Vänersborgs kommun

Riktlinje informationssäkerhet

Antagen av Kommunfullmäktige 2021-03-25

Innehållsförteckning

Dokumenttyp	**Dokumentnamn**	**Antagen**	**Antagen av**
Riktlinje	Riktlinje informationssäkerhet	2021-03-25	Kommunfullmäktige
Dokumentägare	**Dokumentansvarig**	**Reviderad**	**Giltighet**
Kommunstyrelsen	Informationssäkerhetsspecialist		Tillsvidare

Dokumentinformation	**Diarienummer**
Övergripande riktlinjer för informationssäkerhetsarbete	KS 2020/205

Ämnesområde	**Intranät**	**Hemsida**
Säkerhet	☒	☒

Andra styrande dokument som omnämns

Dataskyddsförordningen, även kallad GDPR (Regulation (EU) 2016/679 (General Data Protection Regulation)), Säkerhetsskyddslagen (SFS 2018:585)

Inledning

Hantering av information är grunden för i princip allt arbete i kommunens verksamheter. Genom ett systematiskt arbete med informationssäkerhet kan kommunen öka kvaliteten i sina verksamheter och skapa ett gott förtroende för kommunen.

Korrekt information ska finnas tillgänglig bara för behöriga på ett spårbart sätt när det behövs.

- Genom klassning av informationstillgångar definieras informationens behov av tillgänglighetsstyrning.
- Genom tillämpning av inloggningsautentisering säkerställer organisationen användarens behörig till information.
- Genom spårbarhet i systemlösningar appliceras möjligheten att spåra ändringar av information för de verksamheter som har dessa behov.

Informationssäkerhetsarbetet är väl kommunicerat till verksamheten.

- Genom utbildningsinsatser säkerställs att alla medarbetare erhåller kunskap om kommunens regelverk för informationssäkerhet.
- Verksamhetsspecifika anvisningar anger särskilda förhållningssätt till informationssäkerhet kopplad till verksamhetsområde.

Informationssäkerhetsarbetet sker systematiskt enligt SS-ISO/IEC 27000.

- Ett ledningsstöd för informationssäkerhetsarbetet (LIS) ska skapa ett ramverk för ett kontinuerligt informationssäkerhetsarbete inom hela organisationen.

Omfattning

Riktlinjerna innehåller en översiktlig beskrivning om hur en god informationssäkerhet ska uppnås vid all hantering av information inom Vänersborgs kommuns nämnder, samtliga verksamheter och bolag.

Principer för informationssäkerhet

Att skydda information handlar om att skapa och upprätthålla rutiner utifrån fyra principer:

1. Tillgänglighet - Att informationen alltid är åtkomlig och användbar av behörig när den behövs.
2. Riktighet – Att man kan lita på att informationen är korrekt, aktuell och fullständig och inte manipulerad eller förstörd.

3. Konfidentialitet – Att endast behörig person får ta del av informationen.
4. Spårbarhet – Att det är möjligt att fastställa vem som gjort vad gällande informationsförändring och att kunna verifiera orsaken till en händelse. Appliceras för verksamheter i behov av spårbarhet.

Samband mellan IT-säkerhet och Informationssäkerhet

Informationssäkerhet består av att skapa och upprätthålla lämpligt skydd i information oavsett dess form, oberoende av om den finns i IT-system, papper eller i form av tal. Medan IT-säkerhet fokuserar på säkerhet i IT-miljöer så handlar informationssäkerhet om hur all information ska skyddas oavsett hur den hanteras.

Krav som ställs gällande klassning av informationssäkerhet kan påverka krav som ställs på IT-säkerhet.

Styrning och ansvar för informationssäkerheten

Kommunstyrelsen leder, samordnar och granskar kommunens arbete med informationssäkerhet.

Varje nämnd och styrelse är ansvarig för att upprätthålla informationssäkerheten inom sitt verksamhetsområde och i förekommande fall även för tillhörande externa organisatoriska funktioner om de saknar eget organisationsnummer.

Kommunstyrelsen, nämnder och kommunala bolag är även personuppgiftsansvariga inom respektive verksamhetsområde. Som personuppgiftsansvarig har de det yttersta ansvaret för att all behandling av personuppgifter sker i enlighet med Dataskyddsförordningen, även kallad GDPR (Regulation (EU) 2016/679 (General Data Protection Regulation)).

