Upplands Väsby kommun

Styrdokument

Datum:
2022-10-27

Diarienummer:
KS/2021:396

Informationssäkerhetspolicy för Upplands Väsby kommun

Kategori	Styrdokumentsuppgifter
Nivå	Kommungemensamt
Antagen	Kommunfullmäktige den 12 december 2022
Ikraftträdande	Den 1 januari 2023
Giltig till och med	Tills vidare
Ansvarig ägare	Kommundirektör

Informationssäkerhetspolicy för Upplands Väsby kommun

Versionshistorik

Versionsnummer	Datum	Författare	Version och ändringar
1.0 – KS/2006:148	2007-12-17	Per-Ola Lindahl	Första utgåva – giltig t.o.m. 2012-12-31
2.0 – KS/2011:206	2011-09-12	Per-Ola Lindahl	Andra utgåva (reviderad) – giltig t.o.m. 2015-12-31
3.0 – KS/2015:315	2016-11-21	Per-Ola Lindahl	Tredje utgåva (reviderad) – giltig t.o.m. 2017-12-31
4.0 – KS/2021:396	2022-12-12	Niza Löfdahl	Fjärde utgåva (reviderad) - ändring av innehållet.

1. Informationssäkerhetspolicys roll och omfattning

Informationssäkerhetsarbetet i kommunen är systematiskt och riskbaserat. Arbetet ska stödjas av ett ledningssystem för informationssäkerhet och Myndigheten för samhällsskydd och beredskaps (MSB) metodstöd. Kommunens informationssäkerhetsarbete är en grundförutsättning för att möjliggöra framtida samverkansmöjligheter samt fortsatt digitaliseringsarbete och arbete med e-förvaltning.

Denna informationssäkerhetspolicy fastställs av kommunfullmäktige och anger kommunens grundläggande synsätt och viljeinriktning på en övergripande nivå i informationssäkerhetsarbetet. Policyn konkretiseras av kommunens gemensamma riktlinjer för informationssäkerhet som ska fastställas av kommunstyrelsen. Denna policy är medieoberoende och teknikneutral.

Informationssäkerhetspolicyn gäller för informationssäkerhetsarbete i alla kommunens organ såväl politiska organ som tjänsteorgan. Kommunens revisorer, bolag och stiftelser omfattas också av denna policy. Beslut om tillämpning av policyn ska skrivas in i bolagens ägardirektiv eller motsvarande.

Företag, uppdragstagare, tredje man eller liknade som arbetar på uppdrag av Upplands Väsby kommun och som använder sig av kommunens information omfattas också av denna informationssäkerhetspolicy. Tillämpningen ska regleras genom avtal.

2. Definitioner

I bilaga 1 återfinns förklaringar av ord och begrepp enligt policyn.

3. Målsättning för informationssäkerhetsarbete

Kommunens målsättning är att informationssäkerhetsarbetet:

- möjliggör kommunens arbete med god informationsförvaltning, ökande digitalisering och e-förvaltning. På så sätt får medborgare tillgång till kommunens samhällsservice

enklare, snabbare och säkrare. Informationssäkerhetsarbetet tillgodoser också rätten av att ta del av organisationens allmänna handlingar,

- främjar medborgarens yttrandefrihet och delaktighet,
- säkerställer att fysiska personers rättigheter, friheter och integritet skyddas,
- bidrar till att organisationen har en robust och effektiv informationsförsörjning,
- bidrar till att informationshanteringen är säker och tillförlitlig,
- möjliggör digital kommunikation i kommunens ärendehanteringsprocess,
- möjliggör tillgänglighet av organisationens information och data i den utsträckning som är skälig med hänsyn till informationens skyddsnivå, och
- ska bedrivas på sådant sätt att legala krav och kommunens egna krav, samt krav enligt avtal gällande informationssäkerhet uppfylls.

