Uppsala kommun

Kommunstyrelsens arbetsutskott
Protokollsutdrag

Datum:
2020-01-13

§ 3

Riktlinje för informationssäkerhet

KSN-2019-03509

Beslut

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta

1. **att** fastställa förslag till riktlinje för informationssäkerhet i ärendets **bilaga 1**.

Beslutsgång

Ordförande ställer föreliggande förslag mot avslag och finner att arbetsutskottet bifaller detsamma.

Sammanfattning

I handlingsplanen för ett tryggare och säkrare Uppsala ingår en åtgärd att ta fram och implementera styrdokument för informationssäkerhet (åtgärd 63). Syftet med riktlinjen är att skapa förutsättningar för ett systematiskt och integrerat arbete med informationssäkerhet i Uppsala kommun.

Beslutsunderlag

- Tjänsteskrivelse daterad 19 december 2019
- Bilaga 1, Förslag till riktlinje för informationssäkerhet daterad 17 december 2019.

Uppsala kommun

Kommunledningskontoret
Tjänsteskrivelse till kommunstyrelsen

Datum:
2019-12-17

Diarienummer:
KSN-2019-03509

Handläggare:
Robert Reineck

Riktlinje för informationssäkerhet

Förslag till beslut

Kommunstyrelsen beslutar

1. **att** fastställa förslag till riktlinje för informationssäkerhet i ärendets **bilaga 1**.

Ärendet

I handlingsplanen för ett tryggare och säkrare Uppsala ingår en åtgärd att ta fram och implementera styrdokument för informationssäkerhet (åtgärd 63). Syftet med riktlinjen är att skapa förutsättningar för ett systematiskt och integrerat arbete med informationssäkerhet i Uppsala kommun.

Beredning

Ärendet har beretts av kommunledningskontoret. Övriga förvaltningar och de kommunala bolagen har erbjudits möjlighet att medverka i beredningen.

Ärendet har inga konsekvenser sett ur barn-, jämställdhets- eller näringslivsperspektiven.

Föredragning

Syftet med riktlinjen är att skapa förutsättningar för ett systematiskt och integrerat arbete med informationssäkerhet och hur detta ska bedrivas i nämnder och bolagsstyrelser i Uppsala kommun.

Informationssäkerhetsarbetet ska bidra till att kommunkoncernen kan genomföra verksamheten utan störningar samt skapa en motståndskraft och förmåga till återhämtning i de fall störningar ändå inträffar.

Information är en nödvändig resurs för en väl fungerande offentlig verksamhet.

Postadress: Uppsala kommun, kommunledningskontoret, 753 75 Uppsala
Besöksadress: Stationsgatan 12
Telefon: 018-727 00 00 (växel)
E-post: kommunledningskontoret@uppsala.se
www.uppsala.se

Därför måste kommunkoncernen skydda informationen så:

- att den alltid finns när den behövs (tillgänglighet)
- att den går att lita på, att den är korrekt och inte heller manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den (konfidentialitet)

Riktlinjen utgår från policyn för trygghet och säkerhet och policyn för IT-utveckling och digitalisering.

Ekonomiska konsekvenser

Riktlinjen genomförs inom befintlig ram för kommunstyrelsen.

Beslutsunderlag

- Tjänsteskrivelse daterad 19 december 2019
- Bilaga 1, Förslag till riktlinje för informationssäkerhet daterad 17 december 2019.

Kommunledningskontoret

Joachim Danielsson
Stadsdirektör

Ola Hägglund
Stabsdirektör

Uppsala kommun

Normerande styrdokument

Beslutsfattare:
Kommunstyrelsen

Dokumentansvarig:
CIO

Datum:
2019-12-06

Diarienummer:
KSN-2019-03509

Riktlinje för informationssäkerhet

Policy

Riktlinje

Rutin

Vägledning

Innehåll

Inledning

Denna riktlinje uttrycker hur arbetet med informationssäkerhet ska bedrivas inom Uppsala kommun. Riktlinjen utgår från policyn för trygghet och säkerhet och policyn för IT-utveckling och digitalisering.

Syfte

Syftet med riktlinjen är att skapa förutsättningar för ett systematiskt och integrerat arbete med informationssäkerhet och hur detta tar sig uttryck inom hela kommunkoncernen, både nämnder och bolagsstyrelser inom Uppsala kommun.

Omfattning

Riktlinjen reglerar de områden som omfattas av ISO/IEC 27001, Ledningssystem för informationssäkerhet. Målgrupper är i första hand Uppsala kommuns nämnder och bolagsstyrelser, internrevision samt de som ansvarar för styrdokument inom områden där kontroller för informationssäkerhet bör integreras.

Bakgrund

Informationssäkerhetsarbetet ska bidra till att kommunkoncernen kan genomföra samtliga uppdrag utan störningar samt skapa en motståndskraft och förmåga till återhämtning i de fall störningar ändå inträffar.

Information är en nödvändig resurs för en väl fungerande offentlig verksamhet. Felaktigt hanterad eller frånvaro av information kan i värsta fall få katastrofala följder.

Därför måste kommunkoncernen skydda informationen så:

- att den alltid finns när den behövs (tillgänglighet)
- att den går att lita på, att den är korrekt och inte heller manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den (konfidentialitet)

Skyddet måste anpassas efter behovet och handlar om att hantera de risker som kan medföra att kommunkoncernen inte kan genomföra sitt uppdrag vilket i sin tur kan leda till att skada uppstår på skyddsvärden som människors liv och hälsa, samhällets funktionalitet, demokrati, rättssäkerhet och mänskliga fri- och rättigheter, ekonomi och miljö samt nationell suveränitet.