Organisation för informationssäkerhetsarbetet

Kommundirektören ansvarar för förvaltningarnas organisation av informationssäkerhetsarbetet. Denna preciseras i Anvisningar utifrån dessa Riktlinjer.

Kommunen har även ett utsett dataskyddsombud för alla nämnder vilket är ett krav enligt dataskyddsförordningen. Dataskyddsombudet har en oberoende roll som innebär kontroll av att Dataskyddsförordningen, efterlevs inom organisationen genom exempelvis granskning och informationsinsatser.

Informationsklassning

Informationsklassning är en grundläggande del i arbetet med systematisk informationssäkerhet. Genom att klassificera information utifrån grundprinciperna konfidentialitet, riktighet, tillgänglighet och spårbarhet får organisationen en förståelse för det skydd som krävs och måste anpassas för olika informationsmängder.

Klassning av information ska ske utifrån rättsliga krav, men även interna krav på informationens värde och betydelse för verksamheten ska vägas in.

Informationsklassning utifrån Säkerhetsskyddslagens (SFS 2018:585) kriterier har betydligt högre skyddskrav än den informationsklassning som avses i denna riktlinje.

Vänersborgs kommuns modell för informationsklassning

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
4. Höga skyddskrav	**Konfidentiell** Information som, om den sprids till obehöriga, kan medföra allvarlig negativ påverkan för Vänersborgs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är riktig och fullständig, kan medföra allvarlig negativ påverkan för Vänersborgs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är tillgänglig, kan medföra allvarlig negativ påverkan för Vänersborgs kommun, externa aktörer eller enskilda individer.	Information eller aktivitet som, om den inte är spårbar medför allvarlig konsekvens för Vänersborgs kommun, externa aktörer eller enskilda individer
3. Förhöjda skyddskrav	**Känslig** information som, om den sprids till obehöriga, kan medföra betydande negativ påverkan för Vänersborgs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är riktig och fullständig, kan medföra betydande negativ påverkan för Vänersborgs kommun, externa aktörer eller enskilda individer	Information som, om den ej är tillgänglig, kan medföra betydande negativ påverkan för Vänersborgs kommun, externa aktörer eller enskilda individer.	Information som, om den inte är spårbar medför betydande konsekvens för Vänersborgs kommun, externa aktörer eller enskilda individer.

2. Normala skyddskrav	**Harmlös** information som, om den sprids till obehöriga, kan medföra måttlig negativ påverkan för Vänersborgs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverka för Vänersborgs kommun, externa aktörer eller enskilda individer.	Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan för Vänersborgs kommun, externa aktörer eller enskilda individer.	Information som, om den inte är spårbar medför måttlig konsekvens för Vänersborgs kommun, externa aktörer eller enskilda individer.
1. **Låga skyddskrav**	**Öppen** information kan i regel spridas fritt inom och utom Vänersborgs kommun	Normala skyddskrav avseende informationens riktighet och tillgänglighet.	Normala skyddskrav avseende informationens riktighet och tillgänglighet.	Information som, om den inte är spårbar medför ingen, lindrig eller försumbar konsekvens för Vänersborgs kommun, externa aktörer eller enskilda individer.

Beskrivning av informationsklasser

- **Konfidentiell information** utgörs av uppgifter som berörs av sekretess eller av andra bärande skäl som bedöms hållas konfidentiell. Konfidentiell information får endast vara tillgänglig för enskilda medarbetare som har ett direkt behov av att hantera informationen.
- **Känslig information** utgörs av sådana uppgifter som har ett något högre skyddsvärde än den som klassas som harmlös, men som samtidigt inte riktigt når upp till ett skyddsbehov som finns för information som klassad som konfidentiell. Vad som skiljer den från **harmlös information** är att det ställs högre krav på behörighet så att endast de medarbetare som har ett faktiskt och direkt behov av informationen får ha tillgång till den.
- **Harmlös information** kännetecknas av att den består av harmlösa personuppgifter så som namn, telefonnummer, adress, e-postadress, fastighetsbeteckning, användar-id med mera. Intern information av detta slag kan normalt vara tillgänglig för en avdelning, enhet eller arbetsgrupp som kan ha behov av att hantera informationen.

- **Öppen information** utgörs främst av all den information som inte består av några personuppgifter alls eller andra uppgifter som bedöms vara helt okänsliga för vidare spridning. Öppen information har normalt inga krav på åtkomstbegränsning utan kan normalt spridas fritt inom Vänersborgs kommun.

Anvisningar

Kommundirektören har rätt att anta anvisningar med stöd av denna riktlinje.