4. Principer för informationssäkerhetsarbetet

Upplands Väsby kommuns grundläggande principer gällande för informationssäkerhetsarbete består av:

- informationssäkerhetsarbetet ska vara okomplicerat, praktiskt, pedagogiskt och ska kunna bedrivas systematiskt och kontinuerligt,
- kommunens arbete med informationssäkerhet och informationsförvaltning enligt Reglemente för hantering av information i Upplands Väsby kommun bedrivs gemensamt och kontinuerligt,
- verksamheternas informationsförvaltning bedriver sitt lokala informationssäkerhetsarbete, med stöd av arkivmyndigheten,
- varje verksamhet ska värna en informationssäkerhetskultur inom sin verksamhet,
- samverkan inom kommunens verksamheter och mer externa myndigheter/aktörer sker aktiv och effektiv,
- leverantörsuppföljning är prioriterat och sker kontinuerligt,
- riskhantering, incidenthantering och kontinuitethantering är prioriterat samt ska utvärderas löpande och utvecklas,
- informationssäkerhetsarbetet ska utvärderas och utvecklas löpande på alla nivåer, och
- informationssäkerhetsarbetet ska vara väl kommunicerat med alla anställda och förtroendevalda.

5. Upplands Väsby kommuns informationssäkerhet

5.1. Informationssäkerhetens syfte och dess säkerhetsaspekter

Syfte med informationssäkerhet är att kommunens information ska:

- skyddas från obehörig åtkomst (**konfidentialitet**),
- skyddas från förvanskning och förstörelse, samt att informationen är korrekt och relevant för den process som den ska stödja (**riktighet**), och

- vara lättåtkomlig och sökbar för behörig person i en bestämd utsträckning och tid (**tillgänglighet)**.

Kommunens informationssäkerhetsarbete innebär att ta fram lämpliga åtgärder och lämplig säkerhetsnivå i enlighet med de tre säkerhetsaspekterna som nämns ovan. Dessa tre säkerhetsaspekter ska användas vid informationsklassning. Ett klassningsobjekt är det som är föremål för informationsklassningen.

- Spårbarhet är en annan säkerhetsaspekt som också omfattas i informationssäkerhetsarbetet. Spårbarhet i det här sammanhanget innebär att i efterhand kunna identifiera en specifik händelse eller aktivitet (av vem, vad, när och vilken konsekvens som har/kan ha uppstått/uppstå) . På så sätt kan information som har ändrats eller förlorats återskapas. Denna säkerhetsaspekt ska inte användas för att utvärdera information vid informationsklassning.

5.2. Informationssäkerhetens komponenter

Upplands Väsby kommuns informationssäkerhet består av sju komponenter såsom: organisatorisk informationssäkerhet, fysisk säkerhet, personlig säkerhet, digital säkerhet, lagar och förordningar, kommunens interna styrdokument avseende informationssäkerhet, samt riskbaserat förhållningssätt till informationssäkerhet och informationssäkerhetskultur. Komponenterna förhåller sig till och är beroende av varandra och kan beskrivas enligt följande:

1. **Organisatorisk informationssäkerhet** utgör i detta sammanhang grunden för hur kommunens ledning styr arbetet med fysisk säkerhet, personlig säker och digital säkerhet som ligger inom ramen för informationssäkerhetsarbetet. Den organisatoriska informationssäkerheten delas upp i övergripande, samordnande och lokal nivå.
    - Organisatorisk informationssäkerhet på övergripande nivå styrs av kommunfullmäktige som fattar beslut om kommunens övergripande styrdokument och budget.
    - Kommunstyrelsen har ett samordningsansvar och ska säkerställa att fullmäktiges beslut verkställs, genom att gemensamma riktlinjer, metoder och arbetssätt för informationssäkerhetsarbetet finns tillgängliga och är aktuella.
    - Organisatorisk informationssäkerhet på lokal nivå styrs av nämnderna, kommunens revisorer, bolag och stiftelser som fattar beslut om styrdokument, budget, samarbetsformer och rutiner inom sin verksamhet.

