer, andra organisationer eller på samhällsviktiga funktioner.

K1 Måttlig skada (1): Enskilda individer eller andra organisationer kan notera störningen och uppleva lindriga besvär. Ingen skada på samhällsviktiga funktioner.

K2 Betydande skada (2): Andra organisationer kan påverkas ekonomiskt eller behöver vidta extraordinära åtgärder. Enskilda individer kan uppleva stora besvär eller stor ekonomisk påverkan. Samhällsviktiga funktioner påverkas troligen inte.

K3 Allvarlig skada (3): Samhällsviktiga funktioner påverkas. Individers liv och hälsa äventyras. Det blir omöjligt eller nästa omöjligt att bedriva verksamhet.

K4 Synnerligen allvarlig skada (4): Hot mot rikets säkerhet. Oöverskådliga konsekvenser med omfattande vara för liv och hälsa. Sabotage, brott som kan hota rikets säkerhet samt terroristbrott