NYKVARNS KOMMUN

FÖRFATTNINGSSAMLING
2020-06-17

Policy för informationssäkerhet

Antagen av kommunfullmäktige § 60, 2018-06-20, ansvarig: säkerhetsavdelningen
Reviderad: KF § 19, 2019-03-07, KF § 54, 2020-06-17, KS/2020:110

Innehållsförteckning

1. Inledning och bakgrund

Information är en av kommunens viktigaste tillgångar och hanteringen av information är en viktig del i arbetet. Att information hanteras på rätt sätt är av strategisk betydelse för medarbetare, medborgare och näringsliv. Med informationstillgångar avses all information som används i kommunens verksamhet, oavsett om den behandlas manuellt, digitalt eller automatiserat och oberoende av dess form eller miljö den förekommer i.

Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av vår verksamhet och alla de informationstillgångar som vi äger eller hanterar.

2. Informationssäkerhet

Informationssäkerhet inbegriper tillämpning och hantering av lämpliga säkerhetsåtgärder som tar ett brett spektrum av hot i beaktande, i syfte att säkerställa organisationens verksamhet och dess kontinuitet samt minimera konsekvenserna av informationssäkerhetsincidenter.

Med informationssäkerhet avses att följande krav säkerställs och upprätthålls:

- Konfidentialitet - att åtkomst till informationen kan begränsas (benämndes tidigare sekretess)
- Riktighet - att informationen ska vara tillförlitlig, korrekt och fullständig
- Tillgänglighet - att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet
- Spårbarhet - att alla aktiviteter som rör informationen kan spåras, det vill säga vem som gjort vad och när det gjorts.

3. Syfte

Grundläggande för systematisk, säker och effektiv informationshantering är att informationen behöver vara kartlagd, värderad, klassificerad och att ansvaret för informationen är fastställt.

Arbetet ska bidra till att upprätta en informationssäkerhetskultur inom organisationen. Informationssäkerhetskultur handlar om en organisations gemensamma sätt att tänka och agera i förhållande till risk och informationssäkerhet, dvs. hur en organisation prioriterar och faktiskt arbetar med risker och informationssäkerhet kopplat till sin verksamhet.

Kommunens informationssäkerhetsarbete syftar till:

- att informationssäkerhet är en naturlig och integrerad del i verksamheten,
- att kunskap finns om hur informationssäkerheten säkerställs,
- att alla informationstillgångar klassificeras,
- att hotbilden mot informationstillgångar fortlöpande analyseras,
- att händelser som kan leda till negativa konsekvenser förebyggs och åtgärdas,
- att förmågan att hantera omfattande störningar fortlöpande analyseras och upprätthålls.

4. Lagar och regelverk

Nykvarns kommuns informationssäkerhetsarbete ska vara systematiskt och strukturerat, arbetssättet bygger på den svenska och internationella standarden ledningssystem för informationssäkerhet (LIS). LIS bygger på etablerade standarder, ISO standard 27001 och Myndigheten för samhällsskydd och beredskaps metodstöd för informationssäkerhetsarbete.

Vårt arbete med informationssäkerhet utgår från lagar, förordningar och föreskrifter som bland annat offentlighets- och sekretesslagen, dataskyddsförordningen och lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

Dataskyddsförordningens krav på hantering av personuppgifter ska vara integrerat med det systematiska informationssäkerhetsarbetet.

5. Avgränsning

Policyn för informationssäkerhet gäller för alla informationstillgångar i alla verksamheter inom Nykvarns kommun samt för kommunens helägda bolag. Policyn ska vara en integrerad del av upphandling och avtal med externa parter som kan komma att hantera kommunens information.

6. Målgrupp

Policy för informationssäkerhet gäller för samtliga anställda i Nykvarns kommun och kommunens bolag.

7. Informationssäkerhetsutbildning

All berörd personal och förtroendevalda ska regelbundet få den utbildning som behövs för att informationssäkerheten ska kunna upprätthållas.

8. Informationsklassning

Information som hanteras i kommunen ska klassificeras enligt Sveriges kommuner och regioners självskattningsverktyg, KLASSA. Informationssäkerhetsansvarig ansvarar för informationsklassning.

9. Skyddsåtgärder

Nykvarns kommun ska beskriva och införa organisatoriska, administrativa och tekniska skyddsåtgärder för att nödvändig skyddsnivå uppnås.

10. Kontinuitetshantering

Kontinuitetshantering handlar om att planera för att kunna upprätthålla verksamhet och processer för att skapa en nödvändig förmåga till funktionalitet, oavsett händelse. I syfte att uppfylla policy för informationssäkerhet krävs att organisationen har kontinuitetplaner för att säkra tillgången till information vid händelser som bland annat el-avbrott och IT-störningar.