2. **Fysisk informationssäkerhet** omfattar i det här sammanhanget säkerhet för lokaler där information bevaras/hanteras/kommuniceras, it-utrymme, utrusningar och datamedium som hanterar/bevarar information.
3. **Personlig informationssäkerhet** i det här sammanhanget innebär hur kommunens anställda och förtroendevalda hanterar skyddsvärd information ur ett säkerhetsperspektiv.
4. **Digital informationssäkerhet** enligt policyn består av it-säkerhet, cybersäkerhet och säkerhet för digital kommunikation.
5. **Lagar och förordningar** som ställer krav på informationssäkerheten utgör grunden för informationssäkerhetsarbetet inom organisationen.
6. **Kommunens interna styrdokument** som består av informationssäkerhetspolicy, riktlinjer för informationssäkerhet samt riktlinjer för hantering av personuppgifter och hantering av personer med skyddade personuppgifter. Dessa är kommunens gemensamma styrdokument. Kommunstyrelsen ansvarar för att säkerställa att styrdokumenten finns tillgängliga och är aktuella.
7. **Riskbaserat förhållningsätt till informationssäkerhet och informationssäkerhetskultur**.
    - **Riskbaserat förhållningssätt** i det här sammanhanget innebär att åtgärder för att motverka informationssäkerhetsincidenter, baseras på de risker som är kopplade till hanteringen av kommunens skyddsvärda information. Befintliga resurser används på ett effektivt sätt och i enlighet med ledningens prioriteringar.
    - **Informationssäkerhetskultur** är ett samlingsbegrepp för anställdas och förtroendevaldas gemensamma grundläggande värderingar, antaganden och attityd ifråga om informationssäkerhet.

5.3. Upplands Väsby kommuns ledningssystem för informationssäkerhet

Upplands Väsby kommuns ledningssystem för informationssäkerhet är en integrerad del av kommunens ledningssystem.

Definitioner enligt kapitel 2

antagonist	person, grupp av personer eller organisatorisk enhet som har för avsikt att orsaka negativa effekter eller skador på en studerad verksamhet, t.ex. på samhällsviktig verksamhet eller utrustning[1],
cybersäkerhet	metoder och verktyg som används för att skydda organisationens nätverk- och informationssystem, samt användare av dessa system och andra berörda personer mot antagonistiska hot/angrepp,
informationsklassning	värdering av kommunens informationstillgångar utifrån säkerhetsaspekterna: **konfidentialitet**, **riktighet** och **tillgänglighet**. Informationstillgångarna klassas i olika konsekvensnivåer,
information	verksamhetsinformation som består av alla former av information och även kunskap som organisationens enskilda medarbetare och förtroendevald besitter,
informationstillgång	skyddsobjekt som består av information (skyddsvärd information) och resurs som hanterar/förvaltar/förvarar informationen. Informationen är den primära delen av tillgången. Resursen avser såväl manuell som it-baserad informationshantering. Telekom och kommunikationssystem räkas också som resurs,
informationssystem	applikationer, tjänster eller andra komponenter som hanterar information. I detta begrepp ingår också nätverk och infrastruktur[2],
informationsmängd	en gruppering av information i form av t.ex. dokument, register, databas som innehåller flera informationstyper,
informationstyp	ett visst slag av information som kan finnas lokal inom verksamheten eller hela organisationen t.ex. personuppgifter,
it-säkerhet	metoder och verktyg som använda för att kvalitetssäkra och skydda kommunens digitala

[1] MSB:s skrift ”Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritiska infrastruktur”. MSB 1178 – februari 2018.
[2] Myndighet för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter, MSBFS 2020:7

	information och it-baserade informationssystem utifrån tre aspekterna: konfidentialitet, riktighet och tillgänglighet. Det handlar om att skydda informationen och informationssystem från t.ex. felbedömningar, handhavandefel, brister i hårdvara och applikationer, samt elektroniska störningar som inte är orsakad av antagonister,
klassningsobjekt	informationstillgångar som ska klassas vid ett specifikt tillfälle. Ett klassningsobjekt kan vara enbart information eller information och resurs som hanterar informationen. En nämnd (arkivbildare) kan också klassas om ett klassningsobjekt i vissa sammanhang,
organisation	Upplands Väsby kommunkoncern,
skyddsvärd information	värdefull information som behöver skyddas. T.ex. information om hur organisationen använda IT-system i en specifik verksamhet, uppgifter om enskilda medborgare, organisationens risk- och sårbarhetsanalys, vissa ritningar, vissa uppgifter som kopplar till organisationens nyckelpersoner, samt information som berör hälso- och sjukvård, dricksvatten, energiförsörjning etc. Informationsklassning är en metod som används för att identifiera skyddsbehovet för en viss informationsmängd,
säkerhet för digital kommunikation	att säkra informationsöverföring i digitala kommunikationskanaler både inom kommunens interna och med externa enheter, och
tjänsteorgan	enligt policyn är kontoren.
verksamhet	enligt policyn är kommunens styrelse, nämnder, bolag, stiftelser och revisorer.