För att åstadkomma detta behövs ett systematiskt informationssäkerhetsarbete. Hur detta tar sig uttryck inom Uppsala kommun beskrivs i denna riktlinje.

Liksom i övrigt arbete med intern kontroll så bidrar informationssäkerhetsarbetet till att:

- verksamheten bedrivs ändamålsenligt och kostnadseffektivt,
- den finansiella rapporteringen och informationen om verksamheten är tillförlitlig, samt
- tillämpliga lagar, föreskrifter, policyer och riktlinjer efterlevs.

Arbetet med informationssäkerhet utgår från ISO/IEC 27001:2017, Ledningssystem för informationssäkerhet, samt ISO/IEC 27002:2017, Riktlinjer för informationssäkerhetsåtgärder, och syftar till att bevara förväntad konfidentialitet, riktighet och tillgänglighet med avseende på Uppsala kommuns informationstillgångar.

Definition och begrepp

Informationssäkerhet – Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.

Informationstillgång – Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (till exempel rykte och förtroende).

Lagbestämmelser och krav

Några av de mest framträdande kraven som berör informationssäkerhet står att finna i följande standarder och författningar.

Dataskyddsförordningen GDPR. Dataskyddsförordningen ställer krav på systematiskt informationssäkerhetsarbete med målet att skydda enskildas grundläggande rättigheter och friheter.

NIS-direktivet (Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen) och tillhörande nationell författning ska tillämpas inom valda delar av Uppsala kommuns verksamhet och uttrycker främst tillgänglighetskrav.

Tryckfrihetsförordningen (1949:105) och Offentlighets- och sekretesslagen (2009:400) (OSL) förutsätter ett systematiskt informationssäkerhetsarbete som tryggar offentlighetsprincipen och förhindrar röjandet av uppgifter som omfattas av sekretess.

Säkerhetsskyddslagen (2018:585). Information som är sekretessbelagd med hänsyn till Sveriges säkerhet ges ett särskilt skydd genom säkerhetsskyddslagen.

Arkivlagen (1990:782). En viktig uppgift med många kopplingar till informationssäkerhet är att över tid säkra riktigheten hos och skapa tillgänglighet till allmänna handlingar.

HSL-FS 2016:40 (Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården) föreskriver om informationssäkerhet i de delar av Uppsala kommun som omfattas av patientdatalagen (2008:355)

ISO/IEC 27001:2017, Ledningssystem för informationssäkerhet, samt ISO/IEC 27002:2017, Riktlinjer för informationssäkerhetsåtgärder. Dessa standarder beskriver ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Uppsala kommuns arbete med informationssäkerhet ska utgå från dessa standarder.

Ansvar

Ansvar och mandat med avseende på informationssäkerhet utgår från det ordinarie verksamhetsansvaret. Alla i kommunkoncernen är utifrån sitt eget uppdrag ansvarig för sin del av informationssäkerheten.

Kommunstyrelsen har ett övergripande ansvar för kommunkoncernens interna säkerhetsfrågor och koordinerar arbetet med informationssäkerhet samt verkar normerande, stödjande och uppföljande i relation till kommunkoncernens samtliga verksamheter.

Genomförande

Arbetet med informationssäkerhet ska:

- stärka kommunkoncernens förmåga att identifiera hot, sårbarheter och risker avseende de egna informationstillgångarna,
- skapa förutsättningar att reducera dessa risker till en acceptabel nivå,
- omfatta samtliga informationstillgångar,
- bedrivas systematiskt genom kontroll, uppföljning och styrning utgående från ledningssystemsstandarden SS-ISO/IEC 27001:2017, Ledningssystem för informationssäkerhet,
- integreras i verksamhetsnära styrdokument och arbetssätt samt utgå från krav enligt SS-ISO/IEC 27002:2017, Riktlinjer för informationssäkerhetsåtgärder,
- utformas så att rätt information är tillgänglig för rätt person vid rätt tillfälle,
- skapa en robust hantering av information genom att vara förebyggande och proaktiv samt ha förmågan att hantera de avvikelser och störningar som ändå kan inträffa,
- vara känt och tillämpat i hela organisationen och ge medarbetare förutsättningar för fortlöpande kompetenshöjning för ökat säkerhets-medvetande,
- utgå ifrån de råd och modeller som tas fram av myndigheter med särskilda uppdrag inom informationssäkerhetsområdet,
- bedrivas aktivt i samverkan med Sveriges kommuner och regioner (SKR), samt
- följas upp löpande och förbättras i takt med omgivningens förändrade förutsättningar.

Spridning

Kommunstyrelsen ansvarar för att informera om och implementera riktlinjen.

Nämnder och bolagsstyrelser ansvarar för att riktlinjen tillämpas i den egna verksamheten.

Uppföljning

Varje nämnd och bolagsstyrelse ska följa upp att riktlinjen följs. Kommunstyrelsen följer upp arbetet utifrån riktlinjen årligen i samband med årsredovisningen.

Relaterade dokument

- Policy för trygghet och säkerhet
- Policy för IT-utveckling och digitalisering
- Riktlinje för riskhantering