11. Revidering och Uppföljning

Kommunens informationssäkerhetsarbete är integrerad i kommunens styrmodell och följs upp på kontorsnivå och för helägda kommunala bolagen som rapporterar löpande om sitt informationssäkerhetsarbete till Informationssäkerhetsansvarig.

Policy för revideras vid behov och varje mandatperiod. Säkerhetschefen ansvarar för att policyn för informationssäkerhet följs upp och uppdateras.

12. Roller och ansvar

12.1. Politisk organisation

12.1.1. Kommunfullmäktige

Kommunfullmäktige fastställer i denna policy hur informationssäkerhetsarbetet ska bedrivas i Nykvarns kommun.

12.1.2. Kommunstyrelsen, nämnderna och helägda bolag

Kommunstyrelsen, nämnderna och helägda bolag har det övergripande ansvaret för allt informationssäkerhetsarbete och informationstillgångarna i respektive nämnd/bolag. Kommunstyrelsen, nämnderna och bolagsstyrelser är personuppgiftsansvariga och ansvarar för behandling av personuppgifter. Kommunstyrelsen, nämnderna och bolagsstyrelser ska utse dataskyddsombud som kontrollerar att personuppgifter behandlas på ett korrekt sätt i verksamheten.

12.2. Informationsägare och informationsförvaltare

12.2.1. Informationsägare

Ansvaret för respektive informationstillgång följer verksamhetsansvaret. Informationsägaren avgör vilken information som får hanteras, hur den hanteras och av vem.

12.2.2. Informationsförvaltare

Informationsförvaltaren har det dagliga ansvaret för att upprätthålla informationssäkerheten i ett förvaltningsobjekt. Informationsförvaltaren ska säkerställa att informationssäkerheten följer kraven på konfidentialitet, riktighet, tillgänglighet och spårbarhet.

12.3. Systemägare

Systemägaren har övergripande ansvar för systemet och dess funktionalitet skyddar klassad information, men även förvaltning, underhåll, utveckling och användarbehörigheter. Systemägaren ansvarar för att utse systemförvaltare.

12.4. Informationssäkerhetsansvarig

Informationssäkerhetsansvarig har det övergripande ansvaret att leda, samordna och utveckla kommunens informationssäkerhetsarbete och årligen planera för prioriteringar och aktiviteter.

12.5. Digitaliserings och IT ansvarig

Digitaliserings- och IT ansvarig har det övergripande ansvaret att leda, utveckla och samordna kommunens IT-säkerhetsarbete och kontinuitetsplanering av kommunövergripande IT-system.

12.6. Dataskyddsombud

Dataskyddsombudet utövar tillsyn över kommunens behandling av personuppgifter, lämnar råd och stöd i dataskyddsfrågor.

12.7. Användaren

Alla som hanterar informationstillgångar har ett ansvar att informationssäkerheten upprätthålls.

Varje anställd ansvarar för att följa säkerhetsregler samt att rapportera fel, incidenter och störningar i informationssystem, utrustning och informationsinnehåll enligt fastställda rutiner.

13. Begrepp

Definitioner av begrepp inom informationssäkerhetsområdet utgår från Svenska institutet för standarder SIS-TR 50:2015 med vissa språkliga justeringar.

Begrepp	Definition
Informationssäkerhet	(SS-EN ISO/IEC 27000:2018) Bevarandet av informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.
Konfidentialitet	Informationen är skyddad mot obehörig insyn
Riktighet	Att innehållet i informationen är korrekt och autentisk och inte förvanskad eller kan förvanskas
Tillgänglighet	Att informationen ska vara nåbar när behörig användare behöver den.
Spårbarhet	Att aktiviteter i system entydigt kan härledas till en identifierad användare
Informationsklassning	Att bestämma vilka säkerhetskrav som ska gälla för en informationstillgång, utifrån vilka konsekvenser som kan uppstå om informationen inte hålls tillgänglig, riktig och konfidentiell.
Informationssystem	Applikationer, tjänster eller andra komponenter som hanterar information.
Informationstillgång (verksamhetskritisk)	Information, och resurser som hanterar den, som är av värde för en organisation
Informationsägare	Person eller enhet som har ansvaret för den information som skapas och hanteras inom den egna verksamheten
Informationsförvaltare	Person som hanterar informationen i det dagliga arbetet (Nykvarns kommuns egen definition)
IT-säkerhet	IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet
Ledningssystem för informationssäkerhet (LIS)	Del av organisationens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet
Systemägare	Den som har ett överordnat ansvar för administration, drift och säkerhet för ett informationssystem