Älvkarleby kommun

Riktlinjer för informationssäkerhetsincidenter

Älvkarleby kommun

Antagen av: Kommunstyrelsen , 2024-03-05
Senast reviderad:
ÄKF-nummer:
Handläggare/författare: Joel Gordon Hultsjö , Informationssäkerhetssamordnare .

Älvkarleby kommun

Innehåll

Inledning

Denna riktlinje sätter ramarna för hur Älvkarleby kommun förebygger och hanterar informationssäkerhetsincidenter

Informationssäkerhetsincident: Ett samlingsnamn för IT-incidenter, personuppgiftsincidenter samt de incidenter som rör informationshanteringen och dess informationssäkerhet men som rör icke-digital information.

IT-incident: En oönskad och oplanerad IT-relaterad händelse som kan påverka säkerheten i Älvkarleby kommuns digitala informationshantering och som kan innebära en störning i dess förmåga att bedriva sin verksamhet. Exempel är störningar i driftsmiljöer, mjuk- eller hårdvara, informationsläckage, säkerhetsbrister i produkter, eller angrepp med skadlig kod.

Personuppgiftsincident: En incident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Det innebär även när det sker obehörigt röjande eller obehörig åtkomst till de personuppgifts som lagras, överförs och behandlas i kommunen.

Exempel på informationssäkerhetsincidenter

a) Oplanerade stopp i IT-system som påverkar merparten av kommunanställda, antingen i 4 timmar eller mer, eller återkommande
b) Oplanerade stopp i IT-system som påverkar viktiga delar av Älvkarleby kommuns kommunikation med omvärlden antingen i 4 timmar eller mer, eller återkommande
c) Känsliga, eller stora mängder, personuppgifter som läckts hittas på Internet
d) Upptäckt skadlig kod
e) Missbruk av inloggningsuppgifter för konto med högre behörighet
f) Otillåtet tillträde till server/nätutrustning etc. upptäcks
g) Nya phishing-meddelanden som innehåller Älvkarleby kommuns logga/inloggningsrutor etc.
h) Anställd raderar/ändrar medvetet data i syfte att förstöra data
i) Kommunens konton i sociala medier har använts av obehörig som spridit falsk information
j) Alvkarleby.se (eller andra domäner som kommunen äger) kapas
k) Utrustning med okrypterad och känslig information försvinner
l) Kommunens internetkoppling bryts oavsiktligt, i en timme eller mer
m) Förlorad redundans i central utrustning under längre tid än beräknat
n) Inrapporterade personuppgiftsincidenter
o) Dataförlust av tekniska orsaker
p) Förlust av sekretessbelagda dokument på grund av stöld eller felaktig hantering

Avgränsning

Dessa riktlinjer omfattar inte rapportering av IT-incidenter i informationssystem som har betydelse för säkerhetskänslig verksamhet enligt 2 kap. 4 § första stycket 2 säkerhetsskyddsförordningen (2021:955). Denna typ av incidenter regleras istället av Älvkarleby kommuns rutin för hantering av säkerhetsskyddsklassificerade uppgifter.

Ansvar

Medarbetare

Alla medarbetare har ansvar för att skyndsamt rapportera informationssäkerhetsincidenter de upptäcker. Rapportering bör ske enlig *Rutin för rapportering av informationssäkerhetsincidenter*.

Förvaltningschef

Förvaltningschef har ansvar för att minst en gång per år sammanställa antalet informationssäkerhetsincidenter som skett under det senaste året och redovisa det för nämnd. Denna statistik bör samlas in kontinuerligt och användas som grund för förvaltningens riskbedömningar och informationssäkerhetsarbete.

Avdelningschef- eller enhetschef

En medarbetares närmaste chef har ansvar för att hantera incidentanmälan och vidarebefordra den till rätt instans. Hur en incident ska hanteras och skickas inom organisationen, regleras i *Rutin för rapportering av informationssäkerhetsincidenter.*

Nämnder

Respektive nämnd har ansvar att ta fram tillämpningsrutiner för denna riktlinje och *Rutin för rapportering av informationssäkerhetsincidenter*

Kommunstyrelsens informationssäkerhetssamordnare

Kommunstyrelsens informationssäkerhetsfunktion är ett stöd för att förebygga informationssäkerhetsincidenter och för att göra bedömningar i samband med en incident åt förvaltningarna. Hen arbetar också strategiskt för att förebygga informationssäkerhetsincidenter på ett kommunövergripande plan.

Övergripande tillvägagångssätt vid rapportering

Medarbetare som upptäcker en informationssäkerhetsincident har i första hand ansvar för att skyndsamt minimera konsekvenserna av incidenten och rapportera det som ett ärende till IT-centrum om det är en IT-incident. Därefter har hen ansvar för att rapportera incidenten enligt *Rutin för rapportering av informationssäkerhetsincidenter*. För stöd i bedömningen av allvarligheten av incidenten och vilka åtgärder som bör tillämpas så kan kommunstyrelsens informationssäkerhetssamordnare eller nämndens dataskyddsombud kontaktas.

Rapportering vid utkontraktering

När en extern aktör hanterar Älvkarleby kommuns information ska de skyndsamt rapportera in IT-incidenter som berör informationen till sin kontaktperson på kommunen. Med extern aktör menas inhyrd konsult, tjänsteleverantör eller annan utkontraktering av IT-system. Denna skyldighet ska regleras i kommunens avtal med system- och tjänsteleverantörer.